# Security Target (ASE)

## CONEXA 3.0 - Smart Meter Gateway

VERSION: 1.95.4[1]
DATE: 2024-12-09
TOE VERSION: 1.5

[1] Revision: 2a61a36, Commit-Date: 2024-12-09 16:11:18 +0100

# 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 uniquely identified as CONEXA 3.0 (CC) 1.5. It is the communication unit used within such an intelligent metering system and represented by the product CONEXA 3.0 except for the integrated Security Module and the wireless communication modules.

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 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 A50.7] and [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)) CONEXA 3.0 (CC) 1.5 wird repräsentiert durch das Gerät CONEXA 3.0 mit Ausnahme des integrierten Sicherheitsmoduls und der Funkmodule. 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 A50.7] und den Ergänzungen nach [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 | Security Target (ASE) - CONEXA 3.0 - Smart Meter Gateway |
| Document Version | 1.95.4 |
| Document Date | 2024-12-09 |
| Authors | Theben Smart Energy GmbH |
| Certification Authority | Bundesamt für Sicherheit in der Informationstechnik<br>Federal Office for Information Security, Germany |
| Certification-ID | BSI-DSZ-CC-0918-V6 |
| 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]. |

## 1.3 TOE Reference

The TOE is uniquely identified as follows:

| | |
|---|---|
| TOE Identification | CONEXA 3.0 |
| TOE Version | 1.5 |
| Developer | Theben Smart Energy GmbH |

The TOE comprises the following components:

| Component | Version | Identified by |
|---|---|---|
| Hardware | HW V01.00 / HW V01.01 | Version string |
| Software | v3.80.0-cc | Version string |
| **Guidance documentation** | | |
| Handbuch CONEXA 3.0 für den Gateway Administrator | 2.13.3 | SHA-256 hash value `e3997512641772752d0c600fce2627aa9d78a525d554d3d15e1e26c825fab715` |
| Handbuch CONEXA 3.0 für den Service-Techniker | 2.14.2 | SHA-256 hash value `1e11af36c4135d43a1dba81acaa373025f3f68fa5849a49c2b58add483691b99` |
| Handbuch CONEXA 3.0 für den Letztverbraucher | 2.12.1 | SHA-256 hash value `c89a8f8f0324a7e145b3895fb82cfe56d7698bc95a3b3b86236ff41c1d2d4d66` |
| Conexa 3.0 Profilbeschreibungen | 2.15 | SHA-256 hash value `d10494d8894cde652ebfc3c29b425041a9c055689cef53bb22d19c8cf2b40af6` |
| COSEM HTTP-Webservice | 2.2 | SHA-256 hash value `8abbabcaff546dbfc060d0100bd2fd6a5b99988af99d9b97c759b22626dea8dd` |
| Conexa 3.0 Logmeldungen | 1.10.1 | SHA-256 hash value `8d9443290843def14260ec9e446cbe510814bcf2f0491e5bdae860a42defb9bc` |
| Schnittstellenbeschreibung IF_GW_CON | 1.4 | SHA-256 hash value `26c821592d7245e29ce91fc25c5dacc0c3310f2885fa9e1baff30d7e97103221` |
| Schnittstellenbeschreibung IF_GW_SRV | 1.4 | SHA-256 hash value `ec094d7ff046c387e921bfdd2d494433083030745cc22cdf20824dc5f5feab99` |
| Anhang sichere Auslieferung | 0.16 | SHA-256 hash value `a71d4484abb51133dca17b902a89e6bdc4be5c0fe7c97e93e982b0a1845167bc` |

**Table 1.1: Identifiable parts of the TOE**

73 The TOE uses the services of the Security Module TCOS Smart Meter Security Module Version 1.0,
74 Release 2/P60C144PVE from T-Systems International GmbH, certified under BSI Certification-ID BSI-
75 DSZ-CC-0957-V2-2016, that is physically integrated into the product Conexa 3.0 and hard-wired to the
76 TOE.
77 The term gateway or SMGW (Smart Meter Gateway) that is used within this Security Target refers always
78 to the TOE excluding the GSM and wM-Bus modules and the Security Module.

## 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 B.

| 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] |
| Gateway<br>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]:<br>• Meter Data Collector<br>• Meter Data Management System<br>• Meter Data Aggregator<br>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 |

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

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

| Term | Definition | Source (if any) |
|---|---|---|
| HAN-T | Network interface with a Mezzanine Connector for the connection of an optional non-TOE HAN-Module. The HAN-Module enables the Consumer to connect to the Smart Meter Gateway via the HAN. If not installed, a connection from CLS [HAN] interface has to be provided to the Consumer. | – |
| 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. | – |
| LMN-A-T | LMN-Interface to a non-TOE wireless M-Bus module. The module enables wireless attached Meters to be connected to the LMN. | – |
| 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 |
| 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] |
| Processing Profile | File used to parameterize the Smart Meter Gateway. In this and the following documents the Processing Profiles depend on the Profiles defined by the DKE AK 461.0.142 [DKE COSEM]. | – |
| 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. | – |

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

| Term | Definition | Source (if any) |
|---|---|---|
| SM-T | Physical interface for the connection of the Security Module which is located underneath the enclosing case of the Smart Meter Gateway. The module itself is not part of the TOE. | – |
| 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] |
| WAN-A-T | Physical interface which enables the connection of the Smart Meter Gateway to the WAN via an attached GSM wireless module. The module itself is not part of the TOE. | – |

**Table 1.2: Specific Terms**

# 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].

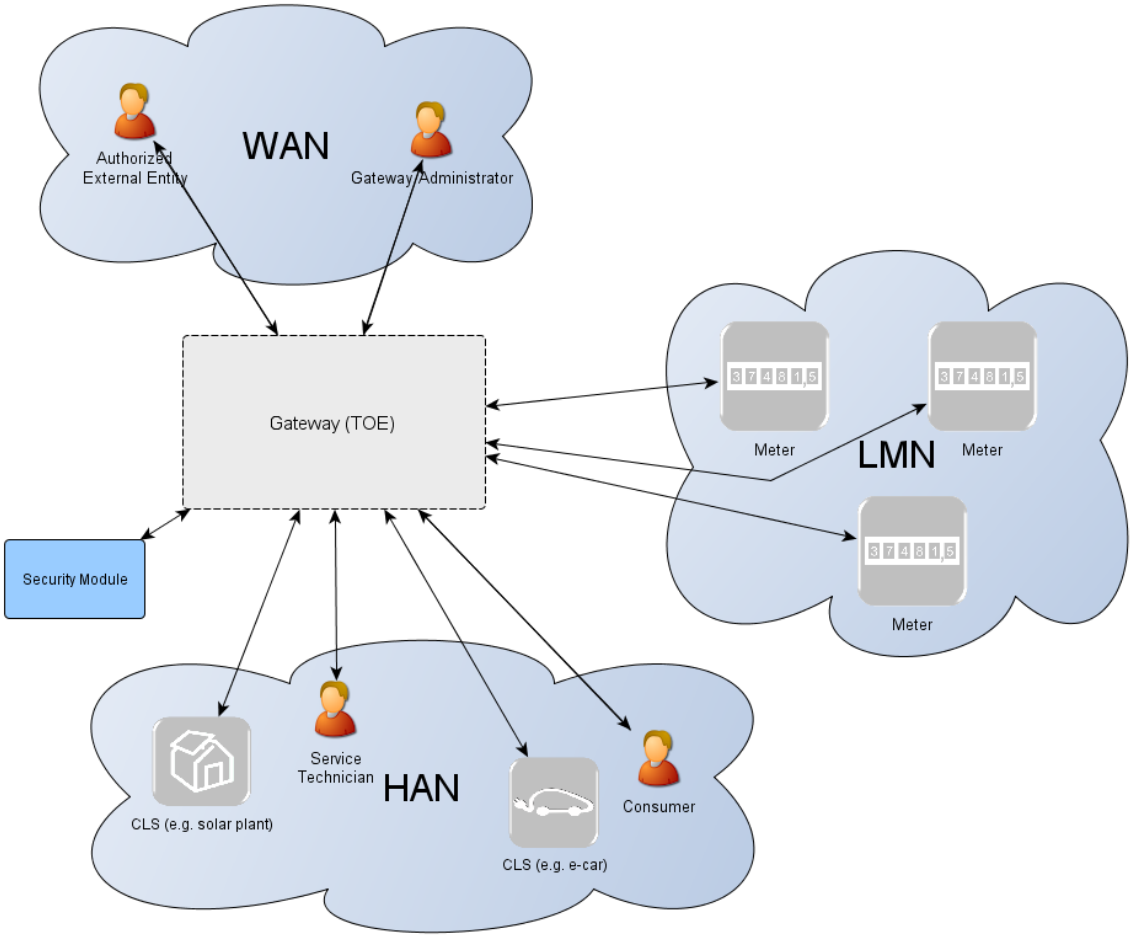



**Figure 1.1: The TOE and its direct environment**

As can be seen in Figure 1.1 a system for smart metering comprises different functional units in the context of the descriptions in this ST:

- The **Gateway** (as defined in this ST) serves as the communication component between the components in the LAN of the Consumer (such as meters and added generation plants) and the outside

[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.

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[6] the information will be encrypted and signed using the services of a Security Module. The Gateway features a mandatory user interface, enabling authorised Consumers to access the data relevant to them.

- The **Meter** itself records the consumption or production of one or more commodities (e.g. electricity, gas, water, heat) and submits those records in defined intervals to the Gateway. The Meter Data has to be signed and encrypted before transfer in order to ensure its confidentiality, authenticity and integrity. The Meter is comparable to a classical meter[7] and has comparable security requirements; it will be sealed as classical meters 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[8].

- 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 1.2) 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 section 1.5.7 and section 1.5.8.

Please note that the arrows of the interfaces within the Smart Metering System as shown in Figure 1.2 indicate the initialization of the information flow. Indeed, the following chapters of this ST will place dedicated requirements on the way an information flow can be initiated.

Some interfaces from the Protection Profile [SMGW-PP] have different implementations in the CONEXA 3.0 TOE. Therefore some more interfaces names have been defined, to ease the description of the various CONEXA 3.0 interface implementations. In Figure 1.2 the interface names comming from the Protection Profile are black coloured. The additional interface names are coloured green.

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

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

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

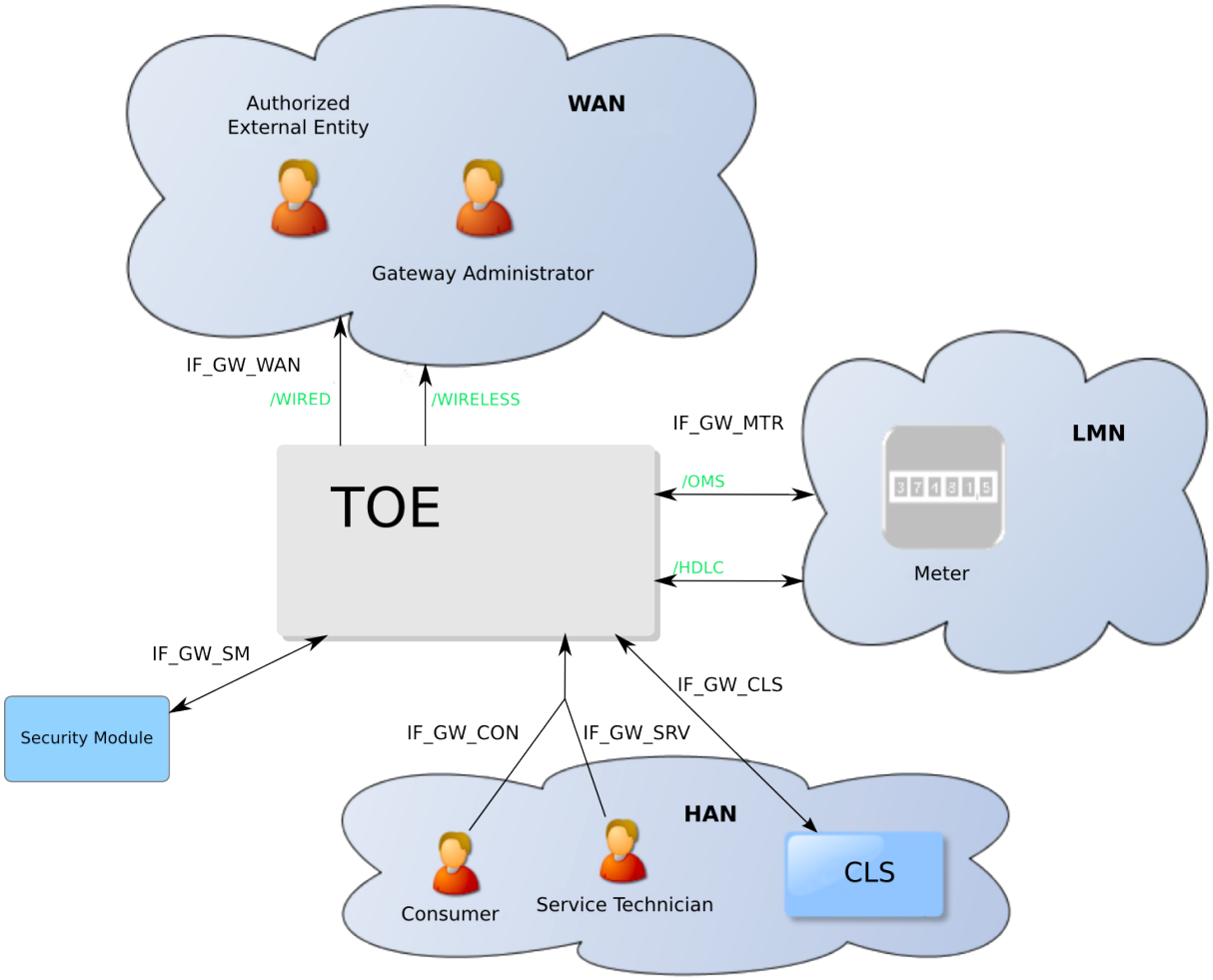



**Figure 1.2: The logical interfaces of the TOE**

### 1.5.3 Requirements on the operational environment of the TOE

For a secure operation of the TOE the Security Module TCOS Smart Meter Security Module Version 1.0 Release 1/P60C144PVA from T-Systems International GmbH that is Common Criteria certified in conformance to [SM-PP] is physically integrated into the Conexa. 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 wired attached Meters located in the LMN network shall provide an TIA-485 interface and support communication via COSEM objects using SML and optionally SMLplus. Further those Meters shall be able to communicate with the TOE using TLS via HDLC. For interfacing to wireless attached Meters, the TOE implements an interface to a wM-Bus module. Wireless attached Meters shall provide a wM-Bus compatible transmitter for unidirectional communication.

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 an interface to a wireless module and an Ethernet interface. To use the wireless module, which is not part of the TOE, 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 send new processing profiles to the TOE.

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[9] 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[10].

### 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)
- **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**

[9] 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.

[10] 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.

177 • **Management** of Security Functionality

178 • **Identification and Authentication** of users

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

#### 180 1.5.6.1 Handling of Meter Data[11]

181 The Gateway is responsible for handling Meter Data. It receives the Meter Data from the Meter(s),
182 processes it, stores it and submits it to external entities.
183 The TOE utilises Processing Profiles to determine which data shall be sent to which component or external
184 entity. A Processing Profile defines:

185 • how Meter Data must be processed,

186 • which processed Meter Data must be sent in which intervals,

187 • to which component or external entity,

188 • signed using which key material,

189 • encrypted using which key material,

190 • whether processed Meter Data shall be pseudonymised or not, and

191 • which pseudonym shall be used to send the data.

192 The Processing Profiles are not only the basis for the security features of the TOE; they also contain
193 functional aspects as they indicate to the Gateway how the Meter Data shall be processed. Further
194 Processing Profiles are used to allocate and connect Meter located in the LMN to the SMGW. More details
195 on the Processing Profiles can be found in [TR 03109-1].
196 The Gateway will restrict access to (processed) Meter Data in the following ways:

197 • Consumers shall be identified and authenticated first before access to any data may be granted,

198 • the Gateway shall accept Meter Data from authorised Meters only,

199 • the Gateway shall send processed Meter Data to correspondingly authorised external entities only.

200 The Gateway shall accept data (e.g. configuration data, firmware updates) from correspondingly autho-
201 rised Gateway Administrators or correspondingly authorised external entities only. This restriction is
202 a prerequisite for a secure operation and therewith for a secure handling of Meter Data. Further, the
203 Gateway shall maintain a Calibration Log with all relevant events that could affect the calibration of the
204 Gateway.
205 These functionalities shall

206 • prevent that the Gateway accepts data from or sends data to unauthorised entities,

207 • ensure that only the minimum amount of data leaves the scope of control of the Consumer[12],

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

[12] 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.

- preserve the integrity of billing processes and as such serve in the interests of the Consumer as well as in the interests of the supplier. Both parties are interested in an billing process that ensures that the value of the consumed amount of a certain commodity (and only the used amount) is transmitted[13],
- 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 1.2) and allows the Consumer to obtain information via this interface. This information comprises the billing-relevant data (to allow the Consumer to verify an invoice) and information about which Meter Data has been and will be sent to which external entity. The TOE ensures that the communication to the Consumer is protected by using TLS and ensures that Consumers only get access to their own data.

#### 1.5.6.2 Confidentiality protection

The TOE protects data from unauthorised disclosure

- while received from a Meter via the LMN,
- 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.
- 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:

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

- 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[14]; specifically connection establishment by an external entity in the WAN or a Meter in the LMN to the WAN is not possible,
- the Gateway can establish connections to devices in the LMN or in the HAN,
- Meters in the LMN are only allowed to establish a connection to the Gateway,
- the Gateway 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).

The communication flows that are enforced by the Gateway between parties in the HAN, LMN and WAN are summarized in the following table[15]:

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

[15] 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.

| **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[16] | No connection establishment allowed | – (see following list) |

**Table 1.3: 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.

#### 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)[17].
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.

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

[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.

In order to allow this kind of re-activeness of 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 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[18] 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**

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

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. 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.

#### 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. If the Gateway Administrator permits it in the Processing Profiles, the 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 1.2 also indicates the cardinality of the interfaces. The following table provides an overview of the mandatory external interfaces of the TOE and provides additional information:

| Interface Name | Description |
|---|---|
| IF_GW_CON | Via this interface the Gateway provides the Consumer[19]with the possibility to review information that is relevant for billing or the privacy of the Consumer. Specifically the access to the Consumer Log is only allowed via this interface. |
| IF_GW_MTR | Interface between the Meter and the Gateway. The Gateway receives Meter Data via this interface. |
| 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. |
| IF_LED | Interface to display actual status information for local users. |

**Table 1.4: TOE external interfaces**

There exist some more interfaces used for production and development purposes. These interfaces are disabled by software in normal operation mode. In [FSP, chapter 3.1] this table will be amended by these interfaces. Their usage and how these interfaces are disabled will be explained in [FSP, chapter 2 and chapter 3] in more detail.

### 1.5.8 TOE physical boundary

The TOE comprises all hard- and software components which are located on the upper circuit board (called CPU Platine) besides the Security Module and including the casing.

### 1.5.9 The interfaces of the TOE and its enclosing case

There are multiple interfaces in different design levels of the TOE and the surrounding environment. The aim of the following Table 1.5 and Figure 1.3 is to give an overview of these set of interfaces, their meaning, and functions.

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

| Description | Physical (TOE boundary) | Physical (SMGW casing) | TSFI (logical) | Subtype |
|---|---|---|---|---|
| WAN interface wired | WAN-1 | WAN-1 | IF_GW_WAN | WIRED |
| WAN interface wireless | WAN-A-T | WAN-A[20] | IF_GW_WAN | WIRELESS |
| HAN interface | HAN-T | HAN[21] | IF_GW_CON<br>IF_GW_CLS<br>IF_GW_SRV | - |
| CLS interface | CLS [HAN] | CLS [HAN] | IF_GW_CON<br>IF_GW_CLS<br>IF_GW_SRV | - |
| LMN interface wired | LMN-1-T | LMN-1 | IF_GW_MTR | HDLC |
| LMN interface wireless | LMN-A-T | LMN-A[22] | IF_GW_MTR | OMS |
| Status LEDs | LEDs | LEDs | - | - |
| SMGW-Casing | Casing | Casing | - | - |
| Interface for the Security Module | SM-T | -[23] | - | - |

**Table 1.5: Assignment of interfaces**

There exist some more interfaces used for production and development purposes. These interfaces are disabled by software in normal operation mode. In [FSP, chapter 3.1] this table will be amended by these interfaces. Their usage and how these interfaces are disabled will be explained in [FSP, chapter 2 and chapter 3] in more detail.

[20] Please note that the interface WAN-A is not the same interface as WAN-A-T. WAN-A is the interface at the output side of the GSM wireless module, which is not part of the TOE.

[21] Please note that the interface HAN is not the same interface as HAN-T. HAN is the interface at the optional HAN-Module, which is not part of the TOE.

[22] Please note that the interface LMN-A is not the same interface as LMN-A-T. LMN-A is the interface at the output side of the wM-Bus wireless module, which is not part of the TOE.

[23] The interface SM-T is not accessible at the casing of the SMGW. This interface terminates under the surrounding SMGW casing. The interface connects to the internal Security Module that is not part of the TOE. In this and the following documents IF_GW_SM will be used for the description of the logical interface to the Security Module.

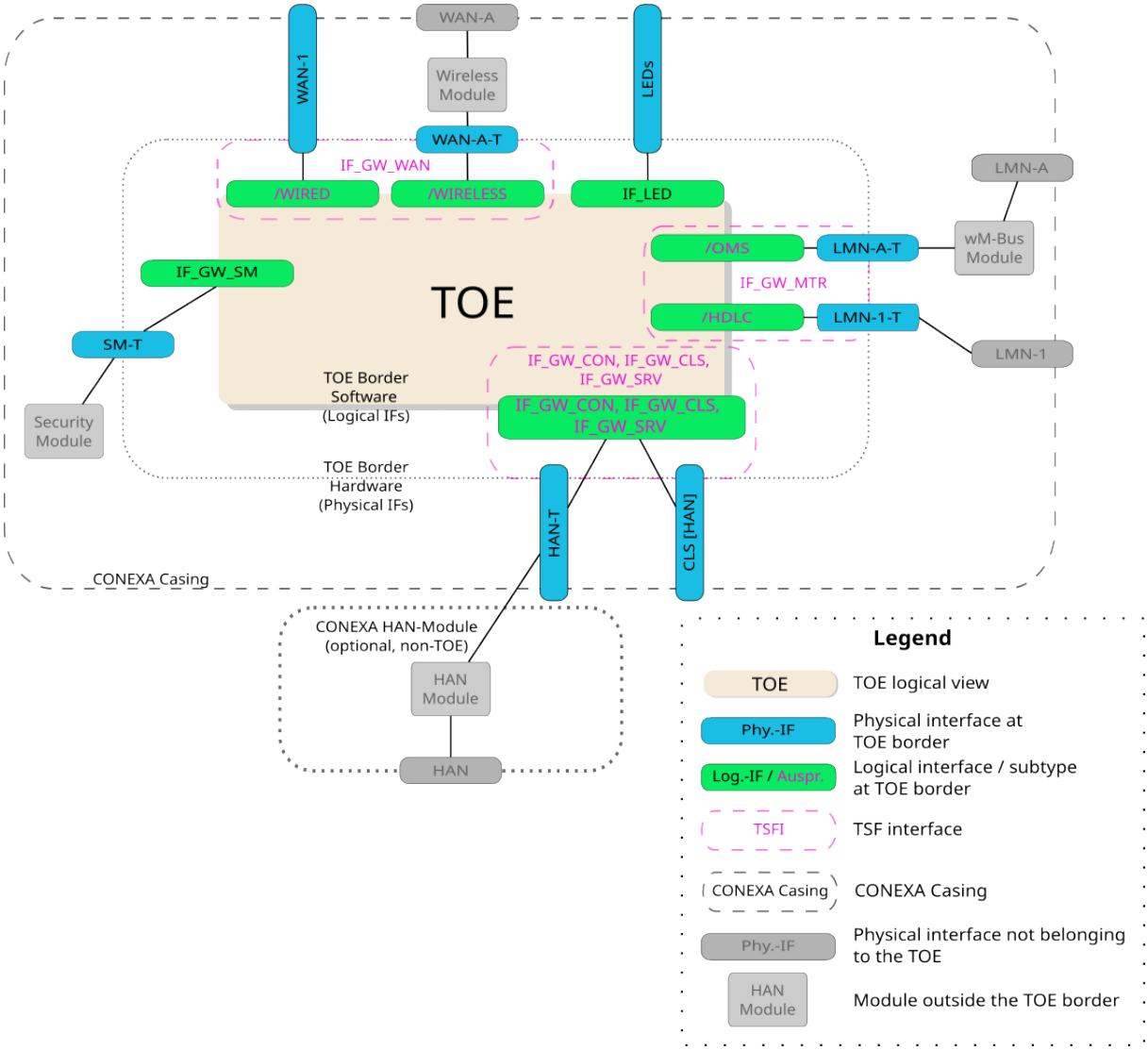



**Figure 1.3: Overview of the interfaces of the CONEXA 3.0 SMGW**

The Figure 1.3 consists on the two big inner circles for the logical (TOE Border Software) and the physical (TOE Border Hardware) TOE borders. The interface names like they are used in this document for the TOE border are placed on these dotted circles. The physical interfaces of the Conexa casing are placed on the outer circle (CONEXA Casing).

To simplify the understanding of the interface structure, the names of the interfaces have different colours. These colours depend on the source of the interface name and the interface type. The interface names taken from the Protection Profile [SMGW-PP] (TSFI) are written in purple colour and surrounded by a purple dotted line. The logical TOE interface names are surrounded by a green coloured box. The physical TOE interface names are surrounded by a blue coloured box. All grey coloured componentes are not part of the CONEXA 3.0 TOE.

#### 1.5.9.1 Overview of the TOE hardware

The minimal implementation of a secure TOE for a Smart Meter Gateway is shown in Figure 1.4 and was taken from the Protection Profile [SMGW-PP].

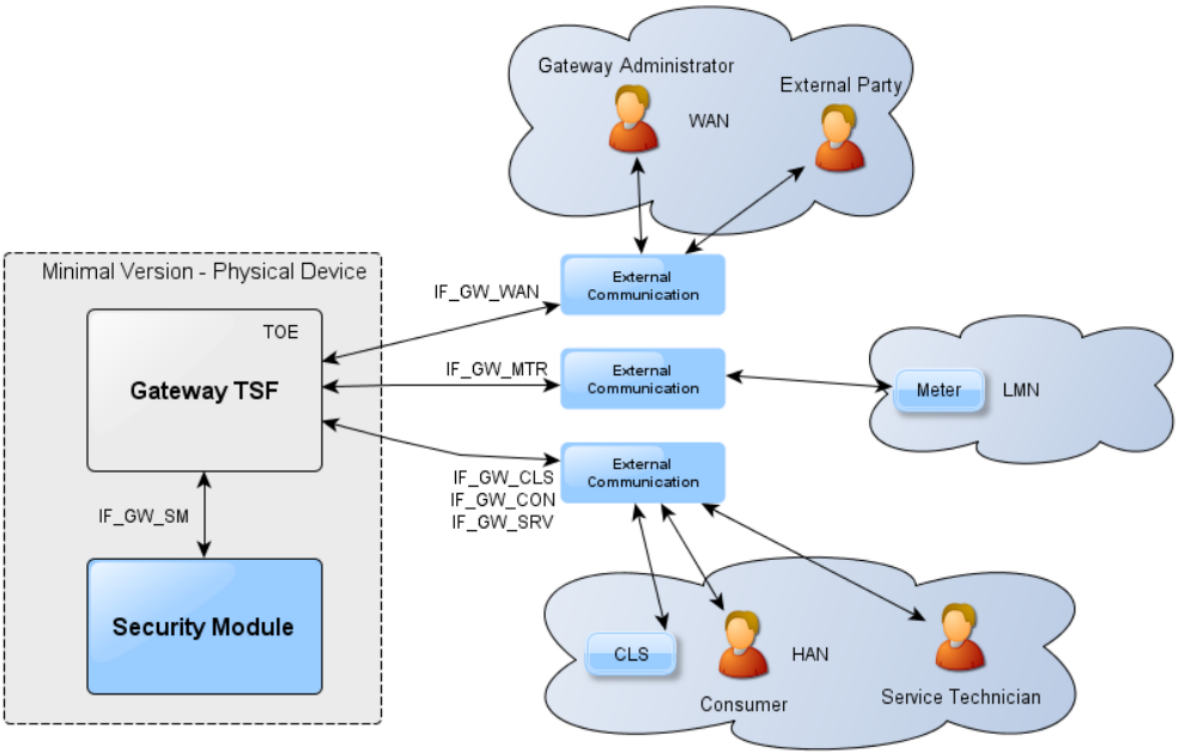



**Figure 1.4: Smart Meter Gateway TOE using external communication devices**

In Figure 1.4 the TOE does not include the external communication devices, that enable the physical connection to the WAN, LMN and HAN. The implementation of the CONEXA 3.0 TOE based in parts on this minimal design version. These parts which use external communication devices are:

- the GSM module for the wireless WAN connection connected at the WAN-A-T interface,
- the RS485 module for the wired LMN connection, connected at the LMN-1-T interface,
- the wM-Bus module for the wireless LMN connection, connected at the LMN-A-T interface and
- the optional HAN-Module for the HAN connection, connected at the HAN-T interface.

The following Figure 1.5 provides an overview about the casing of the SMGW. In particular, the figure shows the external interfaces of the TOE that are visible and connectable at the case of the Smart Meter Gateway. Both wireless interfaces (WAN-A, LMN-A) are not part of the TOE. The TOE border for this interfaces ends at the input side of the corresponding wireless modules.

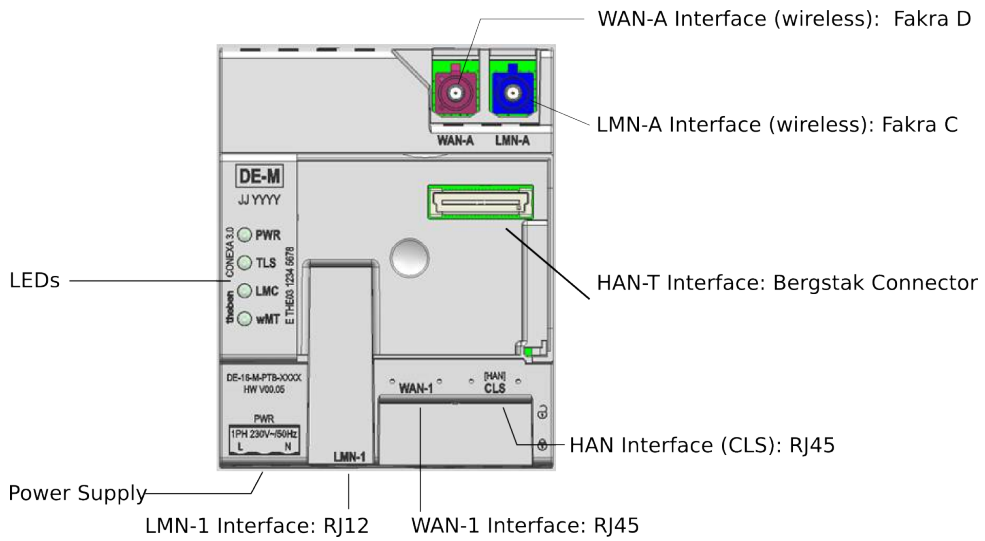



**Figure 1.5: Casing of the TOE - External interfaces**

Figure 1.6 shows the hardware parts of CONEXA 3.0.

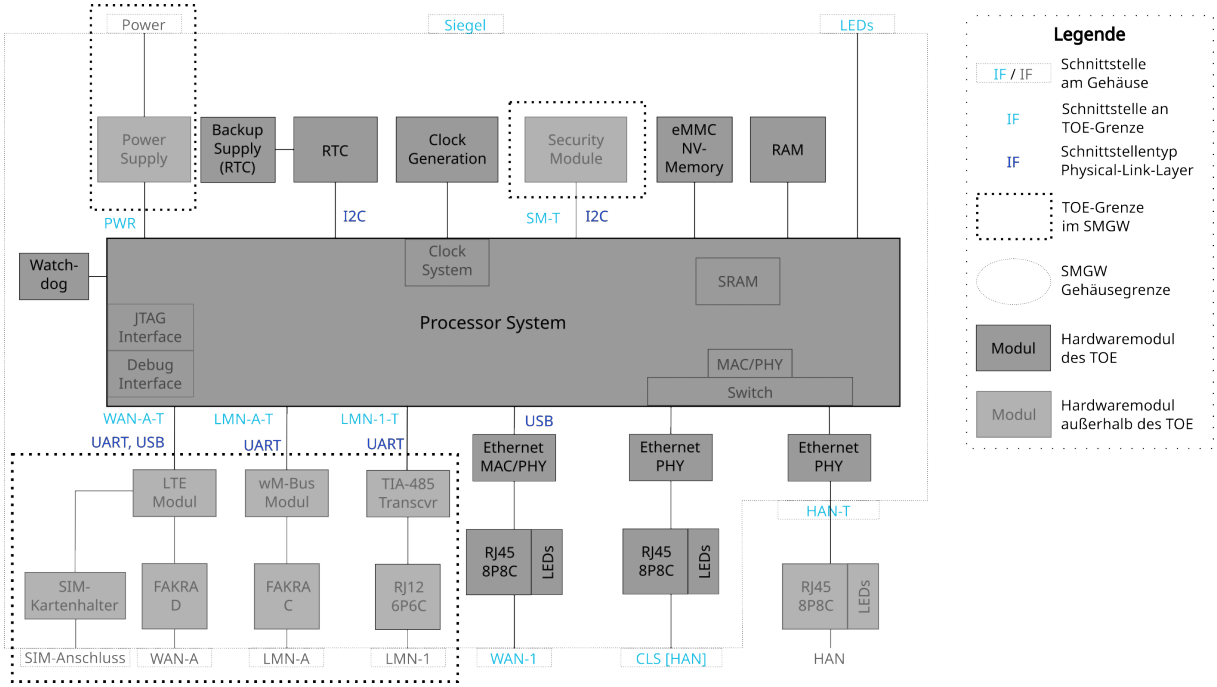



**Figure 1.6: The hardware parts of the TOE**

In Figure 1.6 the physical interfaces at the Conexa casing are surrounded by a small box with small dotted lines. The physical interfaces of the TOE are colored in light blue. The components drawn in light gray and surrounded by a dotted lines are not part of the TOE. Please note that these components are physically integrated into the CONEXA 3.0 but are not part of the TOE.
The components are briefly described below.

**Power Supply**
This component supplies all other components of CONEXA 3.0 with voltage providing the correct powersequencing. It provides the external interface Power (cf. Figure 1.5).

**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.

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

**Security Module**
The Security Module TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE from T-Systems International GmbH, certified under BSI Certification-ID BSI-DSZ-CC-0957-V2-2016, is integrated into the Conexa but is not part of the TOE. Mainly the TOE uses the functionality of the Security Module for cryptographic support. For more information please refer to section 1.5.10.
The logical interface IF_GW_SM is provided on the physical interface SM-T which is located underneath the enclosing case.

**External Memories**
This component provides non-volatile storage used for code and data (FLASH) and random access memory (RAM) used by the Processor System.

**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.

- MAC-PHY / Switch

  These components are used to connect the CPU to the PHYs of the HAN interfaces.

**IF_GW_WAN**
The logical interface IF_GW_WAN is realized by the following two interfaces:

- IF_GW_WAN/WIRELESS

  This interface enables the communication between the TOE and external entities located in the WAN via an attached GSM wireless module, supporting GSM and GPRS and LTE. The physical interface WAN-A-T which is located underneath the enclosing case as shown in Figure 1.6 and a LED that displays the connection status are therefore provided by the TOE. The external interface WAN-A, the FAKRA D-Socket and the SIM card slot and tray are not part of the TOE (cf. Figure 1.5).

- IF_GW_WAN/WIRED

This component implements the external, physical interface WAN-1 (cf. Figure 1.5) and hence, enables a wired connection between the TOE and external entities located in the WAN. As an interface for a router the TOE provides an 8p8c-Socket (RJ45). After the installation and start of operation (cf. section 1.5.11) the Socket is located beneath the sealed casing of the SMGW. Further, an LED located on the frontside of the SMGW casing displays the connection status.

**IF_GW_MTR**

The logical interface IF_GW_MTR is realized by the following two interfaces:

- IF_GW_MTR/OMS

  This interface enables the communication between the TOE and Meters located in the LMN via an attached wM-Bus wireless module, supporting wireless M-Bus. Therefore the TOE provides the physical interface LMN-A-T which is located underneath the enclosing case shown in Figure 1.6. The external interface LMN-A and the FAKRA C-Socket (cf. Figure 1.5) are not part of the TOE.

- IF_GW_MTR/HDLC

  This component provides the external, physical interface LMN-1 (cf. Figure 1.5) and hence, enables a wired connection based on TIA-485 and HDLC communication between the TOE and Meters located in the LMN. Therefore the TOE provides an 6p6c-Socket (RJ12). Further this interface is used to power supply some of the Meters using this interface.

**IF_GW_CON, IF_GW_SRV and IF_GW_CLS**

The physical interface to the HAN is represented by a 8p8c-Socket (RJ45) (CLS [HAN]) and a Bergstak Mezzanine Connector (HAN-T). The two interfaces are separated by an Ethernet Switch which is a part of the CPU. The Mezzanine Connector is used to connect to an optional HAN-Module which provides a 8p8c-Socket (RJ45) and maybe equipped with other non TOE HAN/CLS components. The HAN-Module is not part of the TOE. This way, an user is able to connect a display or another device to get access to the Consumer Log or to view his consumption data (HAN Interface (Consumer), cf. Figure 1.5) if authenticated. If the module is not present the Energy Service Provider has to add an external switch to grant the user access to the HAN. In addition, The other socket is used for the communication between the TOE and the CLS located in the HAN (HAN Interface ( CLS), cf. Figure 1.5). After the installation and start of operation (cf. section 1.5.11) this socket is located inside the sealed cabinet enclosing the SMGW. Both sockets can be used by Service Technicians to read the System Log or start the selftest. Further, the TOE provides two LEDs on the frontside of the SMGW casing which display the connection status.

**IF_LED**

The TOE comprises four LEDs (light emitting diodes) which are located on the front side of the SMGW casing. The LEDs provide information about the connection status of the interfaces of the TOE. It provides the external interface *LED* (cf. Figure 1.5)

**Casing**

The TOE consists of a hardware and a software part. One hardware part is the casing of the Smart Meter Gateway. The casing is an interface for the fixation of a seal to allow an authorized user to detect a physical manipulation. (cf. Figure 1.5)

#### 1.5.9.2 Overview of the TOE software

The TOE software is based on a Linux operating system (OS). The Linux Kernel includes all required hardware drivers for TOE hardware. Also all required Kernel software-modules are built-in. Dynamic loading of drivers or software-modules is deactivated (not built-in by build config) in Kernel.

To get the OS running, a bootloader initializes the TOE hardware, selects kernel image from persistent memory, loads it into RAM and gives control to kernel (boot kernel image). Selecting kernel image is required because kernel is stored twice to have a redundant boot option i.e. on memory defects.

On kernel startup all hardware devices are (re-)initilialized by kernel according built-in configuration (device tree). Kernel image also includes a RAM-disk with a minimal system (root file system) containing a minimal-init process, called miniinit.

The miniinit process prepares the TOE / Linux runtime environment by setting up temporary and pseudo-filesystems. Further miniinit selects and mounts the root file system (root partition). Selecting root file system is required because it is stored twice (each on a separate memory partition) to have a redundant boot option i.e. on memory defects. Finally miniinit switches from RAM-disk to selected root file system. From here a custom init process (smgw-init) located on root file system is taking control.

TOE functionality is split up into several software components named "SMGW applications". Not all of these applications are security-relevant but are necessary for functional operation. Every component is started by smgw-init according a defined start order. Access rights and system capabilities are set-up by smgw-init for each started process as well. Further each process is observed and controlled by smgw-init using implemented software-watchdog and selftest functions. Malfunctions will lead to process restart or even system reboot in case of fatal failures.

Based on selftest results smgw-init may also switch system into a secure minimal operation mode, called "secure state". Not all SMGW application will run on this minimal operation mode (reduced functionality) but full administrative access is available for Gateway Administrator.

After all SMGW applications are started by smgw-init and running as required, TOE interfaces are available for use. Functionality provided by SMGW applications internally (core) and on TOE interfaces is described below.

**Core functionality**
Some TOE functionality is not directly assigned to an interface but is realized by SMGW core applications. One of these functions is configuration handling. Configuration done by Gateway Administrator is stored persistent in TOE and provided to SMGW applications for their special need / required operation.

Initial TOE configuration is done within personalization process on manufacturer site (see section 1.5.11) by initial configuration file provided by Gateway Administrator. Once TOE is initially configured, configuration can only be done by connected Gateway Administrator.

Another core functionality is log handling. All logs issued by SMGW applications are stored into maintained logbooks:

- System Log

  This logbook holds global system events. Some System Logs are send directly to Gateway Administrator on occurence.
  Reading the System Log is restricted to Gateway Administrator and Service Technician.

- Calibration Log

  This logbook holds events required by national calibration authority. Some Calibration Logs are send directly to Gateway Administrator on occurence.
  Reading the Calibration Log is restricted to Gateway Administrator.

- Consumer Log

For each configured Consumer a dedicated logbook is maintained by TOE.
Reading the Consumer Log is restricted to assigned Consumer only. Therefor entries from Consumer Log are never send to Gateway Administrator.

Log handling also includes watching System Logs for security relevant issues. In case of security relevant issue detection, system is switched to secure minimal operation mode, called "secure state".

**Functionality on IF_GW_WAN**
On IF_GW_WAN interface channels to external entities in WAN are established by TOE software. Each channel is a mutual authenticated TLS channel initialized by TOE (TLS client) to a configured endpoint. Required channels for initial operation can be configured within personalization process (initial configuration).

| Channel name | endpoint entity | purpose |
|---|---|---|
| MANAGEMENT | Gateway Administrator | management functions, i.e. configuration or log review |
| ADMIN-SERVICE | Gateway Administrator | sending logs, software update download |
| NTP-TLS | timeserver on behalf of Gateway Administrator | system time syncronization |
| INFO-REPORT | external entity called EMT | sending billing relevant meter data |
| CLS-WAN | external entity called EMT | communication with CLS via TOE (proxy) |

**Table 1.6: WAN channels**

All WAN TLS channels are established by TOE on demand and kept established as long as configured or closed by peer. At least TLS channels on WAN will be closed after 48 hours by TOE.

To enable Gateway Administrator to trigger a MANAGEMENT connection, incoming wake-up messages will be accepted on IF_GW_WAN as described in section 1.5.6.5.

For management purposes on MANAGEMENT channel, TOE is providing a webserver with a RESTful API as specified in [TR 03109-1]. This webserver is reachable via MANAGEMENT channel only and not directy via any TOE interface.

Local time (system time) will be syncronized with a reliable external time source in WAN. For synchronization ntp via TLS channel is used ("NTP-over-TLS" / NTP-TLS).
Without a valid time, system will not get into full operational mode.

For CLS proxy purposes "CLS-WAN" channels are established by TOE. Data transferred on these channels are not handled by TOE but redirected to configured CLS device on IF_GW_CLS and vice versa (proxy functionality).

**Functionality on IF_GW_CON**
IF_GW_CON may be used by users (Consumers) on HAN to access TOE. Therefore the TOE is providing a HTTPS webserver with HTML API on this interface. Following functionality is provided by this webserver:

- View meter data associated to Consumer.

- Review Consumer Log entries.
- Trigger TOE self test.

Consumer authentication on IF_GW_CON is done either via mutual TLS authentication (TLS certificates) or by unique username and password. Each Consumer has to be configured by Gateway Administrator.

**Functionality on IF_GW_SRV**
IF_GW_SRV may be used by a Service Technician on HAN to access TOE. Therefore the TOE is running a HTTPS webserver with a RESTful API on this interface.

Authentication on IF_GW_SRV is done via mutual TLS authentication (TLS certificates) only. Service Technician access has to be configured by Gateway Administrator.

**Functionality on IF_GW_CLS**
A CLS on HAN may establish a connection to TOE via IF_GW_CLS. Connections will be accepted only if device is configured on TOE by Gateway Administrator. Connection is done via SOCKSv5 protocol with included TLS handshake whereby TOE is TLS server. The TOE may also establish a connection as a TLS client to a CLS if configured by Gateway Administrator. Authentication on IF_GW_CLS is done via mutual TLS authentication (TLS certificates) only.

If a configured CLS established a connection on IF_GW_CLS, corresponding CLS-WAN connection to external entity (EMT) on IF_GW_WAN will be established by TOE. For data flow TOE acts only as proxy transferring data from CLS to EMT and vice versa.

**Functionality on IF_GW_MTR**
Meter data is captured/accepted on IF_GW_MTR (LMN) only. There are two physical interfaces provided by TOE:

- IF_GW_MTR/OMS

  This wireless interface is using wireless M-Bus (OMS) protocol to capture meter data.

- IF_GW_MTR/HDLC

  This wired interface is using HDLC protocol on a TIA-485 bus. TOE acts as master on that bus providing bus addresses to connected meters.

All meter communication on IF_GW_MTR is encrypted. Meter data is only captured for meters configured by Gateway Administrator. If meter connection is bi-directional, only configured meters are requested for data.

Captured meter data is transformed to an internal Meter Record format regardless what protocol is used by meter itself. This unified format is used to simplify handling and storage of the data.

After meter data has been captured, it is processed according Processing Profiles configured by Gateway Administrator. Processing meter data covers:

- capturing meter data in a configured interval
- providing billing relevant meter data (tariff data)
- storing captured/tariffied data

603 - sending billing relevant meter data
604 to external entities (EMT) in WAN
605 via INFO-REPORT channel described above

606 - deleting stored data after handling is done
607 or after configured archive period.

### 608 1.5.10 The cryptography of the TOE and its Security Module

609 Parts of the cryptographic functionality used in the upper mentioned functions shall be provided by a
610 Security Module. The Security Module provides strong cryptographic functionality, random number
611 generation, secure storage of secrets and supports the authentication of the Gateway Administrator. The
612 Security Module is a different IT product and not part of the TOE as described in this ST. Nevertheless it
613 is physically embedded into the CONEXA 3.0 and protected by the same level of physical protection.
614 The requirements applicable to the Security Module are specified in a separate PP (see [SM-PP]).
615 The following table provides a more detailed overview on how the cryptographic functions are distributed
616 between the TOE and its Security Module.

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

**Table 1.7: Cryptographic support of the TOE and its Security Module**

#### 1.5.10.1 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 1.7:

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

   Or

   (c) If a unidirectional communication is performed between the Meter and the Gateway the Meter Data is encrypted using a symmetric algorithm (according to [TR 03109-3]) and facilitating a defined data structure to ensure the authenticity and confidentiality.
3. The authenticity and integrity of the Meter Data is verified by the Gateway
4. If (and only if) authenticity and integrity have been verified successfully the Meter Data is further processed by the Gateway according to the rules in the Processing Profile else the cryptographic information flow will be cancelled.
5. The processed Meter Data is encrypted and integrity protected using CMS (according to [TR 03109-1-I]) for the final recipient of the data[24].
6. The processed Meter Data is signed using the services of the Security Module.
7. The processed and signed Meter Data may be stored for a certain amount of time.
8. The processed Meter Data is finally submitted to an authorised external entity in the WAN via an encrypted and mutually authenticated channel.

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

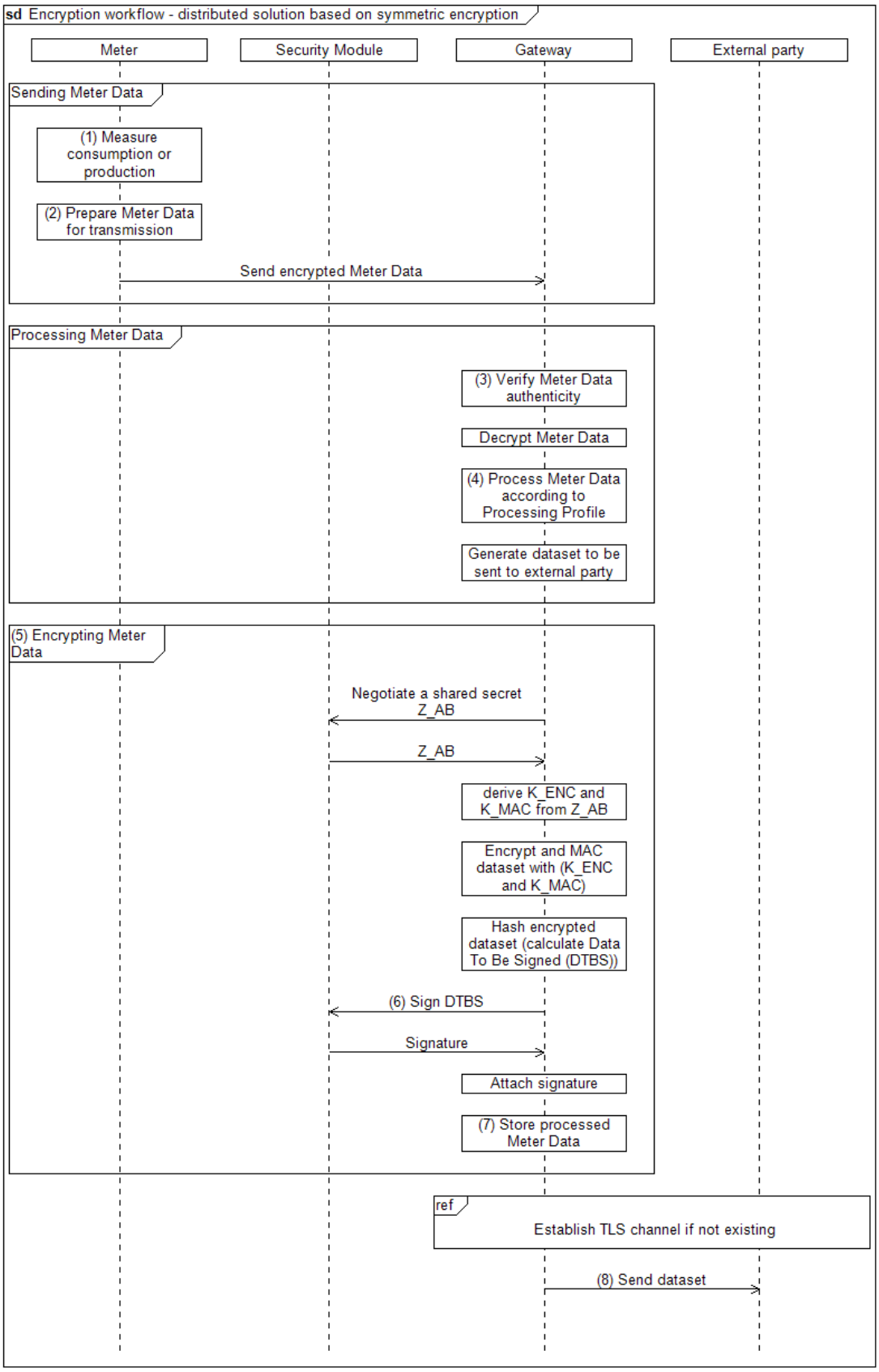



**Figure 1.7: Cryptographic information flow for distributed Meter and Gateway**

655 ### 1.5.11 TOE life-cycle

656 The life-cycle of the Gateway can be separated into the following phases:

657 1. Development
658 2. Production
659 3. Pre-personalization at the developer's premises (without Security Module)
660 4. Pre-personalization and integration of Security Module
661 5. Delivery to the MPO
662 6. Delivery by the MPO to the installation and operational environment
663 7. Normal operation

664 A detailed description of the different phases is provided in [TR 03109-1-VI].
665 The certified configuration of the TOE will be established after phase "Personalization". It is ensured that
666 previous phases are performed by trusted personal in secure environments.

# 2. Conformance Claims

## 2.1 CC Conformance Claims

This ST has been developed using Version 3.1 Revision 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], version 1.3.

In comparison to the PP, the assumption A.Delivery and the security objective for the environment OE.Delivery have been added and a refinement on the assurance component ALC_DEL.1 has been made in order to reduce the certified scope of the TOE delivery to the MPO.

## 2.3 Conformance claim rationale

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.

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. [25]

The security requirements of this ST comply with the security requirements in the Gateway PP [SMGW-PP], as this security target claimed strict conformance to the Gateway PP 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.

## 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.

[25] In consultation with the certification body, the OE.Delivery (mentioned in section 4.2) was added to address a new delivery method.

# 3. Security Problem Definition

## 3.1 External entities

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

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

**Table 3.1: Roles used in the Protection profile**

## 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 3.2 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.<br>Meter Data comprise Consumption or Production Data (billing-relevant) and grid status data (not billing-relevant).<br>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<br>• System Log. | • Integrity<br>• Confidentiality (only authorised SMGW administrators and Service technicians may read the log data) |
| Consumer Log data | Log data from the<br>• Consumer Log. | • Integrity<br>• Confidentiality (only authorised Consumers may read the log data) |
| Calibration Log data | Log data from the<br>• Calibration Log. | • Integrity<br>• Confidentiality (only authorised SMGW administrators may read the log data) |
| Consumption Data | Billing-relevant part of Meter Data.<br>Please note that the term Consumption Data implicitly includes Production Data. | • Integrity and authenticity (comparable to the classical meter and its security requirements)<br>• Confidentiality (due to privacy concerns) |
| Status Data | Grid status data, subset of Meter Data that is not billing-relevant[26]. | • Integrity and authenticity (comparable to the classical meter and its security requirements)<br>• Confidentiality (due to privacy concerns) |

[26] 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 |
|---|---|---|
| Supplementary Data | The Gateway may be used for communication purposes by devices in the LMN or HAN. It may be that the functionality of the Gateway, that is used by such a device is limited to pure (but secure) communication services. Data that is transmitted via the Gateway but that does not belong to one of the aforementioned data types is named Supplementary Data. | • According to their specific need |
| Data | The term Data is used as a hypernym for Meter Data and Supplementary Data. | • According to their specific need |
| Gateway time | Date and time of the real-time clock of the Gateway. Gateway Time is used in Meter Data records sent to external entities. | • Integrity<br>• 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 3.2: Assets (User data)**

701 Table 3.3 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<br>• 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<br>• 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<br>• Confidentiality |
| Firmware update (secondary asset) | Firmware update that is downloaded by the TOE to update the firmware of the TOE. | • Integrity and authenticity |

| Asset | Description | Need for Protection |
|---|---|---|
| Ephemeral keys (secondary asset) | Ephemeral cryptographic material used by the TOE for cryptographic operations. | • Integrity and authenticity<br>• Confidentiality |

**Table 3.3: 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[27],
- if devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is appropriately protected.

[27] 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.

**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.

**A.Delivery** After the reception of the TOE by the MPO, the MPO is responsible for the secure delivery of the TOE to the installation and operational environment. It is assumed that the MPO is trustworthy in context of this delivery and well trained and takes appropriate security measures to ensure protection against undetected manipulation or undetected replacement of the TOE during such a delivery to ensure integrity and authenticity of the TOE. Note that adhering to [MSB-Katalog] is sufficient for MPOs to fulfill this assumption.

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

The level of physical protection that is expected to be provided by the environment is the same level of protection that is expected for classical meters that operate according to the regulations of the national calibration authority [TR 03109-1].

**Application Note 2:** The Processing Profiles that are used for information flow control as referred to by A.ProcessProfile are an essential factor for the preservation of the privacy of the Consumer. The Processing Profiles are used to determine which data shall be sent to which entity at which frequency and how data are processed, e.g. whether the data needs to be related to the Consumer (because it is used for billing purposes) or whether the data shall be pseudonymised.

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

It is essential that Processing Profiles correctly define the amount of information that must be sent to an external entity.

## 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

718 trying to conquer a component of the infrastructure (i.e. Meter, Gateway or Controllable Local
719 System) via the WAN to cause damage to a component itself or to the corresponding grid (e.g. by
720 sending forged Meter Data to an external entity).

721 The definition of the following threats acknowledges that the local attacker (facilitating physical access)
722 has less motivation for an attack than a remote attacker.
723 The specific rationale for this situation is given by the expected benefit of a successful attack. An attacker
724 who has to have physical access to the TOE that they are attacking, will only be able to compromise one
725 TOE at a time. So the effect of a successful attack will always be limited to the attacked TOE. A logical
726 attack from the WAN side on the other hand may have the potential to compromise a large amount of
727 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.

## 728 3.5 Organizational Security Policies (OSPs)

729 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.

730 # 4. Security Objectives

731 ## 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. [28]

[28] 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 [29],
- 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.

[29] 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. [30]

In addition the TOE shall generate the required keys utilising the services of its Security Module[31], ensure that the keys are only used for an acceptable amount of time and destroy ephemeral[32] 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) [33],
- make any physical manipulation within the scope of the intended environment detectable for the Consumer and Gateway Administrator.

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

[31] Please refer to chapter 1.5.10 for an overview on how the cryptographic functions are distributed between the TOE and its Security Module.

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

[33] 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[34] 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.

[34] 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.

**OE.Delivery** After the reception of the TOE by the MPO, the MPO is responsible for the secure delivery of the TOE to the installation and operational environment. The MPO shall be trustworthy in context of this delivery and well trained and shall take appropriate security measures to ensure protection against undetected manipulation or undetected replacement of the TOE during such a delivery to ensure integrity and authenticity of the TOE. Note that adhering to [MSB-Katalog] is sufficient for MPOs to fulfill this security objective.

## 733 4.3 Security Objectives rationale

### 734 4.3.1 Overview

735 The following table gives an overview how the assumptions, threats, and organisational security policies
736 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 | OE.Delivery |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **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 | |
| **A.Delivery** | | | | | | | | | | | | | | | | | | | X |

**Table 4.1: Rationale for Security Objectives**

### 4.3.2 Countering the threats

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

#### 4.3.2.1 General objectives

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

**O.Management** is indispensable as it defines the requirements around the management of the Security Functions. Without a secure management no TOE can be secure. Also **OE.TrustedAdmins** contributes to this aspect as it provides the requirements on the availability of a trustworthy 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.

#### 4.3.4.8 A.Delivery

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

# 5. Extended Component definition

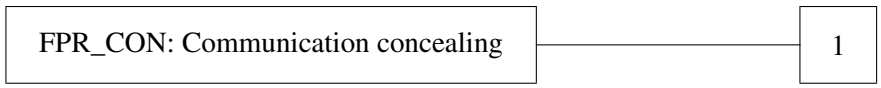
## 5.1 Communication concealing (FPR_CON)

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 6.1: 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<br>• Log all events as defined by Common Criteria for the used SFR<br>• Log all system relevant events on specific functionality<br>• Automated alarms in case of a cumulation of certain events<br>• Inform the Service Technician about the status of the Gateway | • Inform the Consumer about all information flows to the WAN<br>• Inform the Consumer about the Processing Profiles<br>• Inform the Consumer about other metering data (not billing-relevant)<br>• 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<br>• Augmented by specific events for the security functions | • Information about all information flows to the WAN<br>• Information about the current and the previous Processing Profiles<br>• Billing-relevant data needed to verify an invoice<br>• Non-billing-relevant Meter Data<br>• Information about the system status (including relevant errors)<br>• Billing-relevant data needed to verify an invoice | • Calibration relevant data only |

| | System-Log | Consumer-Log | Calibration-Log |
|---|---|---|---|
| **Access** | • Access by authorised Gateway Administrator and via IF_GW_WAN only<br>• Events may only be deleted by an authorised Gateway Administrator via IF_GW_WAN<br>• 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.<br>• The availability of data has to be ensured for a sufficient amount of time<br>• Overwriting old events is possible if the memory is full | • Ring buffer.<br>• The availability of data has to be ensured for a sufficient amount of time<br>• Overwriting old events is possible if the memory is full<br>• 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 6.2: 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 |

920 ### 6.2.2.2 Security audit data generation (FAU_GEN)

921 #### 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:<br>a) Start-up and shutdown of the audit functions;<br>b) All auditable events for the [basic] level of audit; and<br>c) [*other non-privacy relevant auditable events as listed in Table 6.3*]. |
| FAU_GEN.1.2/SYS | The TSF shall record within each audit record at least the following information:<br>a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and<br>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 6.4*]. |
| Hierarchical to: | No other components |
| Dependencies: | FPT_STM.1 |

| SFR | Auditable Event |
|---|---|
| FAU_ARP.1/SYS | Actions taken due to potential security violations. |
| FAU_GEN.1/SYS | - |
| FAU_GEN.1/CON | - |
| FAU_GEN.1/CAL | - |
| FAU_SAA.1/SYS | ~~**Enabling and disabling of any of the analysis mechanisms. Automated responses performed by the tool.**~~ [35] |
| 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.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. |
| FAU_GEN.2 | - |
| FAU_STG.2 | - |
| FCO_NRO.2 | The **failure of** invocation of the non-repudiation service.[36] Identification of the information, the destination, and a copy of the evidence provided. |

[35] It is not possible to disable the analysis mechanism. Automated responses are not foreseen.
[36] It is not possible to store every successful invocation of the non-repudiation service due to memory restrictions.

| SFR | Auditable Event |
|---|---|
| FCS_CKM.1/TLS | ~~**Success and**~~ failure of the activity. [37] The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys). |
| FCS_COP.1/TLS | ~~**Success and**~~ failure, and the type of cryptographic operation. [38] Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. |
| FCS_CKM.1/CMS | ~~**Success and**~~ Failure of the activity.[39] The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).[40] |
| FCS_COP.1/CMS | ~~**Success and**~~ failure, and the type of cryptographic operation. [41] Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. |
| 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_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_CKM.4 | ~~**Success and**~~ failure of the activity. [42] The object attribute(s)~~**, and object value(s)**~~ excluding any sensitive information (e.g. secret or private keys). [43] |
| FCS_COP.1/HASH | ~~**Success and**~~ failure, and the type of cryptographic operation. [44] 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.[45] 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_IFF.1/FW | All decisions on requests for information flow. |
| FDP_IFC.2/MTR | - |
| 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. |

[37] It is not possible to store every successful TLS key management activity due to memory restrictions.
[38] It is not possible to store every successful TLS activity due to memory restrictions.
[39] It is not possible to store every successful CMS key management activity due to memory restrictions.
[40] The attributes and values are fixed within this ST and not configurable. Therefore it is not necessary to log these attributes and values every time.
[41] It is not possible to store every successful CMS activity due to memory restrictions.
[42] It is not possible to store every successful Cryptographic key destruction activity due to memory restrictions.
[43] To prevent the disclosure of sensitive information, object values are not part of the logged items.
[44] It is not possible to store every successful HASH activity due to memory restrictions.
[45] Logging of failures in this context is not possible, because the target that holds the log entries is out of order.

| SFR | Auditable Event |
|---|---|
| FIA_ATD.1 | - |
| 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 (e.g. re-enabling of a terminal). |
| 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). |
| FMT_MOF.1 | All modifications in the behaviour of the functions in the TSF. |
| FMT_SMF.1 | Use of the management functions. |
| FMT_SMR.1 | Modifications to the group of users that are part of a role. |
| FMT_MSA.1/AC | All modifications of the values of security attributes. |
| FMT_MSA.3/AC | - [46] |
| FMT_MSA.1/FW | All modifications of the values of security attributes. |
| FMT_MSA.3/FW | - [47] |
| FMT_MSA.1/MTR | All modifications of the values of security attributes. |
| FMT_MSA.3/MTR | - [48] |
| FPR_CON.1 | - |
| FPR_PSE.1 | The subject/user that requested resolution of the user identity should be audited. |
| FPT_FLS.1 | Failure of the TSF. |
| 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. |
| FPT_PHP.1 | - [49] |
| FTP_ITC.1/WAN | All attempted uses of the trusted channel functions. Identification of the initiator and target of all trusted channel functions. |
| 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. |

**Table 6.3: Auditable Events for System Log**

[46] Initial values can not be changed (cf. FMT_MSA.3/AC)
[47] Initial values can not be changed (cf. FMT_MSA.3/FW)
[48] Initial values can not be changed (cf. FMT_MSA.3/MTR)
[49] Because the detection is performed by human person only, there is nothing to be logged by the TOE.

| Additional Information | Description |
|---|---|
| record_number | Unique log entry identifier. |
| datetime | Date and Time of the event using UTC. |
| event_type | Type of the recorded event. |
| subject_identity | Identity of the subject that causes the event. |
| outcome | Outcome of the performed action |

**Table 6.4: Information that shall be logged**

922 #### 6.2.2.3 Security audit analysis (FAU_SAA)

923 ##### 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:<br>a) Accumulation or combination of [<br>• *a defined number of blocking of IF_GW_CON*<br>• *a process restarted*<br>• *a defined number of incorrect wake-up calls received*<br>• *a defined number of detected telegram replay for each interface*<br>] known to indicate a potential security violation;<br>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. |

924 #### 6.2.2.4 Security audit review (FAU_SAR)

925 ##### 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 |

926 #### 6.2.2.5 Security audit event storage (FAU_STG)

927 ##### 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. |

928 ### 6.2.3 Security Requirements for the Consumer Log

929 #### 6.2.3.1 Security audit data generation (FAU_GEN)

930 ##### 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:<br>a) Start-up and shutdown of the audit functions;<br>b) All auditable events for the [not specified] level of audit; and<br>c) [*all audit events as listed in Table 6.5 and [none]*]. |
| FAU_GEN.1.2/CON | The TSF shall record within each audit record at least the following information:<br>a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and<br>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 6.5 and [Table 6.4]*]. |
| 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<br>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 | - |
| Adding or removing of meters located in the LMN and attached to the respective Consumer | - |
| Changing of authentication information | - |

**Table 6.5: Events for Consumer Log**

931 #### 6.2.3.2 Security audit review (FAU_SAR)

932 ##### 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. |

933 #### 6.2.3.3 Security audit event storage (FAU_STG)

934 ##### 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. |

935 ### 6.2.4 Security Requirements for the Calibration Log

936 #### 6.2.4.1 Security audit data generation (FAU_GEN)

937 ##### 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:<br>a) Start-up and shutdown of the audit functions;<br>b) All auditable events for the [not specified] level of audit; and<br>c) [*all audit events as listed in Table 6.6*]. |
| FAU_GEN.1.2/CAL | The TSF shall record within each audit record at least the following information:<br>a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and<br>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 6.6 and Table 6.4*]. |
| Hierarchical to: | No other components |
| Dependencies: | FPT_STM.1 |
| **Application Note 8:** | The Calibration Log serves to fulfill national requirements in the context of the calibration of the TOE. |

| Event | Additional Information |
|---|---|
| Start of operation of the SMGW | - |
| Adding or removing of meters located in the LMN and attached to a Consumer of the gateway | - |
| Any change to a Processing Profile | - |
| Soft- and Firmwareupdates | - |
| Deviation (more than 3% of the shortest measuring period) between the local time and the reliable timesource provided by the Gateway Administrator. | - |
| Successful synchronisation of the local time using the reliable time source provided by the Gateway Administrator. | - |
| Meter Error | Information provided by the Meter |

**Table 6.6: Events for Calibration Log**

938 #### 6.2.4.2 Security audit review (FAU_SAR)

939 ##### 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 |

940 #### 6.2.4.3 Security audit event storage (FAU_STG)

941 ##### 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 losss |
| 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. |

942 ### 6.2.5 Security Requirements that apply to all logs

943 #### 6.2.5.1 Security audit data generation (FAU_GEN)

944 ##### 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<br>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. |

945 #### 6.2.5.2 Security audit event storage (FAU_STG)

946 ##### 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 records from the Calibration Log and a sufficient, adjustable number of days within a predefined range of days for the System Log and for each Consumer Log of* ] 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. |

947 ## 6.3 Class FCO: Communication

948 ### 6.3.1 Non-repudiation of origin (FCO_NRO)

949 #### 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*[50]] 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.<br>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. |

950 # 6.4 Class FCS: Cryptographic Support

951 ## 6.4.1 Cryptographic support for TLS

952 ### 6.4.1.1 Cryptographic key management (FCS_CKM)

953 #### 6.4.1.1.1 FCS_CKM.1/TLS: Cryptographic key generation for TLS

| | |
|---|---|
| FCS_CKM.1.1/TLS | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*TLS PRF within algorithms defined in FCS_COP.1/TLS, using elliptic curves NIST P-256 (secp256r1), NIST P-384 (secp384r1), BrainpoolP256r1, BrainpoolP384r1 and BrainpoolP512r1*] and specified cryptographic key sizes [AES: *128 bit, 256 bit*, ECC: *256 bit, 384 bit, 512 bit*] that meet the following: [*[RFC 5289], [RFC 5246], [FIPS 180-4], [RFC 2104]*]. |
| Hierarchical to: | No other components |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution, or<br>FCS_COP.1 Cryptographic operation], fulfilled by FCS_COP.1/TLS<br>FCS_CKM.4 Cryptographic key destruction |
| **Application Note 13:** | The Security Module is used for parts of the TLS key negotiation. In particular, the key generation for TLS is performed by the Security Module. The TOE only implements the pseudorandom function (PRF) in accordance to the used cipher suites to generate the key from the master secret. |

954 ### 6.4.1.2 Cryptographic operation (FCS_COP)

955 #### 6.4.1.2.1 FCS_COP.1/TLS: Cryptographic operation for TLS

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

| | |
|---|---|
| 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, using elliptic curves NIST P-256 (secp256r1), NIST P-384 (secp384r1), BrainpoolP256r1, BrainpoolP384r1 and BrainpoolP512r1*] and cryptographic key sizes [*128 bit, 256 bit*] that meet the following: [*[RFC 5289], [RFC 5246], [RFC 2104], [NIST SP800-38A], [NIST SP800-38D], [FIPS 180-4], [FIPS 197]*]. |
| 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<br>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*] and specified cryptographic key sizes [*128bit*] that meet the following: [*[TR 03111]*]. |
| Hierarchical to: | No other components |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], fulfilled by FCS_COP.1/CMS<br>FCS_CKM.4 Cryptographic key destruction |
| **Application Note 14:** | 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-aes-CBC-CMAC-128*] and cryptographic key sizes [*128bit*] that meet the following: [*[RFC 4493], [RFC 5084], [FIPS 197], [NIST SP800-38A], [NIST SP800-38D]*]. |
| 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<br>FCS_CKM.4 Cryptographic key destruction |

961 ### 6.4.3 Cryptographic support for Meter communication encryption

962 #### 6.4.3.1 Cryptographic key management (FCS_CKM)

963 ##### 6.4.3.1.1 FCS_CKM.1/MTR: Cryptographic key generation for Meter communication (symmetric
964 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: [*[RFC 4493], [FIPS 197]*]. |
| 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 |

965 #### 6.4.3.2 Cryptographic operation (FCS_COP)

966 ##### 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 for encryption and decryption and AES-CMAC for integrity protection*] and cryptographic key sizes [*128bit*] that meet the following: [*[RFC 4493], [FIPS 197], [NIST SP800-38A]*]. |
| 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 15:** 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 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 16:** 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.

967 ### 6.4.4 General Cryptographic support

968 #### 6.4.4.1 Cryptographic key management (FCS_CKM)

969 ##### 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]*]. |
| 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 17:** | 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. |

970 #### 6.4.4.2 Cryptographic operation (FCS_COP)

971 ##### 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[51] ] FCS_CKM.4 Cryptographic key destruction |
| **Application Note 18:** | 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. |

972 ##### 6.4.4.2.2 FCS_COP.1/MEM: Cryptographic operation, encryption of TSF and user data

| | |
|---|---|
| FCS_COP.1.1/MEM | The TSF shall perform [*TSF and user data encryption*] in accordance with a specified cryptographic algorithm [*AES-128-CBC ESSIV:SHA256*] and cryptographic key sizes [*128bit*] that meet the following: [*[FIPS 197],[NIST SP800-38A],[FIPS 180-4]*]. |
| Hierarchical to: | No other components |

[51] 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<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation[51]]<br>FCS_CKM.4 Cryptographic key destruction |

**Application Note 19:** Please note that the random number generation mechanism of the Security Module is used for key generation.

**Application Note 20:** 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 [<br>*subjects: external entities in WAN, HAN and LMN*<br>*objects: any information that is sent to, from or via the TOE and any information that is stored in the TOE*] and all operations among subjects and objects covered by the SFP. |
| FDP_ACC.2.2 | The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP. |
| Hierarchical to: | FDP_ACC.1 Subset access control |
| Dependencies: | FDP_ACF.1 Security attribute based access control |

##### 6.5.2.1.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [*Gateway access SFP*] to objects based on the following: [
*subjects: external entities on the WAN, HAN or LMN side*
*objects: any information that is sent to, from or via the TOE*
*attributes: destination interface*].

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

- *an authorised Consumer is only allowed to have read access to his own User Data via the interface IF_GW_CON,*
- *an authorised Service Technician is only allowed to have read access to the System Log via the interface IF_GW_SRV, the Service Technician must not be allowed to read, modify or delete any other TSF data,*
- *an authorised Gateway Administrator is allowed to interact with the TOE only via IF_GW_WAN,*
- *only authorised Gateway Administrators are allowed to establish a wake-up call,*
- *[Meter Data shall be transmitted only via the interface IF_GW_MTR to the Gateway]*].

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

990 ### 6.5.3 Firewall SFP

991 #### 6.5.3.1 Information flow control policy (FDP_IFC)

992 ##### 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: [<br>*subjects: The TOE and external entities on the WAN, HAN or LMN side*<br>*information: any information that is sent to, from or via the TOE*<br>*attributes: destination_interface (TOE, LMN, HAN or WAN), source_interface (TOE, LMN, HAN or WAN), destination_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: [<br>*(if source_interface=HAN or source_interface=TOE) and*<br>*destination_interface=WAN and*<br>*destination_authenticated = true*<br>*Connection establishment is allowed*<br>*[(if source_interface=HAN or source_interface=LMN) and*<br>*destination_interface=TOE and*<br>*source_authentication=true*<br>*Connection establishment is allowed*<br>*if source_interface=TOE and*<br>*(destination_interface=LMN or destination_interface=HAN) and*<br>*destination_authenticated = true*<br>*Connection establishment is allowed*<br>*]*<br>*else*<br>*Connection establishment is denied*<br>]. |
| 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<br>FMT_MSA.3 Static attribute initialisation |
| **Application Note 21:** | 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 |

998 #### 6.5.4.2 Information flow control functions (FDP_IFF)

999 ##### 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: [<br>*subjects: TOE, external entities in WAN, Meters located in LMN*<br>*information: any information that is sent via the TOE*<br>*attributes: destination interface, source interface (LMN or WAN), Processing Profile*<br>]. |
| 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: [<br>• *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:*<br>• *Data received from Meters shall be processed as defined in the corresponding Processing Profile,*<br>• *Results of processing of Meter Data shall be submitted to external entities as defined in the Processing Profiles,*<br>• *The internal system time shall be synchronised as follows:*<br>▪ *The TOE shall compare the system time to a reliable external time source [according to [RFC 5905] within a synchronization interval between 1 minute and 11.6 hours (41653 seconds)].*<br>▪ *If the deviation between the local time and the remote time is acceptable*[52] *the local system time shall be updated according to the remote time.*<br>▪ *If the deviation is not acceptable the TOE*<br>• *shall ensure that any following Meter Data is not used,*<br>• *stop operation*[53] *and*<br>• *inform a Gateway Administrator*]. |
| FDP_IFF.1.4/MTR | The TSF shall explicitly authorise an information flow based on the following rules: [*none*]. |

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

[53] 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.

| | |
|---|---|
| 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<br>FMT_MSA.3 Static attribute initialisation |

**Application Note 22:** 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 reliability of the external source the TOE synchronises the local time only with a time source provided by the Gateway Administrator. After a power cut the TOE can use the integrated Real Time Clock (RTC) for the first adjustment of the local time.

**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 23:** 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.

1000 ### 6.5.5 General Requirements on user data protection

1001 #### 6.5.5.1 Residual information protection (FDP_RIP)

1002 ##### 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 24:** 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.

1003 #### 6.5.5.2 Stored data integrity (FDP_SDI)

1004 ##### 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: [*hash value and valid signature, if expected*]. |
| FDP_SDI.2.2 | Upon detection of a data integrity error, the TSF shall [*always inform the Gateway Administrator*]. |
| Hierarchical to: | FDP_SDI.1 Stored data integrity monitoring |
| Dependencies: | No dependencies. |

**Application Note 25:** This Security Target defines that the TOE shall be capable of detecting integrity errors on all objects.

1005 ## 6.6 Class FIA: Identification and Authentication

1006 ### 6.6.1 User Attribute Definition (FIA_ATD)

1007 #### 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. |

1008 ### 6.6.2 Authentication Failures (FIA_AFL)

1009 #### 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 [*block the interface IF_GW_CON for 5 minutes and create a System Log entry*]. |
| 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 26:** | 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 [<br>• *authentication via certificates at the IF_GW_MTR interface,*<br>• *TLS-authentication via certificates at the IF_GW_WAN interface,*<br>• *TLS-authentication via HAN-certificates at the IF_GW_CON interface,*<br>• *authentication via password at the IF_GW_CON interface,*<br>• *TLS-authentication via HAN-certificates at the IF_GW_SRV interface,*<br>• *authentication **via HAN-certificates** at the IF_GW_CLS interface,*<br>• *verification via a commands' signature*<br>] to support user authentication. |
| FIA_UAU.5.2 | The TSF shall authenticate any user's claimed identity according to the [<br>• *meters shall be authenticated via certificates at the IF_GW_MTR interface only,*<br>• *Gateway administrators shall be authenticated via TLS-certificates at the IF_GW_WAN interface only,*<br>• *Consumers shall be authenticated via TLS-certificates or via password at the IF_GW_CON interface only,*<br>• *Service Technicians shall be authenticated via TLS-certificates at the IF_GW_SRV interface only,*<br>• *CLS shall be authenticated at the IF_GW_CLS only,*<br>• *each command of an Gateway Administrator shall be authenticated by verification of the commands' signature,*<br>• *other external entities shall be authenticated via TLS-certificates at the IF_GW_WAN interface only*<br>]. |

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| **Application Note 27:** | 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 **an external entity** under the conditions [<br>- *TLS channel to the WAN shall be disconnected after 48 hours,*<br>- *TLS channel to the LMN shall be disconnected after 5 MB of transmitted information,*<br>- *Other local users shall be re-authenticated after 10 minutes of inactivity,*<br>]. |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| **Application Note 28:** | 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 29:** | The term "other local users" refers to the roles "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: [

- *set 'User Identity' to configured value*
- *set 'Status of Identity' to not authenticated*
- *set 'Connecting network' to configured selection (WAN, HAN or LMN)*
- *set 'Role membership' to configured selection*

].

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

- *security attribute 'User Identity' is not changeable.*
- *security attribute 'Status of Identity' is changeable.*
- *security attribute 'Connecting network' is not changeable.*
- *security attribute 'Role membership' is not changeable.*

].

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 6.7*].

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<br><br>Display the current time | The management functions must only be accessible for an authorised Consumer and only via the interface IF_GW_CON. **An authorized Service Technician is also able to access the software version number and the current time of the TOE via the interface IF_GW_SRV.** [54] |
| 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[55] |
| 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 6.7: Restrictions on Management Functions**

1022 ### 6.7.1.2 Specification of Management Functions (FMT_SMF)

1023 #### 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 6.8 and Table 6.9 and [none]*].

Hierarchical to: No other components.

Dependencies: No dependencies.

| SFR | Management functionality |
|---|---|
| FAU_ARP.1/SYS | • ~~**The management (addition, removal, or modification) of actions.**~~ [56] |
| FAU_GEN.1/SYS<br>FAU_GEN.1/CON<br>FAU_GEN.1/CAL | - |
| FAU_SAA.1/SYS | • ~~**Maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.**~~ [57] |

[54] The authorized Service Technician must be able to read the software version number and the current time of the TOE via the interface IF_GW_SRV because he has to ensure that the TOE is running correctly the certified firmware.

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

[56] As the actions taken due to potential security violations are fixed within this ST the management functions as defined by Common Criteria part 2 do not apply.

[57] As the rules defined by the Gateway Administrator may be potentially weak, the rules are set fixed by the firmware of the

| SFR | Management functionality |
|---|---|
| FAU_SAR.1/SYS<br>FAU_SAR.1/CON<br>FAU_SAR.1/CAL | -[58] |
| FAU_STG.4/SYS<br>FAU_STG.4/CON | • ~~**Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.**~~[59]<br>• Size configuration of the audit trail that is available before the oldest events get overwritten. |
| FAU_STG.4/CAL | - [60] |
| FAU_GEN.2 | - |
| FAU_STG.2 | • ~~**Maintenance of the parameters that control the audit storage capability for the Consumer Log and the System Log.**~~[61] |
| FCO_NRO.2 | • The management of changes to ~~**information types, fields, originator attributes and recipients**~~ **key material** of evidence.[62] |
| 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 | - |

TOE based upon the security knowledge of the manufacturer. Therefore the management functions as defined in part 2 of Common Criteria do not apply.

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

[59] As the actions to be taken in case of audit storage failure are fixed within this ST not all management functions as defined by Common Criteria part 2 do apply.

[60] 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.

[61] As the parameters that control the audit storage capability are fixed within this ST the management function as defined by Common Criteria part 2 do not apply.

[62] As there exist no standard method for the management of changes to information types, fields, originator attributes and recipients these parameters cannot be changed by the Gateway Administrator. Only the key material used for signature generation can be changed by the Gateway Administrator using a management function.

| SFR | Management functionality |
|---|---|
| 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**~~[63] |
| FDP_ACC.2 | - |
| FDP_ACF.1 | - |
| FDP_IFC.2/FW | - |
| FDP_IFF.1/FW | • Managing the attributes used to make explicit access based decisions.<br>• Add authorised units for communication (pairing).<br>• Management of endpoint to be contacted after successful wake-up call.<br>• 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.**~~[64] |
| FIA_ATD.1 | • ~~**If so indicated in the assignment, the authorised Gateway Administrator might be able to define additional security attributes for users.**~~[65] |

[63] As the key material is created within the production process and brought securely into the Security Module the management functions as defined by Common Criteria part 2 do not apply.

[64] As the actions to be taken upon the detection of an integrity error are fixed within this ST the management functions as defined by Common Criteria part 2 do not apply.

[65] As it is not possible for the Gateway Administrator to define additional security attributes for users the management functions as defined by Common Criteria part 2 do not apply.

| SFR | Management functionality |
|---|---|
| FIA_AFL.1 | • Management of the threshold for unsuccessful authentication attempts;<br>• ~~**Management of actions to be taken in the event of an authentication failure.**~~[66] |
| FIA_UAU.2 | • Management of the authentication data by an Gateway Administrator; |
| FIA_UAU.5 | - [67] |
| FIA_UAU.6 | - [67] |
| FIA_UID.2 | • The management of the user identities. |
| FIA_USB.1 | • ~~**An authorised Gateway Administrator can define default subject security attributes, if so indicated in the assignment of FIA_ATD.1.**~~<br>• ~~**An authorised Gateway Administrator can change subject security attributes, if so indicated in the assignment of FIA_ATD.1.**~~ [68] |
| FMT_MOF.1 | • ~~**Managing the group of roles that can interact with the functions in the TSF.**~~ [69] |
| 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.**~~[70] |
| FMT_MSA.3/AC | - [71] |

[66] As the actions that shall be performed if the threshold of unsuccessful authentication attempts is reached are fixed within this ST not all management functions as defined by Common Criteria part 2 do apply.

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

[68] As it is not possible for the Gateway Administrator to define default subject security attributes or to change subject security attributes the management functions as defined by Common Criteria part 2 do not apply.

[69] As the TOE only supports subject security attributes based on roles and users the management functions as defined by Common Criteria part 2 do not apply.

[70] 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.

| SFR | Management functionality |
|---|---|
| FMT_MSA.1/FW | • ~~**Management of rules by which security attributes inherit specified values.**~~[72] |
| FMT_MSA.3/FW | - [71] |
| FMT_MSA.1/MTR | • ~~**Management of rules by which security attributes inherit specified values.**~~[72] |
| FMT_MSA.3/MTR | - [71] |
| FPR_CON.1 | • Definition of the interval in FPR_CON.1.2 if definable within the operational phase of the TOE. |
| FPR_PSE.1 | - |
| FPT_FLS.1 | - |
| FPT_RPL.1 | - |
| FPT_STM.1 | • Management of a time source. |
| FPT_TST.1 | - [73] |
| FPT_PHP.1 | • Management of the user or role that determines whether physical tampering has occurred.[74] |
| FTP_ITC.1/WAN | - [75] |
| FTP_ITC.1/MTR | - [75] |
| FTP_ITC.1/USR | - [75] |

**Table 6.8: SFR related Management Functionalities**

[71] 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.

[72] 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.

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

[74] This management function will be fulfilled by descriptions in the corresponding guidance documentation.

[75] 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.

| Gateway specific Management Functionalities |
|---|
| Pairing of a Meter[76] |
| Performing a firmware update[76] |
| Management of certificates of external entities in the WAN for communication[76] |
| Displaying the current version number of the TOE |
| Displaying the current time |
| Resetting of the TOE[77]. [78] |

**Table 6.9: 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 [<br>*authorised Consumer,*<br>*authorised Gateway Administrator,*<br>*authorised Service Technician,*<br>*[authorised External Entity]*]. |
| FMT_SMR.1.2 | The TSF shall be able to associate users with roles. |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |

## 6.7.3 Management of security attributes for Gateway access SFP

### 6.7.3.1 Management of security attributes (FMT_MSA)

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

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

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

[76] This management function will be executed by installing a new processing profile

[77] 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**~~

[78] The definition of "resetting the TOE" in this ST is to issue a controlled restart of the TOE. This can be done by request of the authorized Gateway Administrator only. This function has no impact on stored data or the TOE configuration.

| | |
|---|---|
| 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<br>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<br>FDP_IFC.1 Subset information flow control], fulfilled by FDP_IFC.2/FW<br>FMT_SMR.1 Security roles<br>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<br>FMT_SMR.1 Security roles |
| **Application Note 30:** | 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<br>FDP_IFC.1 Subset information flow control], fulfilled by FDP_IFC.2/FW<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |

1037 #### 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<br>FMT_SMR.1 Security roles |

1038 ## 6.8 Class FPR: Privacy

1039 ### 6.8.1 Communication Concealing (FPR_CON)

1040 #### 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 [*frequency how often are Meter Data send to authorized External Entities, the size and the load of the transmitted Meter Data*]. |
| FPR_CON.1.2 | The TSF shall connect to [*authorized External Entities as defined within the Processing Profiles*] in intervals as ~~**follows**~~ [*defined within the Processing Profiles but at least daily*] to conceal the data flow. |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |

1041 ### 6.8.2 Pseudonymity (FPR_PSE)

1042 #### 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 [*alias given by the Gateway Administrator in the Processing Profile*]. |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |

**Application Note 31:** 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.

1043 # 6.9 Class FPT: Protection of the TSF

1044 ## 6.9.1 Fail secure (FPT_FLS)

1045 ### 6.9.1.1 FPT_FLS.1: Failure with preservation of secure state

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

- *the deviation between local system time of the TOE and the reliable external time source is too large,*
- *the deviation between the local time and the reliable time source exceeds 3% of the shortest measuring period supported by the TOE and allowed for billing by the national calibration authority,*
- *the memory consumption of log storage has reached a critical limit,*
- *the memory consumption of metering data storage has reached a critical limit,*
- *the HAN interface is connected to the WAN (HAN-WAN interfaces are not separate or interchanged),*
- *a critical and non-correctable error occurred in the boot process,*

].

Hierarchical to: No other components.

Dependencies: No dependencies.

1046 ## 6.9.2 Replay Detection (FPT_RPL)

1047 ### 6.9.2.1 FPT_RPL.1: Replay detection

[78] These IDs are a placeholder for all possibly personally identifiable information (PII) contained in the Meter Data send to an Authorised External Identity.

| | |
|---|---|
| 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 32:** | 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. 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). Therefore the local clock shall be as exact as required by normative or legislative regulations.<br>A maximum deviation of 3% of the measuring period is allowed to be in conformance with [SMGW-PP]. |

### 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. |

# 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 33:** | 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 |
| | ASE_REQ.2 |
| | ASE_SPD.1 |
| | ASE_TSS.1 |
| Tests | ATE_COV.2 |
| | ATE_DPT.1 |
| | ATE_FUN.1 |
| | ATE_IND.2 |
| Vulnerability Assessment | AVA_VAN.5 |

**Table 6.10: Assurance Requirements**

### 6.11.1 Refinement for ALC_DEL.1 for the following assurance elements

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

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

**Application Note 34:**

"MPO" as the recipient of the TOE delivery is to be understood to also include service technicians or any other agent who act as a contractor on behalf of the MPO.

# 6.12 Security Requirements rationale

## 6.12.1 Security Functional Requirements rationale

### 6.12.1.1 Fulfillment of the Security Objectives

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

| | O.Firewall | O.SeparateIF | O.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 | |
| **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 6.11: Fulfillment of Security Objectives**

The following paragraphs contain more details on this mapping.

#### 6.12.1.1.1 O.Firewall

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

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

#### 6.12.1.1.2 O.SeparateIF

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

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

#### 6.12.1.1.3 O.Conceal

O.Conceal is completely met by **FPR_CON.1** as it defines rules to protect PII from disclosure by analysing the size, load or frequency of transmitted Meter Data.

#### 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 Fulfillment 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 |

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

| SFR | Dependencies | Fulfilled by |
|---|---|---|
| FCS_COP.1/HASH | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction | FCS_CKM.4<br>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<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction | FCS_CKM.4<br>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<br>FMT_MSA.3 Static attribute initialisation | FDP_ACC.2<br>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<br>FMT_MSA.3 Static attribute initialisation | FDP_IFC.2/FW<br>FMT_MSA.3/FW |
| FDP_IFC.2/MTR | FDP_IFF.1 Simple security attributes | FDP_IFF.1/MTR |
| FDP_IFF.1/MTR | FDP_IFC.1 Subset information flow control<br>FMT_MSA.3 Static attribute initialisation | FDP_IFC.2/MTR<br>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<br>FMT_SMF.1 Specification of Management Functions | FMT_SMR1<br>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<br>FDP_IFC.1 Subset information flow control]<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions | FDP_ACC.2<br>FMT_SMR.1<br>FMT_SMF.1 |

| SFR | Dependencies | Fulfilled by |
|---|---|---|
| FMT_MSA.3/AC | FMT_MSA.1 Management of security attributes<br>FMT_SMR.1 Security roles | FMT_MSA.1/AC<br>FMT_SMR.1 |
| FMT_MSA.1/FW | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions | FDP_IFC.2/FW<br>FMT_SMR.1<br>FMT_SMF.1 |
| FMT_MSA.3/FW | FMT_MSA.1 Management of security attributes<br>FMT_SMR.1 Security roles | FMT_MSA.1/FW<br>FMT_SMR.1 |
| FMT_MSA.1/MTR | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions | FDP_IFC.2/MTR<br>FMT_SMR.1<br>FMT_SMF.1 |
| FMT_MSA.3/MTR | FMT_MSA.1 Management of security attributes<br>FMT_SMR.1 Security roles | FMT_MSA.1/MTR<br>FMT_SMR.1 |
| FPR_CON.1 | - | - |
| FPR_PSE.1 | - | - |
| FPT_FLS.1 | - | - |
| FPT_RPL.1 | - | - |
| FPT_STM.1 | - | - |
| FPT_TST.1 | - | - |
| FPT_PHP.1 | - | - |
| FTP_ITC.1/WAN | - | - |
| FTP_ITC.1/MTR | - | - |
| FTP_ITC.1/USR | - | - |

**Table 6.12: SFR Dependencies**

#### 6.12.1.3 Justification for missing dependencies

The hash algorithm as defined in FCS_COP.1/HASH does not need any key material. As such the dependency to an import or generation of key material is omitted for this SFR.
The key material as defined in FCS_COP.1/MEM will be generated and stored into the security module while the integration phase of production of the TOE. There is no dependency to SFR FCS_CKM.1/CMS.

### 6.12.2 Security Assurance Requirements rationale

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

- 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 Smart Meter Gateway. Therefor the TOE records within this log all system relevant events as listed in Table 6.3 (**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**). The TOE detects a potential security violation, if at least one of the following events occur:

- a defined number of blocking of IF_GW_CON
- a process restarted
- a defined number of incorrect wake-up calls received
- a defined number of detected telegram replay for each interface

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**). Therefor a TLS channel between the Gateway and the Gateway Administrator must be in place. The TOE sends a web service request containing CMS-data to the Gateway Administrator. The Gateway Administrator processes the request and if the operation was performed successfully, sends web service request-code OK (including CMS-data, if applicable) to the Gateway. Otherwise the Gateway Administrator sends a web service response that contains the corresponding error code and if applicable CMS-data to the Gateway. To transmit the web service requests and responses the TOE uses HTTP/1.1 in accordance to [RFC 2616].
The TOE ensures that a sufficient amount of storage space is available for the System Log. The time based storage depth (commissioning time) of the audit trail can be configured by the Gateway Administrator using IF_GW_WAN (cf. section 7.5) within a predefined range of days. This range ensures that a minimum of 31 days (one month) of logged entries is always available (**FAU_STG.2**). If the difference of the timestamps of stored log entries exceeds the configured commissioning time the TOE deletes the outdated log entries.
The TOE informs the Gateway Administrator and creates a log entry within the System Log after every elapsed commissioning time interval (**FAU_STG.4/SYS**).
If the audit storage space used for the System Log exceeds a predefined logical limit the TOE informs the Gateway Administrator and creates a log entry within the System Log.

Please note that nobody is able to delete or modify the events that are recorded within the System Log (**FAU_STG.2**).

The **Consumer Log** informs authorized Consumers about all information flows to the WAN, available Processing Profiles, billing relevant and other Meter Data. Therefor the TOE tracks all events as listed in Table 6.5 (**FAU_GEN.1.1/CON**). Only authorized Consumer via IF_GW_CON have the possibility to read all information from the Consumer Log related to them (**FAU_SAR.1/CON**). Especially even the Gateway Administrator is not allowed to read the Consumer Log (**FDP_ACF.1.4**). To provide the information to authorized Consumers the TOE serves static HTML webpages to a client in the HAN network.
The TOE ensures that a sufficient amount of storage space is available for the Consumer Log. The time based storage depth (commissioning time) of the audit trail can be configured by the Gateway Administrator using IF_GW_WAN (cf. section 7.5) within a predefined range of days. This range ensures that a minimum of 465 days (15 months x 31 days) of logged entries is always available (**FAU_STG.2**).
If the difference of the timestamps of stored log entries exceeds the configured commissioning time the TOE deletes the outdated log data. The TOE informs the Gateway Administrator and creates a log entry within the corresponding Consumer Log after every elapsed commissioning time interval (**FAU_STG.4/CON**).
If the audit storage space used for the Consumer Log exceeds a predefined logical limit the TOE informs the Gateway Administrator and creates a log entry within the System Log.
Please note that nobody is able to delete or modify the events that are recorded within the Consumer Log (**FAU_STG.2**).

Within the **Calibration Log** only calibration relevant information as listed in Table 6.6 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**). If the audit storage space used for the Calibration Log exceeds a predefined logical limit the TOE informs the Gateway Administrator and creates a log entry within the System Log. In case the storage space used for all logs is full, the TOE stops operation and enters a secure state (**FAU_STG.4/CAL**).
To ensure that the auditable events listed above are available over the lifetime of the TOE, the storage space reserved for the Calibration Log will be sufficient for at least 8 years of operation. The calculation of the storage space is based on an assumption of expected events per day.
Within all logs each log entry contains the information as listed in Table 6.4 (**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 allows only 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 [RFC 5289], [RFC 5246], [RFC 2104], [NIST SP800-38A], [NIST SP800-38D], [FIPS 180-4] and [FIPS 197], 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 does only implement a pseudorandom function (PRF) in accordance to [RFC 5289] and [RFC 5246] 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 and are implemented according [FIPS 180-4] and [RFC 2104]. As elliptical curves the TOE supports the following:

- NIST P-256 (secp256r1) in accordance to [RFC 5114],
- NIST P-384 (secp384r1) in accordance to [RFC 5114],
- 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 an 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 algorithm (**FCS_COP.1/MTR**):

- AES-CBC with 128 bit key for encryption and decryption in accordance to [FIPS 197] and [NIST SP800-38A]
- AES-CMAC with 128 bit key for integrity protection in accordance to [RFC 4493]

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 [FIPS 197] and [RFC 4493] (**FCS_CKM.1/MTR**).
Please note that a symmetric cryptographic communication protection between Meters and TOE will only be established in two cases:

- A wireless, unidirectional connection between the Meter and the TOE is in place.
- For the first messages of the pairing process (SYM messages) between a wired connected Meter and the TOE.

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 are transferred from the Gateway via a third party, e.g. Gateway Administrator, the content data is always encrypted, MAC-protected and signed for the corresponding external entity. 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 [FIPS 197], [RFC 5084], [NIST SP800-38D],

- id-aes-CBC-CMAC-128 in accordance to [FIPS 197], [RFC 4493], [NIST SP800-38A],

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,

The key needed to perform the key encryption using the algorithms above is derived by the TOE using ECKA-EG with X9.63 Key Derivation Function according to [TR 03111] (**FCS_CKM.1/CMS**). Therefor the TOE uses the hash function SHA-256 (**FCS_COP.1/HASH**) according to [FIPS 180-4].
To provide the authorized External Entity with the capability to verify the origin of the received Meter Data the Gateway signs the encrypted and MAC-protected data using ECDSA in accordance to [TR 03111] with the hash function SHA-256 and the curve BrainpoolP256r1 according to [RFC 5114] (**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 AES-CBC according to [FIPS 197] and [NIST SP800-38A] with a 128 bit key (**FCS_COP.1/MEM**). This key is generated using the random number generation mechanism of the Security Module. It is protected and stored permanently inside the Security Module.
All ephemeral cryptographic keys used for TLS or symmetric AES encryption are destroyed using the method “zeroization” in accordance to [FIPS 140-2]. Therefor 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 and the Security Module are the only places where ephemeral cryptographic keys are stored (**FCS_CKM.4**).
The keys used for symmetric cryptography used for Meter communication that are stored permanently within the SMGW are protected against back-reading. Hence it is ensured that nobody is able to read the symmetric keys used for encryption (**FDP_ACF.1.4**).

## 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. Therefor 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.

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 as two different interfaces. One wired UART interfaces to the wM-Bus wireless module. On this interface the application protocol M-Bus EN 13757-3 according to [DIN EN 13757-3] and a proprietary configuration protocol is used. The wM-Bus wireless module is not part of the TOE. The wireless interface at the output side of this module is implemented as a wM-Bus interface in accordance to [DIN EN 13757-4].

The second wired interface is implemented as an TIA-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] 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 described 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 are 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 uses only 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. 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 modeling is performed via COSEM Interface-classes according to [IEC 62056-6-2] and OBIS Codes in accordance to [IEC 62056-6-1] and [DIN EN 13757-1]. The connection is protected via TLS 1.2 as described in section 7.2.

**Firewall SFP**

The Firewall SFP requires 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. 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 checks as defined in [TR 03109-1, Chapter 3.2.5.4] whether the packet is trustworthy.

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 enforces 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 hash value (SHA-256 (**FCS_COP.1/HASH**)) and the signature, if applicable. Thereby the signature is verified using the services of the Security Module. Upon the detection of a data integrity error, the TOE always informs the Gateway Administrator (**FDP_SDI.2**).
Further this TSF ensures that no residual information can be accessed by an attacker since the TOE frees allocated resources 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**). Therefor 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:

- the attribute role membership shall correspond to only one of the following values (**FMT_SMR.1**):
  - authorized Consumer,
  - authorized Gateway Administrator,
  - authorized Service Technician,
  - authorized External Entity,
- 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,

Within the initial association of the security attributes the status of identity is set to "not authenticated" (**FIA_USB.1**).

Further the TOE prevents that more than one user of the role Gateway Administrator becomes active. Two active Gateway Administrators are allowed temporary only for switching from one Gateway Administrator to another. The maximum time interval allowed for this process are 14 days.
The connection network may only be set to a value from a combination as defined in FDP_ACF.1 depending on the role membership of the user of the connection.
According to the attribute role membership the TOE determines the authentication mechanism that shall be used. Therefor 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 corresponds to the Smart Metering Public Key Infrastructure according to [TR 03109-4]. In addition each Wake-Up command from a 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.

Depending on the configuration by the Gateway Administrator it is allowed for Consumers at the IF_GW_CON interface to authenticate via certificates or via username and password. In 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. In case of Consumer authentication via username and password the required information is transmitted to the TOE via HTTP-Digest-Access-Authentication (**FIA_UAU.5**).

For the authentication mechanism via username and password the Gateway Administrator must set the threshold for unsuccessful authentication attempts[79]. Thereby the threshold shall correspond to an integer between 3 and 10 unsuccessful authentication attempts. The default value is set to 5. If the defined number of unsuccessful authentication attempts is met, the TSF blocks IF_GW_CON for 5 minutes and creates a System Log entry [80](**FIA_AFL.1**). After a successful authentication of a Consumer at IF_GW_CON the counter of unsuccessful authentication attempts 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 match them to corresponding Consumers (**FMT_SMR.1**).

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

- 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, 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 and authorized External Entities.

- Firmware Update
  The TOE provides only the authorized Gateway Administrator with the capability to insert, verify and activate new firmware. The TOE supports only one kind of update.

  – Full update
    Within a full update the TOE updates all updateable software parts.

  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**). After a necessary reboot the TOE starts the activated new firmware.

- 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 successful wake-up call.

- 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.

- Restarting the TOE
  The TOE allows only the authorized Gateway Administrator to trigger a restart of the TOE. This function is not something like a factory reset and has no impact on stored data or the TOE configuration.

- 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. Thereby it is ensured that the storage space does not deceeds a defined minimum number of logged days for each of those logs.

  If the audit trails contain the defined numbers of logged days, the TOE starts to overwrite the oldest log entries.

Especially all management functions as listed in Table 6.8 and the ability to query, modify and delete the security attributes for the access control policy Gateway access SFP and the information control policies Firewall SFP and Meter SFP is restricted to the authorized Gateway Administrator and only accessible via the Interface IF_GW_WAN (**FMT_MSA.1/AC**, **FMT_MSA.1/FW** and **FMT_MSA.1/MTR**). Thereby the restricted default values for these policies can not 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 as described in [TR 03109-1], chapter 3.2.3.1. Within this communication scenario a TLS channel between the Gateway and the Gateway Administrator must be in place. To perform a management function the Gateway Administrator sends a web service request that contains CMS-data, if applicable, to the Gateway. The Gateway receives the web service request and performs the requested operation. If the action was successful the Gateway sends the web service response code "OK" and, if applicable, CMS-data to the Gateway Administrator. Otherwise the TOE sends a web service response that contains the corresponding error code and if applicable CMS-data. To transmit the web service requests and responses the TOE uses HTTP/1.1 in accordance to [RFC 2616].

The Service Technician is allowed to read the software version number of the TOE and to read the current time of the TOE (**FMT_MOF.1**). The Service Technician is also allowed to start the selftest and to read the System Log including the result of the selftest. Those 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 to advertise the software version number and the current time of the TOE (**FMT_MOF.1**).
Furthermore the TOE provides reliable time stamps. Therefor the internal system time of the TOE is synchronized according to [RFC 5905] within an interval between 1 minute and 11.6 hours (41653 seconds) with a reliable external time source provided by the Gateway Administrator (**FDP_IFF.1.3/MTR**).
Therefor the TOE supports the communication mechanisms **NTP over TLS** transmitting NTP-Packets using a TLS 1.2 channel 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 amounts to 3% of the shortest measuring period supported by the TOE and allowed for billing by the national calibration authority. If the deviation time is too large the synchronization will fail. In this case the TOE will tag all following Meter Data, create a log entry within the Calibration Log and inform the Gateway Administrator. Furthermore the TOE will stop the operation and enters a secure state (**FDP_IFF.1.3/MTR**). Please refer to section 7.7 for more details on the secure state.
If the Round Trip Time (RTT) exceeds the amount of 3% of the shortest measuring period supported by the TOE and allowed for billing by the national calibration authority the synchronization will fail. In this case the TOE tries to synchronize the time in a short time interval to overcome mobile network characteristics.
In addition the TOE contains a Real Time Clock (RTC) that shall be adjusted using the internal system time of the TOE, if the internal system time corresponds to the reliable time source. The RTC can be used to synchronize the internal system time of the TOE after a power cut if the deviation does not exceed 3% of the shortest measuring period supported by the TOE (**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**).
Therefor the TOE pseudonymizes the Meter ID and the Consumer ID and ensures that no relation between not billing-relevant data and the identity of the Consumer is possible. The Processing Profile determines the data that shall be sent to defined authorized External Entities at defined points in time. For that reason

each Processing Profile states whether the not billing-relevant data shall be pseudonymized and which pseudonym shall be used [81] (**FPR_PSE.1.2**).
Those Processing Profiles are provided to the Gateway by the Gateway Administrator using the Management functionality of the TOE[82]. Each time when a Processing Profile is updated or a new one added, the TOE checks whether it contains a pseudonym.
If Meter Data shall be provided pseudonymized to an authorized External Entity the TOE removes the unique Meter ID, Consumer ID and all other possibly personally identifiable information (PII) and replaces the IDs or PII by the pseudonym given within the Processing Profile. Thereby the TOE determines the alias for a user and verifies that it conforms to the alias given in the Processing Profile (**FPR_PSE.1.3**). Subsequently the data are encrypted, signed and send out to the authorized External Entity as described within the Processing Profile[83].
Since the Consumer and Meter IDs are pseudonymised the authorized External Entity has no possibility to relate the received data directly to any Consumer (**FPR_PSE.1.1**). Since the TLS channel is authenticated on both sides and the transferred data ist signed and encrypted, the Gateway sending the data is always known to the authorized External Entity.

Further the TOE provides the possibility to conceal the frequency, load and size of Meter Data sent to authorized External Entities to ensure that no information of Consumer behavior can be obtained by an analysis of the sending process (**FPR_CON.1.1**). If the last packet was sent more than 24 hours ago, the TOE sends a packet to the authorized External Entity containing irrelevant data at random points in time between the normal data transfers (**FPR_CON.1.2**).
Further the TOE ensures that no information of Consumer behavior can be obtained by the analysis of the Meter Data size or load sent to authorized External Entities. This is carried out by using a fixed block size (padding) for the transmitted data without correlation to the consumption of the Consumer. The load is protected against analysis by using symmetric encryption. Every time a new CMS data container is send, a new encryption key is used. Also by the analysis of the load of several CMS data container it won't be possible to extract any personally identifiable information.

## 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 and physical attacks and the failure with preservation of a secure state.
Within the self test functionality the TOE implements different tests which are used to define the system health status (**FPT_TST.1**). Those tests can be grouped in three categories:

- periodically running tests,
- tests running at start-up and
- passive detection of 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. The periodically running tests comprise:

- signature verification of all application and operation system files,
- checking for files not listed in the software suite description,

[81] According to the assumption A.ProcessProfile it is assumed that the Processing Profiles are trustworthy and correct.
[82] See section 7.5 for more details on the Management functionality of the TOE.
[83] See section 7.2 for more details on the encryption algorithm and process.

- verification of all log, meter and configuration data and their signatures,
- verification of the time by comparing the internal system time with the time provided by the NTP-Server of the Gateway Administrator,
- running the test routine of every software module of the TOE,
- verification of HAN/WAN separation,
- checking that HAN and WAN interfaces are not interchanged.

In addition the TOE provides a set of mechanisms against replay attacks. Therefor 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). The used TLS-protocol[84] protects the TOE against replay attacks. Further, to detect replay attacks from LMN the TOE checks whether the transmission counter of the received data is monotonically increasing. 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**).
Further this TSF provides different secure states of the TOE, that are used to prevent an attacker from gaining information about the device configuration and the device itself (**FPT_FLS.1**).
In some secure states the system shuts down all functions that have thrown critical errors, have been compromised or cannot work properly because of system state. The TOE enters one of these secure states, if one of the following events occur:

- the deviation between the internal system time and the reliable time source is too large and exceeds 3% of the shortest measuring period supported by the TOE and allowed for billing by the national calibration authority,
- the memory consumption of log and meter data storage has reached a critical limit,
- the HAN interface is connected to the WAN, the HAN-WAN interfaces are not separate or have been interchanged,
- a critical and non-correctable error occurred in the boot process

In other secure states all newly and stored metering data will be marked, so they cannot be used for billing anymore. If one of the following events occur, the TOE enters the secure state:

- the deviation between local system time of the TOE and the reliable external time source is too large

The TOE is protected by a secure boot mechanism using a trust chain from start-up to the TOE application. A critical error in the boot process e.g. by missing boot components, integrity or authentication failures or unexpected version numbers result in a special secure state terminating the TOE application.
Within the others non-terminating secure states the TOE overrides functional requirements and parameters set by the Gateway Administrator in accordance with the following table:

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

| Function | Action take upon entering the secure state |
|---|---|
| **WAN connectivity** | |
| TLS Channels | All TLS channels will be terminated. All TLS channels will be deactivated except those used for connection to the Gateway Administrator |
| Wake-up call | No action taken. |
| **LMN connectivity** | |
| IF_GW_MTR | Will be disabled. |
| **HAN connectivity** | |
| CLS functionality | Will be disabled. |
| TLS Channels | All TLS channels will be terminated. |
| **SMGW Logsystem** | |
| Access to the Consumer Logs | No action taken. |
| Access to the System Log | No action taken. |
| Access to the Calibration Log | No action taken. |
| Application Management | All applications no longer needed will be shut down. |

**Table 7.1: Actions performed entering and within the Secure State of the TOE**

To return to normal operational mode, a complete reboot is required.

In addition the TOE provides a detection mechanisms to determine whether physical tampering of the Gateway has occurred. Therefor a BSI TL-03415 certified seal is affixed at the Gateway in a way that it is not possible to open the casing of the Gateway without visible tampering the seal.
Furthermore it is assured that no critical signals are attachable from outside the casing of the TOE (**FPT_PHP.1**).

## 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 | | | | | | |
| **FAU_STG.4/SYS** | X | | | | | | |
| **FAU_GEN.1/CON** | X | | | | | | |
| **FAU_SAR.1/CON** | X | | | | | | |

| | SF.AU | SF.CR | SF.UD | SF.IA | SF.SM | SF.PR | SF.SP |
|---|---|---|---|---|---|---|---|
| **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 | 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 | | | | |
| **FIA_ATD.1** | | | | X | | | |
| **FIA_AFL.1** | | | | X | | | |
| **FIA_UAU.2** | | | | X | | | |
| **FIA_UAU.5** | | | | X | | | |
| **FIA_UAU.6** | | | | X | | | |
| **FIA_UID.2** | | | | X | | | |
| **FIA_USB.1** | | | | X | | | |
| **FMT_MOF.1** | | | | | X | | |
| **FMT_SMF.1** | | | | | X | | |
| **FMT_SMR.1** | | | X | X | X | | |
| **FMT_MSA.1/AC** | | | | | X | | |

| | SF.AU | SF.CR | SF.UD | SF.IA | SF.SM | SF.PR | SF.SP |
|---|---|---|---|---|---|---|---|
| **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 7.2: Fulfillment of Security Requirements**

# A. Mapping from English to German terms

| English term | German term |
|---|---|
| billing-relevant | abrechnungsrelevant |
| CLS, Controllable Local System | dezentral steuerbare Verbraucher- oder Erzeugersysteme |
| Consumer | Anschlussnutzer<br>Letztverbraucher (im verbrauchenden Sinne)<br>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) |
| MPO | Messstellenbetreiber (MSB) |
| Processing Profiles | Konfigurationsprofile |
| Security Module | Sicherheitsmodul (z.B. eine Smart Card) |
| Service Provider | Diensteanbieter |
| Smart Meter<br>Smart Metering System[85] | Intelligente, in ein Kommunikationsnetz eingebundene, elektronische Messeinrichtung (Messsystem) |
| TOE | EVG (Evaluierungsgegenstand) |
| WAN, Wide Area Network | Weitverkehrsnetz (für Kommunikation) |

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

# B. Glossary

| Term | Description |
|---|---|
| 8p8c | 8 position 8 contact connector |
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| APN | Access Point Name |
| Authenticity | property that an entity is what it claims to be (according to [SD6]) |
| Block Tariff | Tariff in which the charge is based on a series of different energy/volume rates applied to successive usage blocks of given size and supplied during a specified period. (according to [CEN]) |
| CA | Certificate Authority or Certification Authority, an entity that issues digital certificates. |
| CEK | Customer Encryption Key, used for encryption of PPA and ISW. |
| CLS config (secondary asset) | See [ST, section 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]) |
| CPU | Central Processing Unit |
| CPU-SIG | CPU specific signature key, known to the SMGW manufacturer only and identical for all devices. The CPU-Sig Public Key means the same key as MPK. |
| CSS | Cascading Style Sheets |
| DHCP | Dynamic Host Configuration Protocol |
| DKE | Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE |
| DLMS | Device Language Message Specification (originally Distribution Line Message Specification) |
| DNS | Domain Name System |
| DTBS | Data To Be Signed |
| EAL | Evaluation Assurance Level |
| ECC | Elliptic Curve Cryptography |
| eFuse | Memory location that is one time programmable only. The term *OTP-Memory* is used for this functionality as well. |
| eMMC | embedded MultiMediaCard, |

| Term | Description |
|---|---|
| EMT | Externer Marktteilnehmer |
| Energy Service Provider | Organisation offering energy related services to the consumer (according to [CEN]) |
| External entity | See [ST, section 3.1] |
| FAKRA D | 50 ohm radio frequency interface (RFI) for road vehicles (50 Ohm RFI) acc. DIN 72594-1 and USCAR-18 ("'FAchKReis Automobil"') |
| FDT | Flattened Device Tree. Abstraction layer to make the Linux-kernel more hardware independent. |
| FIT-Image | Flattened Image Tree. Image format which consists on a tree structure with subimages and configurations. |
| Firmware update | See [ST, section 3.2] |
| FQDN | Fully qualified domain name. Ein vollständiger Domainname inklusive Toplevel- und Subdomains, sofern vorhanden. |
| Gateway Administrator (GWA) | See [ST, section 3.1] |
| Gateway config (secondary asset) | See [ST, section 3.2] |
| Gateway time | See [ST, section 3.2] |
| GID | Group ID. Gruppen ID einer Benutzergruppe im Linux-Rechtemanagement. |
| GPIO | General Purpose IO |
| GPRS | General Packet Radio Service |
| GSM | Global System for Mobile |
| HDLC | High-Level Data Link Control |
| HAN-Module | Optional module which is not part of the TOE, providing a 8p8c modular socket (RJ45) for HAN connections. |
| Home Area Network (HAN) | In-house LAN which interconnects domestic equipment and can be used for energy management purposes. (according to [CEN]) |
| HREF-Anchor | HTML Anchor Tag using a "'href"'-attribute for setting a hyperlink. |
| HTML | Hypertext Markup Language |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HyperText Transfer Protocol Secure |
| HUID | Herstellerübergreifende Identifikationsnummer des DKE |
| Integrity | property that sensitive data has not been modified or deleted in an unauthorised and undetected manner (according to [SD6]) |
| IPC | Inter Process Communication |
| ISW | Initial Software. Part of the Secure Signed Image (SSI) and same as U-Boot-SPL. |
| IT-System | Computersystem |

| Term | Description |
|---|---|
| JSON | JavaScript Object Notation |
| KEK | Key Encryption Key, used for encryption of the CEK. |
| LAN | Local Area Network |
| LED | Light-emitting diode |
| Local attacker | See [ST, section 3.4] |
| LSM | Linux Security Modul |
| LTE | Long Term Evolution |
| MAC | Message Authentication Code |
| MB | Mega Byte |
| M-Bus | Meter-Bus |
| Meter | See [ST, section 1.4] |
| Meter config (secondary asset) | See [ST, section 3.2] |
| Meter Data | See [ST, section 3.2] |
| Meter Data Aggregator (MDA) | Entity which offers services to aggregate metering data by grid supply point on a contractual basis.<br>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).<br>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]) |
| Metrological Area Network | In-house data communication network which interconnects metrological equipment (i.e. Meters). |
| MLO | The name "MLO" is a setpoint value for the first stage bootloader file (Minimal Bootloader) of the used processor system for the startup from memory devices. |
| MPK | Master Public Key used for Secure Boot process. |
| MPO | Metering Point Operator. |
| NTP | Network Time Protocol |
| NTPd | NTP daemon |
| OMS | Open Metering System |
| OS | Operating System |

| Term | Description |
|---|---|
| OSS | Open Source Software. Software that uses a GPL or similar license type. |
| OTP-Memory | Memory location that is one time programmable only. The term *eFuse* is used for this functionality as well. |
| PC | Protocol Converter |
| 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. |
| PIN | Personal Identification Number. |
| PKA | Public Keys Accelerator. Hardware unit for fast asymmetric public-key based decryption. |
| PKC | Public Keys Certificate. List containing public keys for Secure Boot. Structure defined by the CPU manufacturer. |
| PLMN | Public Land Mobile Network. Access to PLMN is achieved using radio communication and communications towers. Sometimes the name PLMN is used for the addition of Mobile Country Code (MCC) and Mobile Network Code (MNC) only. |
| PPA | Primary Protected Application. Application loaded by the ROM-Bootcode to extend the ROM-Code und to configure the hardware firewall. |
| PRNG | Pseudo Random Number Generator |
| Processing Profiles (Auswerteprofile) | Processing Profiles contain the necessary information to receive, process and send the metering data. The virtual container "'Processing Profile"' includes parts from the KAF HAN WAN-Profil, the KAF LMN-Profil and the TAF-Profil. |
| 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 |
| RMII | Reduced Media Independent Interface |
| RNG | Random Number Generator |
| TIA-485 | Standard defining the electrical characteristics of drivers and receivers for use in balanced digital multipoint systems, also known as RS-485 or EIA-485. |
| RTC | Real Time Clock |
| SAP | Service Access Point |
| Secure Boot | Manufacturer specific name of the secure initialisation (boot) feature. |
| Secure Signed Image (SSI) | Image containing the PPA, PKC and ISW. |

| Term | Description |
|---|---|
| Sensor | See: Meter |
| Service Technician | See [ST, section 3.1] |
| SFP | Security Functional Policy |
| SHA | Secure Hash Algorithm |
| SIM | Subscriber Identity Module |
| SLAAC | Stateless Address Autoconfiguration |
| SML | Smart Message Language |
| SMLplus | Smart Message Language plus. SML extension to support overhead reduced realtime readout of meterdata. ([SMLplus]) |
| SMPF | Smart Metering Platform Framework |
| SOCKSv5 | Socket Secure version 5, internet protocol that routes network packets between a client and server through a proxy server. |
| SPL | Secondary Programm Loader. U-Boot based first stage bootloader. Fullname U-Boot-SPL. |
| 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 |
| TOC | Table of Contents |
| TOE | Target of Evaluation – set of software, firmware and/or hardware possibly accompanied by guidance |
| TPM | Trusted Platform Module |
| TSF | TOE security functionality |
| UART | Universal Asynchronous Receiver Transmitter |
| UDP | User Datagram Protocol |
| UID | User ID. Benutzer ID eines Benutzers im Linux-Rechtemanagement. |
| WAN attacker | See [ST, section 3.4] |
| WLAN | Wireless Local Area Network |
| wMBus | wireless M-Bus |
| XML | Extensible Markup Language |
| XSD | XML Schema Definition |

# Bibliography


[CC] *Common Criteria for Information Technology Security Evaluation –*
- *Part 1: Introduction and general model*
- *Part 2: Security functional requirements*
- *Part 3: Security assurance requirements*

(Cit. on pp. 7, 33, 55, 78).

[CEN] *SMART METERS CO-ORDINATION GROUP (SM-CG), TR 50572, M/441 first phase deliverable – Communication – Annex: Glossary* (cit. on pp. 5–7, 119–121, 123).

[DIN EN 13757-1] DIN. *DIN EN 13757-1: Kommunikationssysteme für Zähler und deren Fernablesung, Teil 1: Datenaustausch*. Norm-Entwurf (cit. on p. 108).

[DIN EN 13757-3] DIN. *DIN EN 13757-3: Kommunikationssysteme für Zähler und deren Fernablesung, Teil 3: Spezielle Anwendungsschicht*. Norm (cit. on p. 108).

[DIN EN 13757-4] DIN. *DIN EN 13757-4: Kommunikationssysteme für Zähler und deren Fernablesung, Teil 4: Zählerauslesung über Funk (Fernablesung von Zählern im SRD-Band von 868 MHz bis 870 Mhz)*. Norm (cit. on p. 108).

[DKE COSEM] DKE. *Smart Meter Gateway, Teil 2: Klassen-Definition zur TR 03109 nach COSEM* (cit. on p. 6).

[FIPS 140-2] NIST. *FIPS PUB 140-2: Security Requirements for Cryptographic Modules, Part 2* (cit. on pp. 72, 107).

[FIPS 180-4] NIST. *FIPS PUB 180-4: Secure Hash Standard* (cit. on pp. 69, 70, 72, 105–107).

[FIPS 197] NIST. *FIPS PUB 197: Advanced Encryption Standard (AES)* (cit. on pp. 70–72, 105–107).

[FSP] Theben Smart Energy GmbH. *Funktionale Spezifikation (ADV_FSP.4), CONEXA 3.0 Smart Meter Gateway* (cit. on pp. 18, 19).

[IEC 62056-6-1] IEC. *IEC 62056-6-1: Electricity metering – Data exchange for meter reading, tariff and load control – Part 6-1: COSEM Object Identification System (OBIS)* (cit. on p. 108).

[IEC 62056-6-2] IEC. *IEC 62056-6-2: Electricity metering – Data exchange for meter reading, tariff and load control – Part 6-2: Interface classes, FDIS IEC, Melbourne meeting* (cit. on p. 108).

[IEEE 802.3] IEEE. *IEEE 802.3 Ethernet Working Group - IEEE Standard for Ethernet* (cit. on p. 108).

[MSB-Katalog] BSI. *Anforderungskatalog zur MSB-Lieferkette, in der aktuell gültigen Fassung*. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/MSB/MSB_node.html (cit. on pp. 38, 47).

[NIST SP800-38A] NIST. *Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation*. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf (cit. on pp. 70–72, 105–107).

[NIST SP800-38D] NIST. *Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf (cit. on pp. 70, 105, 106).

[PTB A50.7] PTB. *PTB-A50.7: Physikalisch-Technische Bundesanstalt: Anforderungen an elektronische und softwaregesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme* (cit. on pp. 1, 2, 9).

[PTB A50.8] PTB. *PTB-A50.8: Physikalisch-Technische Bundesanstalt: Anforderungen an elektronische und softwaregesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme* (cit. on pp. 1, 2).

[RFC 2104] IETF. *RFC 2104, HMAC: Keyed-Hashing for Message Authentication* (cit. on pp. 69, 70, 105, 106).

[RFC 2616] IETF. *RFC 2616, R. Fielding et al.: Hypertext Transfer Protocol - HTTP/1.1* (cit. on pp. 104, 108, 112).

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

[RFC 4493] IETF. *RFC 4493, J. H. Song, J. Lee, T. Iwata: The AES-CMAC Algorithm* (cit. on pp. 70, 71, 106, 107).

[RFC 5084] IETF. *RFC 5084, R. Housley: Using AES-CCM amd AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)* (cit. on pp. 70, 106).

[RFC 5114] IETF. *RFC 5114, M. Lepinski, S. Kent: Additional Diffie-Hellman Groups for Use with IETF Standards* (cit. on pp. 106, 107).

[RFC 5246] IETF. *RFC 5246, T. Dierks, E. Rescorla: The Transport Layer Security (TLS) Protocol Version 1.2* (cit. on pp. 69, 70, 105, 106).

[RFC 5289] IETF. *RFC 5289, E. Rescorla: TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)* (cit. on pp. 69, 70, 105, 106).

[RFC 5639] IETF. *RFC 5639, M. Lochter, J. Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation* (cit. on p. 106).

[RFC 5905] IETF. *RFC 5905, D. Mills, et al.: Network Time Protocol Version 4: Protocol and Algorithms Specification* (cit. on pp. 76, 112).

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

[SM-PP] BSI. *Common Criteria Protection Profile for a Security Module for Smart Metering Systems (BSI-CC-PP-0077)* (cit. on pp. 6, 9, 10, 28, 40, 46).

[SMGW-PP] BSI. *Common Criteria Protection Profile for a Gateway for Smart Metering Systems (BSI-CC-PP-0073)* (cit. on pp. 1–3, 9, 20, 33, 91).

[SMLplus] Hausheld AG. *SMLplus* (cit. on p. 123).

[ST] Theben Smart Energy GmbH. *Security Target (ASE), CONEXA 3.0 - Smart Meter Gateway* (cit. on pp. 119–121, 123).

[TIA 485] TIA. *Electrical Characteristics of Generators and Receivers for Use in Balanced Multipoint Systems* (cit. on p. 108).

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

[TR 03109-1] BSI. *BSI TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems* (cit. on pp. 11, 12, 16, 26, 38, 41, 45, 69, 73, 79, 80, 104, 108, 110, 112).

[TR 03109-1-I] BSI. *BSI TR-03109-1 Anlage I: CMS Datenformat für die Inhaltsdatenverschlüsselung und -signatur* (cit. on p. 30).

[TR 03109-1-VI] BSI. *BSI TR-03109-1 Anlage VI: Betriebsprozesse* (cit. on p. 32).

[TR 03109-3] BSI. *BSI TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen* (cit. on pp. 16, 30, 38, 47).

[TR 03109-4] BSI. *BSI TR-03109-4: Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways* (cit. on p. 110).

[TR 03111] BSI. *BSI TR-03111: Elliptic Curve Cryptography (ECC)* (cit. on pp. 70, 107).