



Security Target

SMGW Version 1.3.2

1 **Version History**

Version	Datum	Name	Änderungen
1.4	10.01.2025	C. Miller	SMGW 1.3.2

Contents

Contents	3
1 Introduction	6
1.1 ST reference	6
1.2 TOE reference	6
1.3 Introduction.....	10
1.4 TOE Overview	11
1.4.1 Introduction	11
1.4.2 Overview of the Gateway in a Smart Metering System	12
1.4.3 TOE description.....	15
1.4.4 TOE Type definition	16
1.4.5 TOE logical boundary	19
1.4.6 The logical interfaces of the TOE	27
1.4.7 The cryptography of the TOE and its Security Module	28
TOE life-cycle	32
2 Conformance Claims	33
2.1 CC Conformance Claim	33
2.2 PP Claim / Conformance Statement	33
2.3 Package Claim	33
2.4 Conformance Claim Rationale	33
3 Security Problem Definition	35
3.1 External entities	35
3.2 Assets.....	35
3.3 Assumptions	39
3.4 Threats.....	41
3.5 Organizational Security Policies.....	45
4 Security Objectives	47
4.1 Security Objectives for the TOE	47
4.2 Security Objectives for the Operational Environment.....	52
4.3 Security Objective Rationale.....	54
4.3.1 Overview	54
4.3.2 Countering the threats.....	56
4.3.3 Coverage of organisational security policies	59
4.3.4 Coverage of assumptions	59
5 Extended Component definition	61
5.1 Communication concealing (FPR_CON)	61
5.2 Family behaviour	61
5.3 Component levelling.....	61
5.4 Management.....	61
5.5 Audit	61
5.6 Communication concealing (FPR_CON.1)	61
6 Security Requirements.....	63
6.1 Overview.....	63

45	6.2 Class FAU: Security Audit.....	67
46	6.2.1 Introduction	67
47	6.2.2 Security Requirements for the System Log	69
48	6.2.3 Security Requirements for the Consumer Log	72
49	6.2.4 Security Requirements for the Calibration Log	75
50	6.2.5 Security Requirements that apply to all logs	80
51	6.3 Class FCO: Communication.....	82
52	6.3.1 Non-repudiation of origin (FCO_NRO)	82
53	6.4 Class FCS: Cryptographic Support	83
54	6.4.1 Cryptographic support for TLS.....	83
55	6.4.2 Cryptographic support for CMS	84
56	6.4.3 Cryptographic support for Meter communication encryption	86
57	6.4.4 General Cryptographic support.....	88
58	6.5 Class FDP: User Data Protection	91
59	6.5.1 Introduction to the Security Functional Policies	91
60	6.5.2 Gateway Access SFP	91
61	6.5.3 Firewall SFP	93
62	6.5.4 Meter SFP	96
63	6.5.5 General Requirements on user data protection.....	100
64	6.6 Class FIA: Identification and Authentication	101
65	6.6.1 User Attribute Definition (FIA_ATD)	101
66	6.6.2 Authentication Failures (FIA_AFL)	102
67	6.6.3 User Authentication (FIA_UAU)	102
68	6.6.4 User identification (FIA_UID)	104
69	6.6.5 User-subject binding (FIA_USB).....	105
70	6.7 Class FMT: Security Management	106
71	6.7.1 Management of the TSF.....	106
72	6.7.2 Security management roles (FMT_SMR)	113
73	6.7.3 Management of security attributes for Gateway access SFP.....	114
74	6.7.4 Management of security attributes for Firewall SFP	115
75	6.7.5 Management of security attributes for Meter SFP	116
76	6.8 Class FPR: Privacy	117
77	6.8.1 Communication Concealing (FPR_CON)	117
78	6.8.2 Pseudonymity (FPR_PSE)	118
79	6.9 Class FPT: Protection of the TSF	119
80	6.9.1 Fail secure (FPT_FLS).....	119
81	6.9.2 Replay Detection (FPT_RPL).....	120
82	6.9.3 Time stamps (FPT_STM)	120
83	6.9.4 TSF self test (FPT_TST).....	120
84	6.9.5 TSF physical protection (FPT_PHP).....	121
85	6.10 Class FTP: Trusted path/channels.....	121
86	6.10.1 Inter-TSF trusted channel (FTP_ITC).....	121

87	6.11	Security Assurance Requirements for the TOE.....	123
88	6.12	Security Requirements rationale	125
89	6.12.1	Security Functional Requirements rationale.....	125
90	6.12.2	Security Assurance Requirements rationale	138
91	7	TOE Summary Specification.....	139
92	7.1	SF.1: Authentication of Communication and Role Assignment for external	
93		entities.....	139
94	7.2	SF.2: Acceptance and Deposition of Meter Data, Encryption of Meter Data for	
95		WAN transmission.....	146
96	7.3	SF.3: Administration, Configuration and SW Update	148
97	7.4	SF.4: Displaying Consumption Data.....	150
98	7.5	SF.5: Audit and Logging.....	151
99	7.6	SF.6: TOE Integrity Protection	153
100	7.7	TSS Rationale.....	154
101	8	List of Tables.....	158
102	9	List of Figures	159
103	10	Appendix	160
104	10.1	Mapping from English to German terms	160
105	10.2	Glossary	162
106	11	Literature	167
107			

1 Introduction

1.1 ST reference

Title:	Security Target, SMGW Version 1.3.2
Editors:	Power Plus Communications AG
CC-Version:	3.1 Revision 5
Assurance Level:	EAL 4+, augmented by AVA_VAN.5 and ALC_FLR.2
General Status:	Final
Document Version:	1.4
Document Date:	10.01.2025
TOE:	SMGW Version 1.3.2
Certification ID:	BSI-DSZ-CC-0831-V8-2023

This document contains the security target of the *SMGW Version 1.3.2*.

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

1.2 TOE reference

The TOE described in this security target is the *SMGW Version 1.3.2*.

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

- *BPL Smart Meter Gateway* (BPL-SMGW), SMGW-B-1A-111-00 or SMGW-B-1B-111-00
- *CDMA Smart Meter Gateway* (CDMA-SMGW), SMGW-C-1A-111-00
- *ETH Smart Meter Gateway* (ETH-SMGW), SMGW-E-1A-111-00 or SMGW-E-1B-111-00
- *GPRS Smart Meter Gateway* (GPRS-SMGW), SMGW-G-1A-111-30

- *LTE Smart Meter Gateway* (LTE-SMGW), SMGW-L-1A-111-30, SMGW-L-1A-111-10, SMGW-L-1B-111-30, SMGW-L-1B-111-10, SMGW-K-1B-111-10, SMGW-K-1B-111-20 or SMGW-K-1B-111-30
- *powerWAN-ETH Smart Meter Gateway* (pWE-SMGW), SMGW-P-1B-111-00
- *G.hn Smart Meter Gateway* (G.hn-SMGW), SMGW-N-1B-111-00
- *LTE450 Smart Meter Gateway* (LTE450-SMGW), SMGW-V-1A-111-20 or SMGW-V-1B-111-20

The TOE comprises the following parts:

- hardware device of the hardware generation 1A or 1B according to Table 1, including the TOE's main circuit board, a carrier board, a power-supply unit and a radio module for communication with wireless meter (included in the hardware device "*Smart Meter Gateway*")
- firmware including software application (loaded into the circuit board)
 - "*SMGW Software Version 1.3.2*", identified by the value 33918-34868 which comprises of two revision numbers of the underlying version control system for the TOE, where the first part is for the operating system and the second part is for the SMGW application
- manuals
 - „Handbuch für Verbraucher, Smart Meter Gateway“ [AGD_CONSUMER], identified by the SHA-256 hash value 4816009774a634d207edb00ca6408bb28c26daf2c6c9185ced1f1215088a02e4
 - „Handbuch für Service-Techniker, Smart Meter Gateway“ [AGD_Techniker], identified by the SHA-256 hash value 1be4058c8db43bcf730387c9f14f0e87bc84db5520815804daaf8f5de1ed6c5a
 - „Handbuch für Hersteller von Smart-Meter Gateway-Administrations-Software, Smart Meter Gateway“ [AGD_GWA], identified by the SHA-256 hash value 4c2e9765853136121c370f7ba6bf9c5e969a704020153e065f9dad1977c9f586
 - „Logmeldungen, SMGW“ [SMGW_Logging] identified by the SHA-256 hash value f3a935b6ae1713ccdaa02411b377377a8e4f7dfb092a181efe1a6c9a86f17a64
 - „Auslieferungs- und Fertigungsprozeduren, Anhang Sichere Auslieferung“ [AGD_SEC], identified by the SHA-256 hash value 88ec18e33637440cca7f93456789b33819c3dc4fcd46a2c711e50e235756aa8

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

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

#	Characteristic	Value	Description
1	Product family	SMGW	each classification of a type start with this value
2		-	<i>Delimiter</i>
3	Communication Technology	B	Product Type „BPL Smart Meter Gateway“
		H	Product Type “BPL Smart Meter Gateway”
		C	Product Type „CDMA Smart Meter Gateway“
		E	Product Type „ETH Smart Meter Gateway“
		G	Product Type „GPRS Smart Meter Gateway“
		L	Product Type „LTE Smart Meter Gateway“
		J	Product Type “LTE Smart Meter Gateway”
		K	Product Type „LTE Smart Meter Gateway“
		D	Product Type „LTE Smart Meter Gateway“
		O	Product Type „LTE Smart Meter Gateway“

#	Characteristic	Value	Description
		P	Product Type „powerWAN-ETH Smart Meter Gateway“
		N	Product Type „G.hn Smart Meter Gateway“
		V	Product Type “LTE450 Smart Meter Gateway”
4		-	<i>Delimiter</i>
5	Hardware generation	1A	Identification of hardware generation; version 1.0 of “SMGW Hardware”
		1B	Identification of hardware generation; version 1.0.1 of “SMGW Hardware” (with new power adapter)
		2A	Identification of hardware generation; version 2.0 of “SMGW Hardware”
		2B	Identification of hardware generation; version 2B of “SMGW Hardware”
6		-	<i>Delimiter</i>
7	HAN Interface	1	Ethernet
8	CLS Interface	1	Ethernet
9	LMN Interface	1	Wireless and wired
10		-	<i>Delimiter</i>
11	SIM card type	0	<i>None</i>
		1	SIM card assembled at factory and SIM slot
		2	SIM card assembled at factory only

#	Characteristic	Value	Description
		3	SIM slot only
12	reserved	0	

Table 1: Smart Meter Gateway product classifications

1.3 Introduction

The increasing use of *green energy* and upcoming technologies around e-mobility lead to an increasing demand for functions of a so called smart grid. A smart grid hereby refers to a commodity¹ network that intelligently integrates the behaviour and actions of all entities connected to it – suppliers of natural resources and energy, its consumers and those that are both – in order to efficiently ensure a more sustainable, economic and secure supply of a certain commodity (definition adopted from [CEN]).

In its vision such a smart grid would allow to invoke consumer devices to regulate the load and availability of resources or energy in the grid, e.g. by using consumer devices to store energy or by triggering the use of energy based upon the current load of the grid². Basic features of such a smart use of energy or resources are already reality. Providers of electricity in Germany, for example, have to offer at least one tariff that has the purpose to motivate the consumer to save energy.

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

An essential aspect for all considerations of a smart grid is the so called *Smart Metering System* that meters the consumption or production of certain commodities at the

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

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

consumers' side and allows sending the information about the consumption or production to external entities, which is then the basis for e. g. billing the consumption or production.

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

The Target of Evaluation (TOE) that is described in this document is an electronic unit comprising hardware and software/firmware³ used for collection, storage and provision of Meter Data⁴ from one or more Meters of one or multiple commodities.

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

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

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

1.4 TOE Overview

1.4.1 Introduction

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

There are various different vocabularies existing in the area of Smart Grid, Smart Metering and Home Automation. Furthermore, the Common Criteria maintain their own vocabulary. The Protection Profile [PP_GW, chapter 1.3] provides an overview over the

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

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

most prominent terms used in this Security Target to avoid any bias which is not fully repeated here.

1.4.2 Overview of the Gateway in a Smart Metering System

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

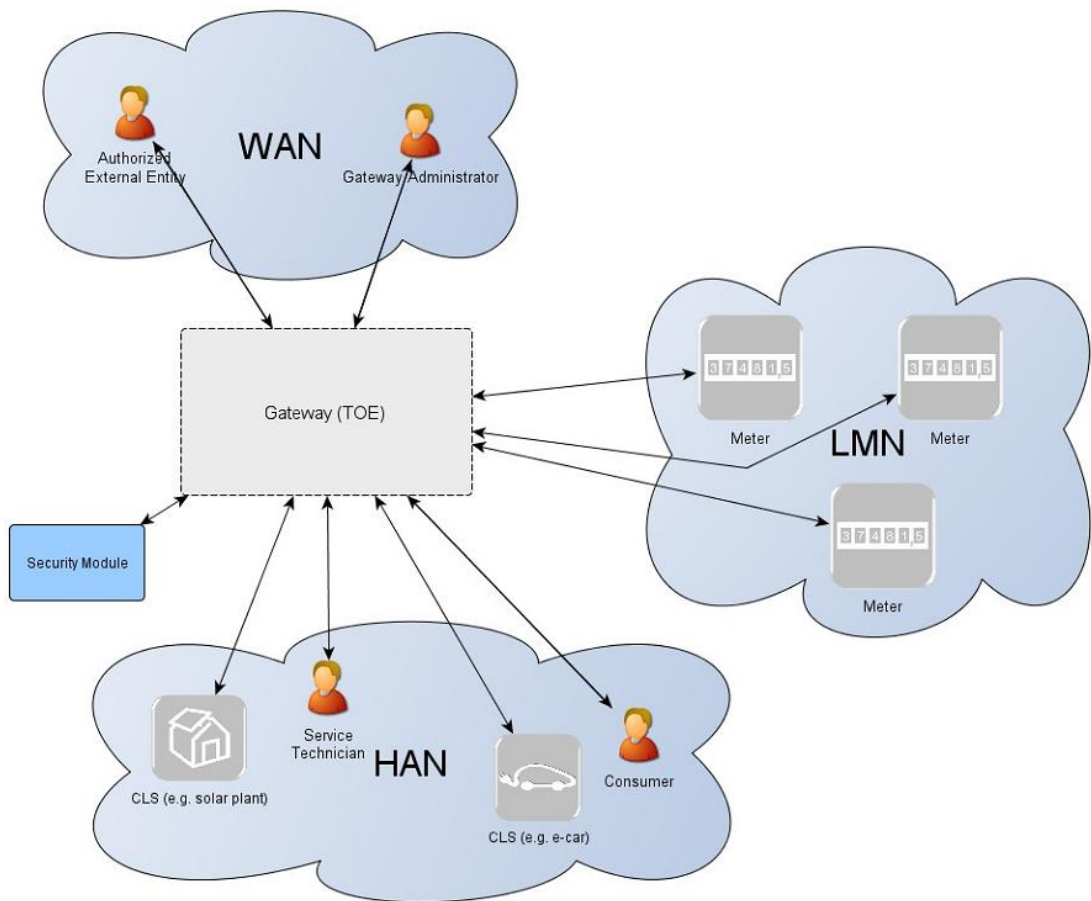


Figure 1: The TOE and its direct environment

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

- The **Gateway** (as defined in this ST) serves as the communication component between the components in the local area network (LAN) of the consumer and

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.

the outside world. It can be seen as a special kind of firewall dedicated to the smart metering functionality. It also collects, processes and stores the records from Meter(s) and ensures that only authorised parties have access to them or derivatives thereof. Before sending meter data⁶ 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 meter⁷ and has comparable security requirements; it will be sealed as classical meters according to the regulations of the calibration authority. The Meter further supports the encryption and integrity protection of its connection to the Gateway⁸.
- The Gateway utilises the services of a **Security Module** (e.g. a smart card) as a cryptographic service provider and as a secure storage for confidential assets. The Security Module will be evaluated separately according to the requirements in the corresponding Protection Profile (c.f. [SecModPP]).

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

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

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

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

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

the following chapters of this ST will place dedicated requirements on the way an information flow can be initiated⁹.

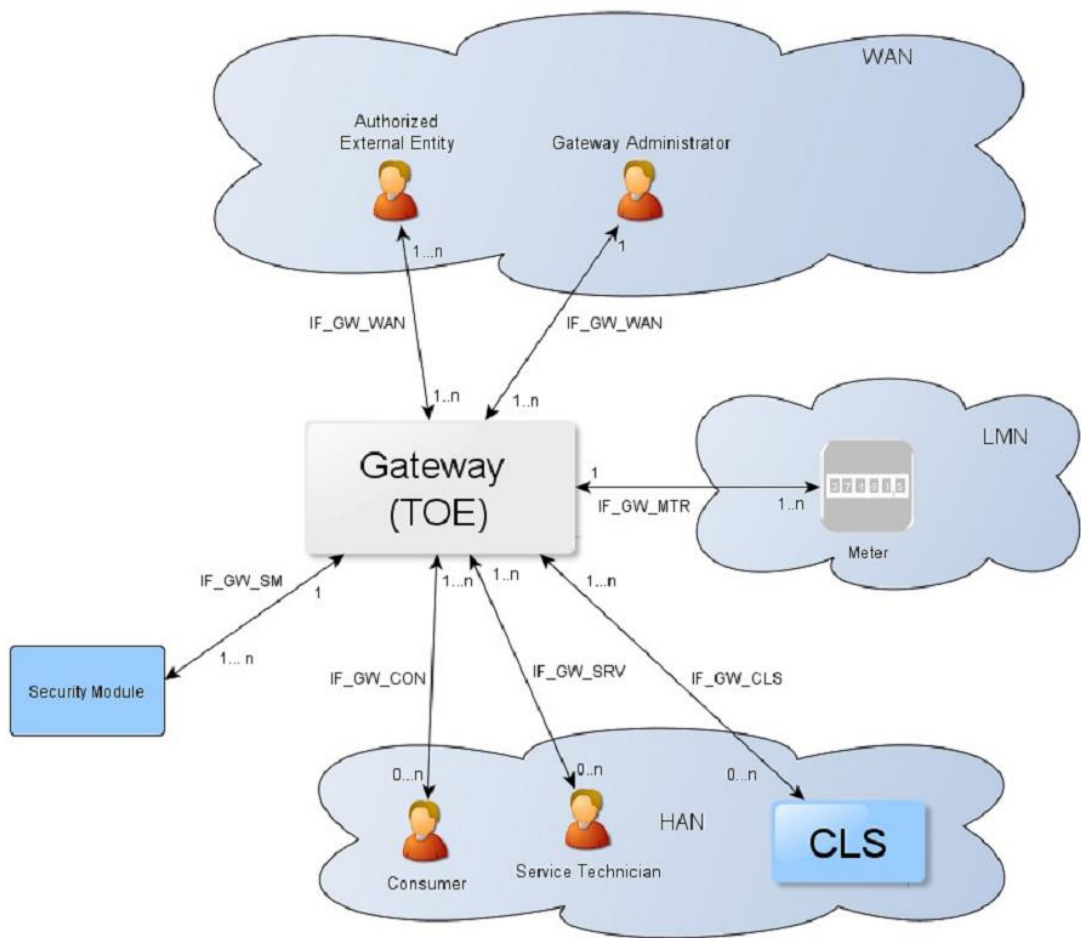


Figure 2: The logical interfaces of the TOE

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

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

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

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

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

1.4.3 TOE description

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

Typically, the Gateway will be placed in the household or premises of the consumer¹⁰ of the commodity and enables access to local Meter(s) (i.e. the unit(s) used for measuring the consumption or production of electric power, gas, water, heat etc.) and may enable access to Controllable Local Systems (e.g. power generation plants, controllable loads such as air condition and intelligent household appliances).

The TOE has a fail-safe design that specifically ensures that any malfunction can not impact the delivery of a commodity, e.g. energy, gas or water¹¹.

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

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

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

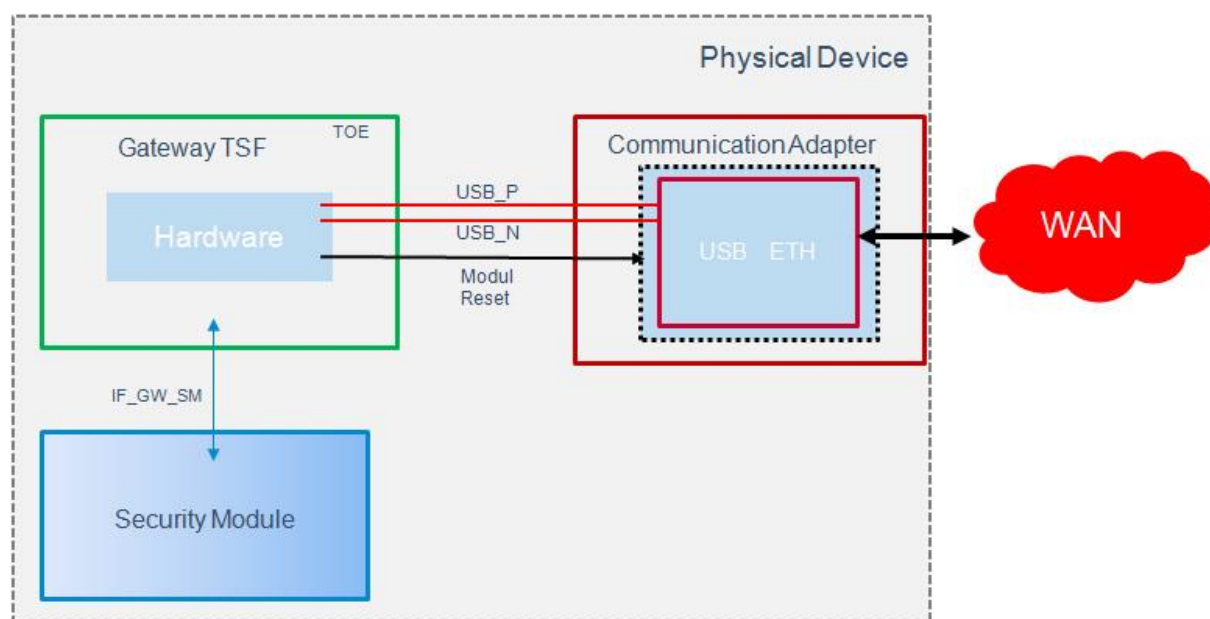


Figure 3: The product with its TOE and non-TOE parts

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

1.4.4 TOE Type definition

At first, the TOE is a communication Gateway. It provides different external communication interfaces and enables the data communication between these interfaces and connected IT systems. It further collects, processes and stores Meter Data and is responsible for the distribution of this data to external parties.

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

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

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

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

The TOE-design includes the following components:

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

The TOE evaluation does not include the evaluation of the Security Module. In fact, the TOE relies on the security functionality of the Security Module but it must be security evaluated in a separate security evaluation¹².

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

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

The TOE supports the following communication protocols:

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

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

The TOE provides the following physical interfaces for communication

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

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

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

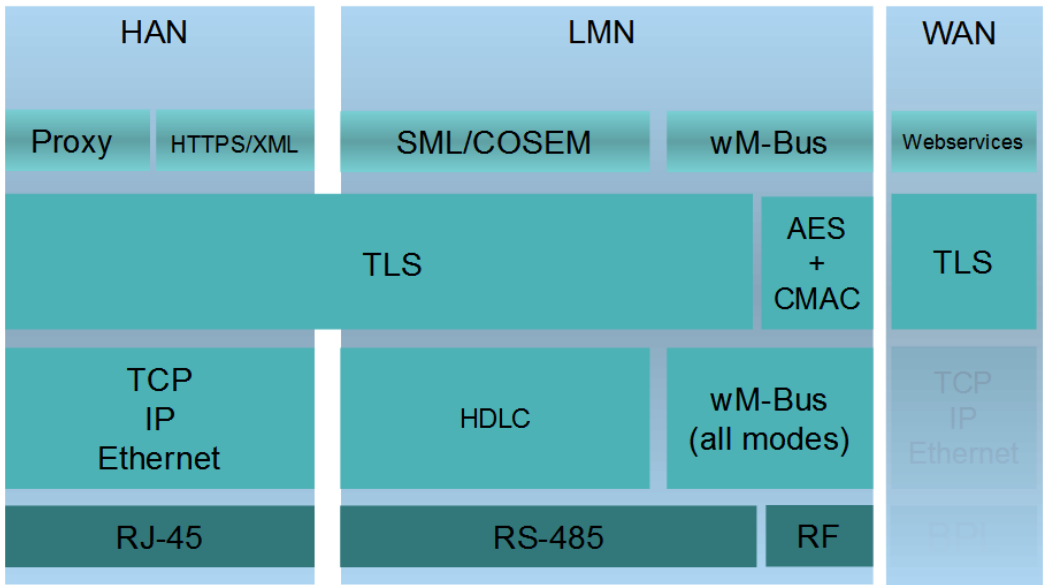


Figure 4: The TOE's protocol stack

The TOE provides the following functionality:

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

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

1.4.5 TOE logical boundary

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

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

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

1.4.5.1 Handling of Meter Data¹³

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

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

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

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

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

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

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

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

These functionalities:

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

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

1.4.5.2 Confidentiality protection

The TOE protects data from unauthorised disclosure

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

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

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

1.4.5.3 Integrity and Authenticity protection

The Gateway provides the following authenticity and integrity protection:

- Verification of authenticity and integrity when receiving Meter Data from a Meter via the LMN, to verify that the Meter Data have been sent from an authentic Meter and have not been altered during transmission. The TOE utilises the services of its Security Module for aspects of this functionality.
- Application of authenticity and integrity protection measures when sending processed Meter Data to an external entity, to enable the external entity to verify that the processed Meter Data have been sent from an authentic Gateway and have not been changed during transmission. The TOE utilises the services of its Security Module for aspects of this functionality.
- Verification of authenticity and integrity when receiving data from an external entity (e.g. configuration settings or firmware updates) to verify that the data have been sent from an authentic and authorised external entity and have not been changed during transmission. The TOE utilises the services of its Security Module for aspects of this functionality.

These functionalities

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

- facilitate the integrity of billing processes and serve for the interests of the consumer as well as for the interest of the supplier. Both parties are interested in the transmission of correct processed Meter Data to be used for billing,
- protect the Smart Metering System and a corresponding large scale Smart Grid infrastructure by preventing that data (e.g. Meter Data, configuration settings, or firmware updates) from forged components (with the aim to cause damage to the Smart Grid) will be accepted in the system.

1.4.5.4 Information flow control and firewall

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

- only the Gateway may establish a connection to an external entity in the WAN¹⁴; specifically connection establishment by an external entity in the WAN or a Meter in the LMN to the WAN is not possible,
- the Gateway can establish connections to devices in the LMN or in the HAN,
- Meters in the LMN are only allowed to establish a connection to the Gateway,
- the Gateway shall offer a wake-up service that allows external entities in the WAN to trigger a connection establishment by the Gateway,
- connections are allowed to pre-configured addresses only,
- only cryptographically-protected (i.e. encrypted, integrity protected and mutually authenticated) connections are possible.¹⁵

These functionalities

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

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

¹⁵ To establish an encrypted channel the TOE may use the required protocols such as DHCP or PPP. Beside the establishment of an encrypted channel no unprotected communication between the TOE and external entities located in the WAN or LAN is allowed.

Meter Data (with the aim to cause damage to the Smart Grid), and by preventing that widely distributed Smart Metering Systems can be abused as a platform for malicious software/firmware to attack other systems in the WAN (e.g. a WAN attacker who would be able to install a botnet on components of the Smart Metering System).

The communication flows that are enforced by the Gateway between parties in the HAN, LMN and WAN are summarized in the following table¹⁶:

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

Table 2: Communication flows between devices in different networks

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

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

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

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

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

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

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

1.4.5.5 Wake-Up-Service

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

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

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

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

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

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

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

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

1.4.5.6 Privacy Preservation

The preservation of the privacy of the consumer is an essential aspect that is implemented by the functionality of the TOE as required by this ST.

This contains two aspects:

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

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

Monitoring of Data Transfers

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

Configuration Reporting

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

Audit Log and Monitoring

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

1.4.5.7 Management of Security Functions

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

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

System Status

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

1.4.5.8 Identification and Authentication

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

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

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

1.4.6 The logical interfaces of the TOE

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

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

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

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

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

Table 3: Mandatory TOE external interfaces

1.4.7 The cryptography of the TOE and its Security Module

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

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

Aspect	TOE	Security Module
Communication with external entities	<ul style="list-style-type: none">• encryption• decryption• hashing• key derivation• MAC generation• MAC verification• secure storage of the TLS certificates	Key negotiation: <ul style="list-style-type: none">• support of the authentication of the external entity• secure storage of the private key• random number generation• digital signature verification and generation
Communication with the consumer	<ul style="list-style-type: none">• encryption• decryption• hashing• key derivation• MAC generation• MAC verification• secure storage of the TLS certificates	Key negotiation: <ul style="list-style-type: none">• support of the authentication of the consumer• secure storage of the private key• digital signature verification and generation• random number generation

Communication with the Meter	<ul style="list-style-type: none">• encryption• decryption• hashing• key derivation• MAC generation• MAC verification• secure storage of the TLS certificates	Key negotiation (in case of TLS connection): <ul style="list-style-type: none">• support of the authentication of the meter• secure storage of the private key• digital signature verification and generation• random number generation
Signing data before submission to an external entity	<ul style="list-style-type: none">• hashing	Signature creation <ul style="list-style-type: none">• secure storage of the private key
Content data encryption and integrity protection	<ul style="list-style-type: none">• encryption• decryption• MAC generation• key derivation• secure storage of the public Key	Key negotiation: <ul style="list-style-type: none">• secure storage of the private key• random number generation

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

1.4.7.1 Content data encryption vs. an encrypted channel

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

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

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

This concept of encryption on two layers facilitates use cases in which the external party that the TOE communicates with is not the final recipient of the Meter Data. In

this way, it is for example possible that the Gateway Administrator receives Meter Data that they forward to other parties. In such a case, the Gateway Administrator is the endpoint of the trusted channel but cannot read the Meter Data.

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

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

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

1. The Meter measures the consumption or production of a certain commodity.
2. The Meter Data is prepared for transmission:
 - a. The Meter Data is typically signed (typically using the services of an integrated Security Module).
 - b. If the communication between the Meter and the Gateway is performed bidirectional, the Meter Data is transmitted via an encrypted and mutually authenticated channel to the Gateway. Please note that the submission of this information may be triggered by the Meter or the Gateway.
- or
- c. If a unidirectional communication is performed between the Meter and the Gateway, the Meter Data is encrypted using a symmetric algorithm (according to [TR-03109-3]) and facilitating a defined data structure to ensure the authenticity and confidentiality.
3. The authenticity and integrity of the Meter Data is verified by the Gateway.
4. If (and only if) authenticity and integrity have been verified successfully, the Meter Data is further processed by the Gateway according to the rules in the Processing Profile else the cryptographic information flow will be cancelled.
5. The processed Meter Data is encrypted and integrity protected using CMS (according to [TR-03109-1-I]) for the final recipient of the data²¹.
6. The processed Meter Data is signed using the services of the Security Module.
7. The processed and signed Meter Data may be stored for a certain amount of time.

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

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

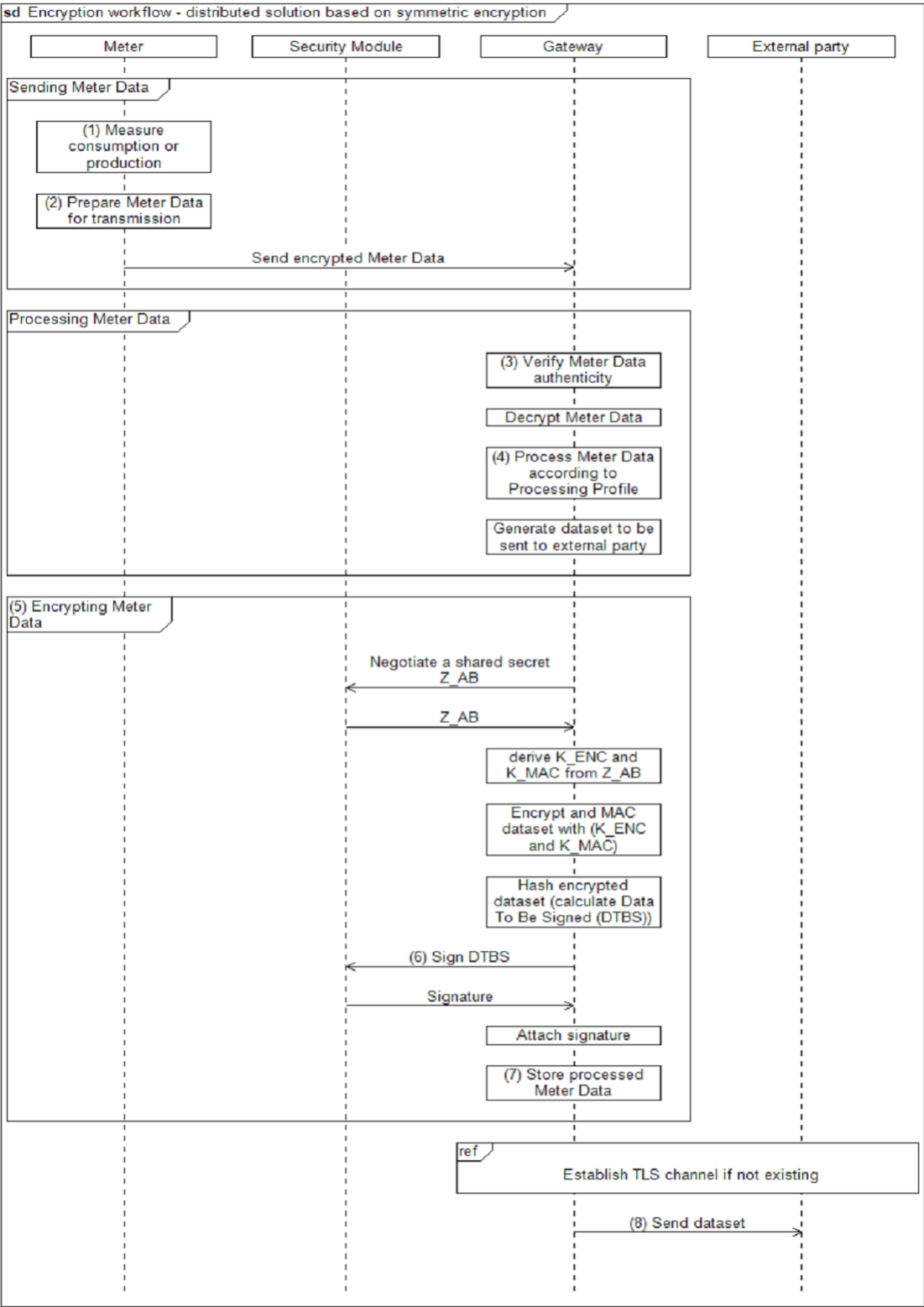


Figure 5: Cryptographic information flow for distributed Meters and Gateway

674 TOE life-cycle

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

- 676 1. Development
- 677 2. Production
- 678 3. Pre-personalization at the developer's premises (without Security Module)
- 679 4. Pre-personalization and integration of Security Module
- 680 5. Delivery to the MPO
- 681 6. Delivery by the MPO to the installation and operational environment
- 682 7. Installation and start of operation
- 683 8. Personalization
- 684 9. Normal operation

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

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

2 Conformance Claims

2.1 CC Conformance Claim

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

2.2 PP Claim / Conformance Statement

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

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 Package Claim

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

2.4 Conformance Claim Rationale

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

This Security Target is consistent to the TOE type according to [PP_GW] because the TOE is a communication Gateway that provides different external communication interfaces and enables the data communication between these interfaces and connected IT systems. It further collects processes, and stores Meter Data.

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

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

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

721

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 <i>user</i> or <i>external entity</i> serve as a hypernym for all entities mentioned before.

Table 5: Roles used in the Security Target

3.2 Assets

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

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

Asset	Description	Need for Protection
Meter Data	<p>Meter readings that allow calculation of the quantity of a commodity, e.g. electricity, gas, water or heat consumed over a period.</p> <p>Meter Data comprise Consumption or Production Data (billing-relevant) and grid status data (not billing-relevant).</p> <p>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.</p>	<ul style="list-style-type: none"> According to their specific need (see below)
System log data	<p>Log data from the</p> <ul style="list-style-type: none"> system log. 	<ul style="list-style-type: none"> Integrity Confidentiality (only authorised SMGW administrators and Service technicians may read the log data)
Consumer log data	<p>Log data from the</p> <ul style="list-style-type: none"> consumer log. 	<ul style="list-style-type: none"> Integrity Confidentiality (only authorised Consumers may read the log data)
Calibration log data	<p>Log data from the</p> <ul style="list-style-type: none"> calibration log. 	<ul style="list-style-type: none"> Integrity Confidentiality (only authorised SMGW administrators may read the log data)
Consumption Data	<p>Billing-relevant part of Meter Data. Please note that the term <i>Consumption Data</i> implicitly includes Production Data.</p>	<ul style="list-style-type: none"> Integrity and authenticity (comparable to the classical meter and its security requirements) Confidentiality (due to privacy concerns)

Status Data	Grid status data, subset of Meter Data that is not billing-relevant ²² .	<ul style="list-style-type: none"> Integrity and authenticity (comparable to the classical meter and its security requirements) Confidentiality (due to privacy concerns)
Supplementary Data	The Gateway may be used for communication purposes by devices in the LMN or HAN. It may be that the functionality of the Gateway that is used by such a device is limited to pure (but secure) communication services. Data that is transmitted via the Gateway but that does not belong to one of the aforementioned data types is named <i>Supplementary Data</i> .	<ul style="list-style-type: none"> According to their specific need
Data	The term <i>Data</i> is used as hypernym for <i>Meter Data and Supplementary Data</i> .	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Integrity Authenticity (when time is adjusted to an external reference time)
Personally Identifiable Information (PII)	Personally Identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.	<ul style="list-style-type: none"> Confidentiality

Table 6: Assets (User data)

Table 7 lists all assets typified as “TSF data”:

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

Asset	Description	Need for Protection
Meter config (secondary asset)	Configuration data of the Meter to control its behaviour including the Meter identity. Configuration data is transmitted to the Meter via the Gateway.	<ul style="list-style-type: none">• Integrity and authenticity• Confidentiality
Gateway config (secondary asset)	Configuration data of the Gateway to control its behaviour including the Gateway identity, the Processing Profiles and certificate/key material for authentication.	<ul style="list-style-type: none">• Integrity and authenticity• Confidentiality
CLS config (secondary asset)	Configuration data of a CLS to control its behaviour. Configuration data is transmitted to the CLS via the Gateway.	<ul style="list-style-type: none">• Integrity and authenticity• Confidentiality
Firmware update (secondary asset)	Firmware update that is downloaded by the TOE to update the firmware of the TOE.	<ul style="list-style-type: none">• Integrity and authenticity
Ephemeral keys (secondary asset)	Ephemeral cryptographic material used by the TOE for cryptographic operations.	<ul style="list-style-type: none">• Integrity and authenticity• Confidentiality

Table 7: Assets (TSF data)

3.3 Assumptions

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

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

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

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

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

A.Update It is assumed that firmware updates for the Gateway that can be provided by an authorised external entity have undergone a certification process according to this 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 LMN²³,
- if devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is appropriately protected.

A.Keygen

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

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-LK] 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].

²³ Please note that this assumption holds on a logical level rather than on a physical one. It may be possible that the Meters in the LMN have a physical connection to other devices that would in theory also allow a communication. This is specifically true for wireless communication technologies. It is further possible that signals of Meters are amplified by other devices or other Meters on the physical level without violating this assumption. However, it is assumed that the Meters do only communicate with the TOE and that only the TOE is able to decrypt the data sent by the Meter.

Application Note 2:

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

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

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

3.4 Threats

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

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

834 infrastructure (i.e. Meter, Gateway or Controllable Local System) via the WAN
835 to cause damage to a component itself or to the corresponding grid (e.g. by
836 sending forged Meter Data to an external entity).

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

842

843 **T.DataModificationLocal** A local attacker may try to modify (i.e. alter, delete, insert,
844 replay or redirect) Meter Data when transmitted between
845 Meter and Gateway, Gateway and Consumer, or Gateway
846 and external entities. The objective of the attacker may be
847 to alter billing-relevant information or grid status infor-
848 mation. The attacker may perform the attack via any inter-
849 face (LMN, HAN, or WAN).

850 In order to achieve the modification, the attacker may also
851 try to modify secondary assets like the firmware or config-
852 uration parameters of the Gateway.

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

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

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

865 **T.TimeModification** A local attacker or WAN attacker may try to alter the Gate-
866 way time. The motivation of the attacker could be e.g. to

867		change the relation between date/time and measured consumption or production values in the Meter Data records
868		(e.g. to influence the balance of the next invoice).
869		
870	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
871		when transmitted between Gateway and external entities in the WAN.
872		
873		
874		
875	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
876		Meters of more than one Consumer are served by one Gateway.
877		
878		
879		
880	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).
881		
882		
883		
884		
885		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.
886		
887	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).
888		
889		
890		
891		
892	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.
893		
894		
895		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.
896		
897		
898	T.Privacy	A WAN attacker may try to obtain more detailed information from the Gateway than actually required to fulfil the
899		

900 tasks defined by its role or the contract with the Consumer.
901 This includes scenarios in which an external entity that is
902 primarily authorised to obtain information from the TOE
903 tries to obtain more information than the information that
904 has been authorised as well as scenarios in which an at-
905 tacker who is not authorised at all tries to obtain infor-
906 mation.
907

3.5 Organizational Security Policies

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

OSP.SM

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

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

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

OSP.Log

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

1. A system log of relevant events in order to allow an authorised Gateway Administrator to analyse the status of the TOE. The TOE shall also analyse the system log automatically for a cumulation of security relevant events.
2. A consumer log that contains information about the information flows that have been initiated to the WAN and information about the Processing Profiles causing this information flow as well as the billing-relevant information.
3. A calibration log (as defined in chapter 6.2.1) that provides the Gateway Administrator with a possibility to review calibration relevant events.

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

1. Access to the information in the system log shall only be allowed for an authorised Gateway

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

2. Access to the information in the calibration log shall only be allowed for an authorised Gateway Administrator via the IF_GW_WAN interface of the TOE.
3. Access to the information in the consumer log shall only be allowed for an authorised Consumer via the IF_GW_CON interface of the TOE. The Consumer shall only have access to their own information.

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

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

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

4 Security Objectives

4.1 Security Objectives for the TOE

O.Firewall

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

The firewall:

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

O.SeparateIF

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

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

991	O.Conceal	To protect the privacy of its Consumers, the TOE shall con-
992		ceal the communication with external entities in the WAN
993		in order to ensure that no privacy-relevant information may
994		be obtained by analysing the frequency, load, size or the
995		absence of external communication. ²⁴
996	O.Meter	The TOE receives or polls information about the consump-
997		tion or production of different commodities from one or mul-
998		multiple Meters and is responsible for handling this Meter
999		Data.
1000		This includes that:
1001		• The TOE shall ensure that the communication to
1002		the Meter(s) is established in an Gateway Adminis-
1003		trator-definable interval or an interval as defined by
1004		the Meter,
1005		• the TOE shall enforce encryption and integrity pro-
1006		tection for the communication with the Meter ²⁵ ,
1007		• the TOE shall verify the integrity and authenticity of
1008		the data received from a Meter before handling it
1009		further,
1010		• the TOE shall process the data according to the
1011		definition in the corresponding Processing Profile,
1012		• the TOE shall encrypt the processed Meter Data for
1013		the final recipient, sign the data and
1014		• deliver the encrypted data to authorised external
1015		entities as defined in the corresponding Processing
1016		Profiles facilitating an encrypted channel,
1017		• the TOE shall store processed Meter Data if an ex-
1018		ternal entity cannot be reached and re-try to send

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

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

1019 the data until a configurable number of unsuccessful
 1020 retries has been reached,
 1021 • the TOE shall pseudonymize the data for parties
 1022 that do not need the relation between the processed
 1023 Meter Data and the identity of the Consumer.
 1024

1025 **O.Crypt**

1026 The TOE shall provide cryptographic functionality as follows:

- 1027 • authentication, integrity protection and encryption
- 1028 of the communication and data to external entities
- 1029 in the WAN,
- 1030 • authentication, integrity protection and encryption
- 1031 of the communication to the Meter,
- 1032 • authentication, integrity protection and encryption
- 1033 of the communication to the Consumer,
- 1034 • replay detection for all communications with external
- 1035 entities,
- 1036 • encryption of the persistently stored TSF and user
- 1037 data of the TOE²⁶.

1038 In addition, the TOE shall generate the required keys utilising
 1039 the services of its Security Module²⁷, ensure that the
 1040 keys are only used for an acceptable amount of time and
 1041 destroy ephemeral²⁸ keys if no longer needed.²⁹

1042 **O.Time**

1043 The TOE shall provide reliable time stamps and update
 1044 its internal clock in regular intervals by retrieving reliable
 1045 time information from a dedicated reliable source in the
 WAN.

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

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

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

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

1046	O.Protect	The TOE shall implement functionality to protect its security functions against malfunctions and tampering.
1047		
1048		Specifically, the TOE shall
1049		<ul style="list-style-type: none"> • encrypt its TSF and user data as long as it is not in use,
1050		
1051		<ul style="list-style-type: none"> • overwrite any information that is no longer needed to ensure that it is no longer available via the external interfaces of the TOE³⁰,
1052		
1053		
1054		<ul style="list-style-type: none"> • monitor user data and the TOE firmware for integrity errors,
1055		
1056		<ul style="list-style-type: none"> • contain a test that detects whether the interfaces for WAN and LAN are separate,
1057		
1058		<ul style="list-style-type: none"> • have a fail-safe design that specifically ensures that no malfunction can impact the delivery of a commodity (e.g. energy, gas, heat or water)³¹,
1059		
1060		
1061		<ul style="list-style-type: none"> • make any physical manipulation within the scope of the intended environment detectable for the Consumer and Gateway Administrator.
1062		
1063		
1064	O.Management	The TOE shall only provide authorised Gateway Administrators with functions for the management of the security features.
1065		
1066		
1067		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.
1068		
1069		
1070		
1071		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
1072		
1073		

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

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

1074		and that only authentic and integrity protected updates are
1075		applied.
1076	O.Log	The TOE shall maintain a set of log files as defined in [TR-
1077		03109-1] as follows:
1078		1. A system log of relevant events in order to allow an
1079		authorised Gateway Administrator or an authorised
1080		Service Technician to analyse the status of the
1081		TOE. The TOE shall also analyse the system log
1082		automatically for a cumulation of security relevant
1083		events.
1084		2. A consumer log that contains information about the
1085		information flows that have been initiated to the
1086		WAN and information about the Processing Profiles
1087		causing this information flow as well as the billing-
1088		relevant information and information about the sys-
1089		tem status (including relevant error messages).
1090		3. A calibration log that provides the Gateway Admin-
1091		istrator with a possibility to review calibration rele-
1092		vant events.
1093		The TOE shall further limit access to the information in the
1094		different log files as follows:
1095		1. Access to the information in the system log shall
1096		only be allowed for an authorised Gateway Admin-
1097		istrator via IF_GW_WAN or for an authorised Ser-
1098		vice Technician via IF_GW_SRV.
1099		2. Access to the information in the consumer log shall
1100		only be allowed for an authorised Consumer via the
1101		IF_GW_CON interface of the TOE and via a se-
1102		cured (i.e. confidentiality and integrity protected)
1103		connection. The Consumer shall only have access
1104		to their own information.
1105		3. Read-only access to the information in the calibra-
1106		tion log shall only be allowed for an authorised

1107 Gateway Administrator via the WAN interface of the
1108 TOE.

1109 The system log may overwrite the oldest events in case
1110 that the audit trail gets full.

1111 For the consumer log, the TOE shall ensure that a suffi-
1112 cient amount of events is available (in order to allow a Con-
1113 sumer to verify an invoice) but may overwrite older events
1114 in case that the audit trail gets full.

1115 For the calibration log however, the TOE shall ensure the
1116 availability of all events over the lifetime of the TOE.

1117 **O.Access** The TOE shall control the access of external entities in
1118 WAN, HAN or LMN to any information that is sent to, from
1119 or via the TOE via its external interfaces³². Access control
1120 shall depend on the destination interface that is used to
1121 send that information.

1122

1123 4.2 Security Objectives for the Operational Environment

1124 **OE.ExternalPrivacy** Authorised and authenticated external entities receiving
1125 any kind of private or billing-relevant data shall be trustwor-
1126 thy and shall not perform unauthorised analyses of these
1127 data with respect to the corresponding consumer(s).

1128 **OE.TrustedAdmins** The Gateway Administrator and the Service Technician
1129 shall be trustworthy and well-trained.

1130 **OE.PhysicalProtection** The TOE shall be installed in a non-public environment
1131 within the premises of the Consumer that provides a basic
1132 level of physical protection. This protection shall cover the
1133 TOE, the Meters that the TOE communicates with and the
1134 communication channel between the TOE and its Security

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

1135		Module. Only authorised individuals may physically access
1136		the TOE.
1137	OE.Profile	The Processing Profiles that are used when handling data
1138		shall be obtained from a trustworthy and reliable source
1139		only.
1140	OE.SM	The environment shall provide the services of a certified
1141		Security Module for
1142		<ul style="list-style-type: none">• verification of digital signatures,
1143		<ul style="list-style-type: none">• generation of digital signatures,
1144		<ul style="list-style-type: none">• key agreement,
1145		<ul style="list-style-type: none">• key transport,
1146		<ul style="list-style-type: none">• key storage,
1147		<ul style="list-style-type: none">• Random Number Generation.
1148		The Security Module used shall be certified according to
1149		[SecModPP] and shall be used in accordance with its rele-
1150		vant guidance documentation.
1151	OE.Update	The firmware updates for the Gateway that can be pro-
1152		vided by an authorised external entity shall undergo a cer-
1153		tification process according to this Security Target before
1154		they are issued to show that the update is implemented
1155		correctly. The external entity that is authorised to provide
1156		the update shall be trustworthy and ensure that no mal-
1157		ware is introduced via a firmware update.
1158	OE.Network	It shall be ensured that
1159		<ul style="list-style-type: none">• a WAN network connection with a sufficient reliabil-
1160		ity and bandwidth for the individual situation is
1161		available,
1162		<ul style="list-style-type: none">• one or more trustworthy sources for an update of
1163		the system time are available in the WAN,
1164		<ul style="list-style-type: none">• the Gateway is the only communication gateway for
1165		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-LK] is sufficient for MPOs to fulfill this security objective.

4.3 Security Objective Rationale

4.3.1 Overview

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

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access	OE.SM	OE.ExternalPrivacy	OE.TrustedAdmins	OE.PhysicalProtec-	OE.Profile	OE.Update	OE.Network	OE.Keygen	OE.Delivery
T.DataModification-Local				X	X		X	X					X	X					

T.DataModification-WAN	X				X		X	X					X						
T.TimeModification					X	X	X	X					X	X					
T.DisclosureWAN	X		X		X		X	X					X						
T.DisclosureLocal				X	X		X	X					X	X					
T.Infrastructure	X	X		X	X		X	X					X						
T.ResidualData							X	X					X						
T.ResidentData	X				X		X	X		X			X	X					
T.Privacy	X		X	X	X		X	X					X		X				
OSP.SM					X		X	X			X		X						
OSP.Log							X	X	X	X			X						
A.ExternalPrivacy												X							
A.TrustedAdmins													X						
A.PhysicalProtection														X					
A.ProcessProfile															X				
A.Update																X			
A.Network																	X		
A.Keygen																		X	
A.Delivery																			X

Table 8: Rationale for Security Objectives

4.3.2 Countering the threats

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

4.3.2.1 General objectives

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

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

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

4.3.2.2 T.DataModificationLocal

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

O.Meter defines that the TOE will enforce the encryption of communication when receiving Meter Data from the Meter. **O.Crypt** defines the required cryptographic functionality. The objectives together ensure that the communication between the Meter and the TOE cannot be modified or released.

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

4.3.2.3 T.DataModificationWAN

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

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

1221 4.3.2.4 T.TimeModification

1222 The threat **T.TimeModification** is countered by a combination of the security objectives
1223 **O.Time**, **O.Crypt** and **OE.PhysicalProtection**.

1224 **O.Time** defines that the TOE needs a reliable time stamp mechanism that is also up-
1225 dated from reliable sources regularly in the WAN. **O.Crypt** defines the required crypto-
1226 graphic functionality for the communication to external entities in the WAN. Therewith,
1227 O.Time and O.Crypt are the core objective to counter the threat T.TimeModification.

1228 **OE.PhysicalProtection** is of relevance as it ensures that access to the TOE is limited.

1229 4.3.2.5 T.DisclosureWAN

1230 The threat **T.DisclosureWAN** is countered by a combination of the security objectives
1231 **O.Firewall**, **O.Conceal** and **O.Crypt**.

1232 **O.Firewall** defines the connections for the devices within the LAN to external entities
1233 within the WAN and shall provide firewall functionality in order to protect the devices of
1234 the LMN and HAN (as long as they use the Gateway) and itself against threats from the
1235 WAN side. **O.Crypt** defines the required cryptographic functionality. Both objectives to-
1236 gether ensure that the communication between the Meter and the TOE cannot be dis-
1237 closed.

1238 **O.Conceal** ensures that no information can be disclosed based on additional character-
1239 istics of the communication like frequency, load or the absence of a communication.

1240 4.3.2.6 T.DisclosureLocal

1241 The threat **T.DisclosureLocal** is countered by a combination of the security objectives
1242 **O.Meter**, **O.Crypt** and **OE.PhysicalProtection**.

1243 **O.Meter** defines that the TOE will enforce the encryption and integrity protection of com-
1244 munication when polling or receiving Meter Data from the Meter. **O.Crypt** defines the
1245 required cryptographic functionality. Both objectives together ensure that the communi-
1246 cation between the Meter and the TOE cannot be disclosed.

1247 **OE.PhysicalProtection** is of relevance as it ensures that access to the TOE is limited.

1248 4.3.2.7 T.Infrastructure

1249 The threat **T.Infrastructure** is countered by a combination of the security objectives
1250 **O.Firewall**, **O.SeparateIF**, **O.Meter** and **O.Crypt**.

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

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

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

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

4.3.2.8 T.ResidualData

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

4.3.2.9 T.ResidentData

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

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

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

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

4.3.2.10 T.Privacy

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

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

4.3.3 Coverage of organisational security policies

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

4.3.3.1 OSP.SM

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

4.3.3.2 OSP.Log

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

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

4.3.4 Coverage of assumptions

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

4.3.4.1 A.ExternalPrivacy

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

1313 4.3.4.2 A.TrustedAdmins

1314 The assumption **A.TrustedAdmins** is directly and completely covered by the security
1315 objective **OE.TrustedAdmins**. The assumption and the objective for the environment
1316 are drafted in a way that the correspondence is obvious.

1317 4.3.4.3 A.PhysicalProtection

1318 The assumption **A.PhysicalProtection** is directly and completely covered by the secu-
1319 rity objective **OE.PhysicalProtection**. The assumption and the objective for the envi-
1320 ronment are drafted in a way that the correspondence is obvious.

1321 4.3.4.4 A.ProcessProfile

1322 The assumption **A.ProcessProfile** is directly and completely covered by the security
1323 objective **OE.Profile**. The assumption and the objective for the environment are drafted
1324 in a way that the correspondence is obvious.

1325 4.3.4.5 A.Update

1326 The assumption **A.Update** is directly and completely covered by the security objective
1327 **OE.Update**. The assumption and the objective for the environment are drafted in a way
1328 that the correspondence is obvious.

1329 4.3.4.6 A.Network

1330 The assumption **A.Network** is directly and completely covered by the security objective
1331 **OE.Network**. The assumption and the objective for the environment are drafted in a way
1332 that the correspondence is obvious.

1333 4.3.4.7 A.Keygen

1334 The assumption **A.Keygen** is directly and completely covered by the security objective
1335 **OE.Keygen**. The assumption and the objective for the environment are drafted in a way
1336 that the correspondence is obvious.

1337 4.3.4.8 A.Delivery

1338 The assumption **A.Delivery** is directly and completely covered by the security objective
1339 **OE.Delivery**. The assumption and the objective for the environment are drafted in a way
1340 that the correspondence is obvious.

1341

5 Extended Component definition

5.1 Communication concealing (FPR_CON)

The additional family Communication concealing (FPR_CON) of the Class FPR (Privacy) is defined here to describe the specific IT security functional requirements of the TOE. The TOE shall prevent attacks against Personally Identifiable Information (PII) of the Consumer that may be obtained by an attacker by observing the encrypted communication of the TOE with remote entities.

5.2 Family behaviour

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

5.3 Component levelling

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

5.4 Management

- The following actions could be considered for the management functions in FMT:
- a. Definition of the interval in FPR_CON.1.2 if definable within the operational phase of the TOE.

5.5 Audit

There are no auditable events foreseen.

5.6 Communication concealing (FPR_CON.1)

- | | |
|------------------|----------------------|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |

1370	FPR_CON.1.1	The TSF shall enforce the [assignment: <i>information</i>
1371		<i>flow policy</i>] in order to ensure that no personally iden-
1372		tifiable information (PII) can be obtained by an analysis
1373		of [assignment: <i>characteristics of the information flow</i>
1374		<i>that need to be concealed</i>].
1375	FPR_CON.1.2	The TSF shall connect to [assignment: <i>list of external</i>
1376		<i>entities</i>] in intervals as follows [selection: <i>weekly,</i>
1377		<i>daily, hourly, [assignment: other interval]</i>] to conceal
1378		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

1399

Table 9: List of Security Functional Requirements

1400 **6.2 Class FAU: Security Audit**

1401 **6.2.1 Introduction**

1402 The TOE compliant to this Security Target shall implement three different audit logs as
1403 defined in **OSP.Log** and **O.Log**. The following table provides an overview over the three
1404 audit logs before the following chapters introduce the SFRs related to those audit logs.

	System-Log	Consumer-Log	Calibration-Log
Purpose	<ul style="list-style-type: none">• Inform the Gateway Administrator about security relevant events• Log all events as defined by Common Criteria [CC] for the used SFR• Log all system relevant events on specific functionality• Automated alarms in case of a cumulation of certain events• Inform the Service Technician about the status of the Gateway	<ul style="list-style-type: none">• Inform the Consumer about all information flows to the WAN• Inform the Consumer about the Processing Profiles• Inform the Consumer about other metering data (not billing-relevant)• Inform the Consumer about all billing-relevant data needed to verify an invoice	<ul style="list-style-type: none">• Track changes that are relevant for the calibration of the TOE relevant data needed to verify an invoice
Data	<ul style="list-style-type: none">• As defined by CC part 2• Augmented by specific events for the security functions	<ul style="list-style-type: none">• Information about all information flows to the WAN• Information about the current and the previous Processing Profiles• Non-billing-relevant Meter Data• Information about the system status (including relevant errors)	<ul style="list-style-type: none">• Calibration relevant data only

		<ul style="list-style-type: none"> Billing-relevant data needed to verify an invoice 	
Access	<ul style="list-style-type: none"> Access by authorised Gateway Administrator and via IF_GW_WAN only Events may only be deleted by an authorised Gateway Administrator via IF_GW_WAN Read access by authorised Service Technician via IF_GW_SRV only 	<ul style="list-style-type: none"> Read access by authorised Consumer and via IF_GW_CON only to the data related to the current consumer 	<ul style="list-style-type: none"> Read access by authorised Gateway Administrator and via IF_GW_WAN only
Deletion	<ul style="list-style-type: none"> Ring buffer. The availability of data has to be ensured for a sufficient amount of time Overwriting old events is possible if the memory is full. 	<ul style="list-style-type: none"> Ring buffer. The availability of data has to be ensured for a sufficient amount of time. Overwriting old events is possible if the memory is full Retention period is set by authorised Gateway Administrator on request by consumer, data older than this are deleted. 	<ul style="list-style-type: none"> The availability of data has to be ensured over the lifetime of the TOE.

1405

Table 10: Overview over audit processes

1406	6.2.2 Security Requirements for the System Log	
1407	6.2.2.1 Security audit automatic response (FAU_ARP)	
1408	6.2.2.1.1 FAU_ARP.1/SYS: Security Alarms for system log	
1409	FAU_ARP.1.1/SYS	The TSF shall take <i>inform an authorised Gateway Administrator and create a log entry in the system log</i> ³³
1410		upon detection of a potential security violation.
1411		
1412	Hierarchical to:	No other components
1413	Dependencies:	FAU_SAA.1 Potential violation analysis
1414		
1415	6.2.2.2 Security audit data generation (FAU_GEN)	
1416	6.2.2.2.1 FAU_GEN.1/SYS: Audit data generation for system log	
1417	FAU_GEN.1.1/SYS	The TSF shall be able to generate an audit record of the
1418		following auditable events:
1419		a) Start-up and shutdown of the audit functions;
1420		b) All auditable events for the <u>basic</u> ³⁴ level of audit; and
1421		c) <i>other non privacy relevant auditable events: none</i> ³⁵ .
1422	FAU_GEN.1.2/SYS	The TSF shall record within each audit record at least the
1423		following information:
1424		a) Date and time of the event, type of event, subject identity
1425		(if applicable), and the outcome (success or failure) of the
1426		event; and
1427		b) For each audit event type, based on the auditable event
1428		definitions of the functional components included in the
1429		PP/ST ³⁶ , <i>other audit relevant information: none</i> ³⁷ .

33 [assignment: *list of actions*]

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

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

36 [refinement: *PP/ST*]

37 [assignment: *other audit relevant information*]

1430	Hierarchical to:	No other components
1431	Dependencies:	FPT_STM.1
1432	6.2.2.3 Security audit analysis (FAU_SAA)	
1433	6.2.2.3.1 FAU_SAA.1/SYS: Potential violation analysis for system	
1434	log	
1435	FAU_SAA.1.1./SYS	The TSF shall be able to apply a set of rules in monitoring
1436		the audited events and based upon these rules indicate a
1437		potential violation of the enforcement of the SFRs.
1438	FAU_SAA.1.2/SYS	The TSF shall enforce the following rules for monitoring
1439		audited events:
1440		a) Accumulation or combination of
1441		<ul style="list-style-type: none"> • <i>Start-up and shutdown of the audit functions</i>
1442		<ul style="list-style-type: none"> • <i>all auditable events for the basic level of audit</i>
1443		<ul style="list-style-type: none"> • <i>all types of failures in the TSF as listed in</i>
1444		<i>FPT_FLS.1</i> ³⁸
1445		known to indicate a potential security violation.
1446		b) <i>any other rules: none</i> ³⁹ .
1447	Hierarchical to:	No other components
1448	Dependencies:	FAU_GEN.1
1449	6.2.2.4 Security audit review (FAU_SAR)	
1450	6.2.2.4.1 FAU_SAR.1/SYS: Audit Review for system log	
1451	FAU_SAR.1.1/SYS	The TSF shall provide <i>only authorised Gateway</i>
1452		<i>Administrators via the IF_GW_WAN interface and</i>
1453		<i>authorised Service Technicians via the IF_GW_SRV</i>

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

³⁹ [assignment: *any other rules*]

1454		<i>interface</i> ⁴⁰ with the capability to read all information ⁴¹
1455		from the system audit records ⁴² .
1456	FAU_SAR.1.2/SYS	The TSF shall provide the audit records in a manner
1457		suitable for the user to interpret the information.
1458	Hierarchical to:	No other components
1459	Dependencies:	FAU_GEN.1
1460	6.2.2.5 Security audit event storage (FAU_STG)	
1461	6.2.2.5.1 FAU_STG.4/SYS: Prevention of audit data loss for	
1462	systemlog	
1463	FAU_STG.4.1/SYS	The TSF shall <u>overwrite the oldest stored audit records</u> ⁴³
1464		and other actions to be taken in case of audit storage
1465		failure: none ⁴⁴ if the system audit trail ⁴⁵ is full.
1466	Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
1467	Dependencies:	FAU_STG.1 Protected audit trail storage
1468	Application Note 4:	The size of the audit trail that is available before the oldest
1469		events get overwritten is configurable for the Gateway
1470		Administrator.

⁴⁰ [assignment: *authorised users*]

⁴¹ [assignment: *list of audit information*]

⁴² [refinement: *audit records*]

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

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

⁴⁵ [refinement: *audit trail*]

1471	6.2.3 Security Requirements for the Consumer Log	
1472	6.2.3.1 Security audit data generation (FAU_GEN)	
1473	6.2.3.1.1 FAU_GEN.1/CON: Audit data generation for consumer log	
1474	FAU_GEN.1.1/CON	The TSF shall be able to generate an audit record of the
1475		following auditable events:
1476		a) Start-up and shutdown of the audit functions;
1477		b) All auditable events for the <u>not specified</u> ⁴⁶ level of audit;
1478		and
1479		c) <i>all audit events as listed in Table 11 and additional</i>
1480		<i>events: none</i> ⁴⁷ .
1481	FAU_GEN.1.2/CON	The TSF shall record within each audit record at least the
1482		following information:
1483		a) Date and time of the event, type of event, subject identity
1484		(if applicable), and the outcome (success or failure) of the
1485		event; and
1486		b) For each audit event type, based on the auditable event
1487		definitions of the functional components included in the
1488		PP/ST ⁴⁸ , <i>additional information as listed in Table 11 and</i>
1489		<i>additional events: none</i> ⁴⁹ .
1490	Hierarchical to:	No other components
1491	Dependencies:	FPT_STM.1
1492		

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

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

⁴⁸ [refinement: *PP/ST*]

⁴⁹ [assignment: *other audit relevant information*]

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

Table 11: Events for consumer log

6.2.3.2 Security audit review (FAU_SAR)

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

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

⁵⁰ [assignment: *authorised users*]

1499		<i>information that are related to them</i> ⁵¹ from the consumer
1500		audit records ⁵² .
1501	FAU_SAR.1.2/CON	The TSF shall provide the audit records in a manner
1502		suitable for the user to interpret the information.
1503	Hierarchical to:	No other components
1504	Dependencies:	FAU_GEN.1
1505	Application Note 5:	FAU_SAR.1.2/CON shall ensure that the Consumer is
1506		able to interpret the information that is provided to him in a
1507		way that allows him to verify the invoice.
1508	6.2.3.3 Security audit event storage (FAU_STG)	
1509	6.2.3.3.1 FAU_STG.4/CON: Prevention of audit data loss for the	
1510	consumer log	
1511	FAU_STG.4.1/CON	The TSF shall <u>overwrite the oldest stored audit records</u> and
1512		<i>interrupt metrological operation in case that the oldest</i>
1513		<i>audit record must still be kept for billing verification</i> ⁵³ if the
1514		consumer audit trail is full.
1515	Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
1516	Dependencies:	FAU_STG.1 Protected audit trail storage
1517	Application Note 6:	The size of the audit trail that is available before the oldest
1518		events get overwritten is configurable for the Gateway
1519		Administrator.

⁵¹ [assignment: *list of audit information*]

⁵² [refinement: *audit records*]

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

1520	6.2.4 Security Requirements for the Calibration Log	
1521	6.2.4.1 Security audit data generation (FAU_GEN)	
1522	6.2.4.1.1 FAU_GEN.1/CAL: Audit data generation for calibration log	
1523	FAU_GEN.1.1/CAL	The TSF shall be able to generate an audit record of the
1524		following auditable events:
1525		a) Start-up and shutdown of the audit functions;
1526		b) All auditable events for the <u>not specified</u> ⁵⁴ level of audit;
1527		and
1528		c) <i>all calibration-relevant information according to Table</i>
1529		<i>12</i> ⁵⁵ .
1530	FAU_GEN.1.2/CAL	The TSF shall record within each audit record at least the
1531		following information:
1532		a) Date and time of the event, type of event, subject identity
1533		(if applicable), and the outcome (success or failure) of the
1534		event; and
1535		b) For each audit event type, based on the auditable event
1536		definitions of the functional components included in the
1537		PP/ST ⁵⁶ , <i>other audit relevant information: none</i> ⁵⁷ .
1538	Hierarchical to:	No other components
1539	Dependencies:	FPT_STM.1
1540	Application Note 7:	The calibration log serves to fulfil national requirements in
1541		the context of the calibration of the TOE.
1542		

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

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

⁵⁶ [refinement: *PP/ST*]

⁵⁷ [assignment: *other audit relevant information*]

Event / Parameter	Content
Commissioning	Commissioning of the SMGW MUST be logged in calibration log.
Event of self-test	Initiation of self-test MUST be logged in calibration log.
New meter	Connection and registration of a new meter MUST be logged in calibration log.
Meter removal	Removal of a meter from SMGW MUST be logged in calibration log.
Change of tarification profiles	<p>Every change (incl. parameter change) of a tarification profile according to [TR-03109-1, 4.4], provided the parameter is relevant for calibration regulations (see below) as well as new storage or removal of tarification profiles MUST be logged in calibration log.</p> <p>Parameter relevant for calibration regulations are:</p> <ul style="list-style-type: none"> • Device-ID of a meter - Unique identifier of the meter, which send the input values for a TAF • OBIS value of the measured variable of the meter - Unique value for the measured variable of the meter for the used TAF • Metering point name - Unique name of the metering point • Billing period - Period in which a billing should be done • Consumer ID • Validity period - Period for which the TAF is booked • Definition of tariff stages - Defines different tariff stages and associated OBIS values. Here it will be defined which tariff stage is valid at the time of rule set activation • Tariff switching time - Defines to the split second the switching of tariff stages. The time points can be defined as periodic values • Register period - Time distance of two consecutive measured value acquisitions for meter readings

Change of meter profiles	<p>Every change (incl. parameter change) of a meter profile according to [TR-03109-1, 4.4], provided the parameter is relevant for calibration regulations (see below) as well as new storage or removal of meter profiles MUST be logged in calibration log.</p> <p>Parameter relevant for legal metrology are:</p> <ul style="list-style-type: none"> • Device-ID - Unique identifier of the meter according to DIN 43863-5 • Key material - Public key for inner signature (dependent on the used meter in LMN) • Register period - Interval during receipt of meter values • Displaying interval ('Anzeigeintervall') - Interval during which the actual meter value (only during display) must be updated in case of bidirectional communication between meter and SMGW • Balancing ('Saldierend') - Determines if the meter is balancing ('saldierend') and meter values can grow and fall • OBIS values - OBIS values according to IEC-62056-6-1 resp. EN 13757-1 • Converter factor ('Wandlerfaktor') - Value is 1 in case of directly connected meter. In usage of converter counter ('Wandlerzähler') the value may be different.
Software update	Every update of the code which touches calibration regulations (serialized COSEM-objects, rules) MUST be logged in calibration log.
Firmware update	Every firmware update (incl. operating system update if applicable) MUST be logged in calibration log.
Error messages of a meter	<p>All FATAL messages of a connected meter MUST be logged in calibration log according to</p> <p>0 - no error</p> <p>1 - Warning, no action to be done according to calibration authority, meter value valid</p>

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

1543 **Table 12: Content of calibration log**

1544

1545	6.2.4.2 Security audit review (FAU_SAR)	
1546	6.2.4.2.1 FAU_SAR.1/CAL: Audit Review for the calibration log	
1547	FAU_SAR.1.1/CAL	The TSF shall provide <i>only authorised Gateway</i>
1548		<i>Administrators via the IF_GW_WAN interface</i> ⁵⁸ with the
1549		capability to read <i>all information</i> ⁵⁹ from the calibration
1550		audit records ⁶⁰ .
1551	FAU_SAR.1.2/CAL	The TSF shall provide the audit records in a manner
1552		suitable for the user to interpret the information.
1553	Hierarchical to:	No other components
1554	Dependencies:	FAU_GEN.1
1555	6.2.4.3 Security audit event storage (FAU_STG)	
1556	6.2.4.3.1 FAU_STG.4/CAL: Prevention of audit data loss for	
1557	calibration log	
1558	FAU_STG.4.1/CAL	The TSF shall <u>ignore audited events</u> ⁶¹ and <i>stop the</i>
1559		<i>operation of the TOE and inform a Gateway</i>
1560		<i>Administrator</i> ⁶² if the calibration audit trail ⁶³ is full.
1561	Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
1562	Dependencies:	FAU_STG.1 Protected audit trail storage
1563	Application Note 8:	As outlined in the introduction it has to be ensured that the
1564		events of the calibration log are available over the lifetime
1565		of the TOE.

58 [assignment: *authorised users*]

59 [assignment: *list of audit information*]

60 [refinement: *audit records*]

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

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

63 [refinement: *audit trail*]

1566	6.2.5 Security Requirements that apply to all logs	
1567	6.2.5.1 Security audit data generation (FAU_GEN)	
1568	6.2.5.1.1 FAU_GEN.2: User identity association	
1569	FAU_GEN.2.1	For audit events resulting from actions of identified users,
1570		the TSF shall be able to associate each auditable event
1571		with the identity of the user that caused the event.
1572	Hierarchical to:	No other components
1573	Dependencies:	FAU_GEN.1
1574		FIA_UID.1
1575	Application Note 9:	Please note that FAU_GEN.2 applies to all audit logs, the
1576		system log, the calibration log, and the consumer log.

1577	6.2.5.2 Security audit event storage (FAU_STG)	
1578	6.2.5.2.1 FAU_STG.2: Guarantees of audit data availability	
1579	FAU_STG.2.1	The TSF shall protect the stored audit records in the all
1580		audit trails ⁶⁴ from unauthorised deletion.
1581	FAU_STG.2.2	The TSF shall be able to <u>prevent</u> ⁶⁵ unauthorised
1582		modifications to the stored audit records in the all audit
1583		trails ⁶⁶ .
1584	FAU_STG.2.3	The TSF shall ensure that <i>all</i> ⁶⁷ stored audit records will be
1585		maintained when the following conditions occur: <u>audit</u>
1586		<u>storage exhaustion or failure</u> ⁶⁸ .
1587	Hierarchical to:	FAU_STG.1 Protected audit trail storage
1588	Dependencies:	FAU_GEN.1
1589	Application Note 10:	Please note that FAU_STG.2 applies to all audit logs, the
1590		system log, the calibration log, and the consumer log.

⁶⁴ [refinement: *audit trail*]

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

⁶⁶ [refinement: *audit trail*]

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

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

6.3 Class FCO: Communication

6.3.1 Non-repudiation of origin (FCO_NRO)

6.3.1.1 FCO_NRO.2: Enforced proof of origin

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

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

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to recipient, Consumer⁷³ given *limitations of the digital signature according to TR-03109-1*⁷⁴.

Hierarchical to: FCO_NRO.1 Selective proof of origin

Dependencies: FIA_UID.1 Timing of identification

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

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

⁶⁹ [assignment: *list of information types*]

⁷⁰ [assignment: *list of attributes*]

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

⁷² [assignment: *list of information fields*]

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

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

6.4 Class FCS: Cryptographic Support

6.4.1 Cryptographic support for TLS

6.4.1.1 Cryptographic key management (FCS_CKM)

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

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

Hierarchical to: No other components.

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

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

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

6.4.1.2 Cryptographic operation (FCS_COP)

6.4.1.2.1 FCS_COP.1/TLS: Cryptographic operation for TLS

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

⁷⁵ [assignment: *key generation algorithm*]
⁷⁶ [assignment: *cryptographic key sizes*]
⁷⁷ [assignment: *list of standards*]
⁷⁸ [assignment: *list of cryptographic operations*]

1637 *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,*
 1638 *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,*
 1639 *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,*
 1640 *and*
 1641 *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
 1642 ⁷⁹ *using elliptic curves BrainpoolP256r1, BrainpoolP384r1,*
 1643 *BrainpoolP512r1 (according to [RFC 5639]), NIST P-256,*
 1644 *and NIST P-384 (according to [RFC 5114]) and*
 1645 *cryptographic key sizes 128 bit or 256 bit* ⁸⁰ *that meet the*
 1646 *following: [RFC 2104], [RFC 5114], [RFC 5246],*
 1647 *[RFC 5289], [RFC 5639], [NIST 800-38A], and [NIST 800-*
 1648 *38D]* ⁸¹.

1649 Hierarchical to: No other components.

1650 Dependencies: [FDP_ITC.1 Import of user data without security attributes,
 1651 or

1652 FDP_ITC.2 Import of user data with security attributes, or

1653 FCS_CKM.1 Cryptographic key generation], fulfilled by

1654 FCS_CKM.1/TLS

1655 FCS_CKM.4 Cryptographic key destruction

1656 **Application Note 14:** The TOE uses only cryptographic specifications and
 1657 algorithms as described in [TR-03109-3].

1658 **6.4.2 Cryptographic support for CMS**

1659 6.4.2.1 Cryptographic key management (FCS_CKM)

1660 **6.4.2.1.1 FCS_CKM.1/CMS: Cryptographic key generation for CMS**

1661 FCS_CKM.1.1/CMS The TSF shall generate cryptographic keys in accordance
 1662 with a specified cryptographic key generation algorithm
 1663 *ECKA-EG* ⁸² and specified cryptographic key sizes 128

79 [assignment: *cryptographic algorithm*]

80 [assignment: *cryptographic key sizes*]

81 [assignment: *list of standards*]

82 [assignment: *cryptographic key generation algorithm*]

1664		<i>bit</i> ⁸³ that meet the following: [X9.63] in combination with
1665		[RFC 3565] ⁸⁴ .
1666	Hierarchical to:	No other components.
1667	Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or
1668		FCS_COP.1 Cryptographic operation], fulfilled by
1669		FCS_COP.1/CMS
1670		FCS_CKM.4 Cryptographic key destruction
1671	Application Note 15:	The TOE utilises the services of its Security Module for the
1672		generation of random numbers and for all cryptographic
1673		operations with the private asymmetric key of a CMS cer-
1674		tificate.
1675	Application Note 16:	The TOE uses only cryptographic specifications and
1676		algorithms as described in [TR-03109-3].
1677	6.4.2.2 Cryptographic operation (FCS_COP)	
1678	6.4.2.2.1 FCS_COP.1/CMS: Cryptographic operation for CMS	
1679	FCS_COP.1.1/CMS	The TSF shall perform
1680		<i>symmetric encryption, decryption and integrity protection</i>
1681		in accordance with a specified cryptographic algorithm
1682		<i>AES-CBC-CMAC or AES-GCM</i> ⁸⁵ and cryptographic key
1683		sizes <i>128 bit</i> ⁸⁶ that meet the following: [FIPS Pub. 197],

83 [assignment: *cryptographic key sizes*]
84 [assignment: *list of standards*]
85 [assignment: *list of cryptographic operations*]
86 [assignment: *cryptographic key sizes*]

1684		<i>[NIST 800-38D], [RFC 4493], [RFC 5084], and [RFC 5652]</i>
1685		<i>in combination with [NIST 800-38A]⁸⁷.</i>
1686	Hierarchical to:	No other components.
1687	Dependencies:	[FDP_ITC.1 Import of user data without security attributes,
1688		or
1689		FDP_ITC.2 Import of user data with security attributes, or
1690		FCS_CKM.1 Cryptographic key generation], fulfilled by
1691		FCS_CKM.1/CMS
1692		FCS_CKM.4 Cryptographic key destruction
1693	Application Note 17:	The TOE uses only cryptographic specifications and
1694		algorithms as described in [TR-03109-3].
1695	6.4.3 Cryptographic support for Meter communication encryption	
1696	6.4.3.1 Cryptographic key management (FCS_CKM)	
1697	6.4.3.1.1 FCS_CKM.1/MTR: Cryptographic key generation for Meter	
1698	communication (symmetric encryption)	
1699	FCS_CKM.1.1/MTR	The TSF shall generate cryptographic keys in accordance
1700		with a specified cryptographic key generation algorithm
1701		AES-CMAC ⁸⁸ and specified cryptographic key sizes 128
1702		bit ⁸⁹ that meet the following: <i>[FIPS Pub. 197], and</i>
1703		<i>[RFC 4493]⁹⁰.</i>
1704	Hierarchical to:	No other components.
1705	Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or
1706		FCS_COP.1 Cryptographic operation], fulfilled by
1707		FCS_COP.1/MTR
1708		FCS_CKM.4 Cryptographic key destruction

87 [assignment: *list of standards*]

88 [assignment: *cryptographic key generation algorithm*]

89 [assignment: *cryptographic key sizes*]

90 [assignment: *list of standards*]

1709	Application Note 18:	The TOE uses only cryptographic specifications and
1710		algorithms as described in [TR-03109-3].
1711	6.4.3.2 Cryptographic operation (FCS_COP)	
1712	6.4.3.2.1 FCS_COP.1/MTR: Cryptographic operation for Meter	
1713	communication encryption	
1714	FCS_COP.1.1/MTR	The TSF shall perform symmetric encryption, decryption,
1715		integrity protection ⁹¹ in accordance with a specified
1716		cryptographic algorithm AES-CBC-CMAC ⁹² and
1717		cryptographic key sizes 128 bit ⁹³ that meet the following:
1718		[FIPS Pub. 197] and [RFC 4493] in combination with
1719		[ISO 10116] ⁹⁴ .
1720	Hierarchical to:	No other components.
1721	Dependencies:	[FDP_ITC.1 Import of user data without security attributes,
1722		or
1723		FDP_ITC.2 Import of user data with security attributes, or
1724		FCS_CKM.1 Cryptographic key generation], fulfilled by
1725		FCS_CKM.1/MTR
1726		FCS_CKM.4 Cryptographic key destruction
1727	Application Note 19:	The ST allows different scenarios of key generation for
1728		Meter communication encryption. Those are:
1729		1. If a TLS encryption is being used, the key
1730		generation/negotiation is as defined by
1731		FCS_CKM.1/TLS.
1732		2. If AES encryption is being used, the key has been
1733		brought into the Gateway via a management
1734		function during the pairing process for the Meter

91 [assignment: *list of cryptographic operations*]
92 [assignment: *cryptographic algorithm*]
93 [assignment: *cryptographic key sizes*]
94 [assignment: *list of standards*]

1735 (see FMT_SMF.1) as defined by
1736 FCS_COP.1/MTR.

1737 **Application Note 20:** If the connection between the Meter and TOE is
1738 unidirectional, the communication between the Meter and
1739 the TOE is secured by the use of a symmetric AES
1740 encryption. If a bidirectional connection between the Meter
1741 and the TOE is established, the communication is secured
1742 by a TLS channel as described in chapter 6.4.1. As the
1743 TOE shall be interoperable with all kind of Meters, both
1744 kinds of encryption are implemented.

1745 **Application Note 21:** The TOE uses only cryptographic specifications and
1746 algorithms as described in [TR-03109-3].

1747 **6.4.4 General Cryptographic support**

1748 6.4.4.1 Cryptographic key management (FCS_CKM)

1749 **6.4.4.1.1 FCS_CKM.4: Cryptographic key destruction**

1750 FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance
1751 with a specified cryptographic key destruction method
1752 *Zeroisation*⁹⁵ that meets the following: *none*⁹⁶.

1753 Hierarchical to: No other components.

1754 Dependencies: [FDP_ITC.1 Import of user data without security attributes,
1755 or

1756 FDP_ITC.2 Import of user data with security attributes, or
1757 FCS_CKM.1 Cryptographic key generation], fulfilled by
1758 FCS_CKM.1/TLS and

1759 FCS_CKM.1/CMS and FCS_CKM.1/MTR

1760 **Application Note 22:** Please note that as against the requirement FDP_RIP.2,
1761 the mechanisms implementing the requirement from
1762 FCS_CKM.4 shall be suitable to avoid attackers with

95 [assignment: *cryptographic key destruction method*]

96 [assignment: *list of standards*]

1763 physical access to the TOE from accessing the keys after
 1764 they are no longer used.

1765 6.4.4.2 Cryptographic operation (FCS_COP)

1766 **6.4.4.2.1 FCS_COP.1/HASH: Cryptographic operation, hashing for**
 1767 **signatures**

1768 FCS_COP.1.1/HASH The TSF shall perform *hashing for signature creation and*
 1769 *verification*⁹⁷ in accordance with a specified cryptographic
 1770 algorithm *SHA-256, SHA-384 and SHA-512*⁹⁸ and
 1771 cryptographic key sizes *none*⁹⁹ that meet the following:
 1772 *[FIPS Pub. 180-4]*¹⁰⁰.

1773 Hierarchical to: No other components.

1774 Dependencies: [FDP_ITC.1 Import of user data without security attributes,
 1775 or

1776 FDP_ITC.2 Import of user data with security attributes, or

1777 FCS_CKM.1 Cryptographic key generation¹⁰¹

1778 FCS_CKM.4 Cryptographic key destruction

1779 **Application Note 23:** The TOE is only responsible for hashing of data in the
 1780 context of digital signatures. The actual signature
 1781 operation and the handling (i.e. protection) of the
 1782 cryptographic keys in this context is performed by the
 1783 Security Module.

1784 **Application Note 24:** The TOE uses only cryptographic specifications and
 1785 algorithms as described in [TR-03109-3].

97 [assignment: *list of cryptographic operations*]

98 [assignment: *cryptographic algorithm*]

99 [assignment: *cryptographic key sizes*]

100 [assignment: *list of standards*]

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

1786	6.4.4.2.2	<i>FCS_COP.1/MEM: Cryptographic operation, encryption of</i>
1787		<i>TSF and user data</i>
1788	FCS_COP.1.1/MEM	The TSF shall perform <i>TSF and user data encryption and</i>
1789		<i>decryption</i> ¹⁰² in accordance with a specified cryptographic
1790		algorithm <i>AES-XTS</i> ¹⁰³ and cryptographic key sizes <i>128</i>
1791		<i>bit</i> ¹⁰⁴ that meet the following: <i>[FIPS Pub. 197]</i> and
1792		<i>[NIST 800-38E]</i> ¹⁰⁵ .
1793	Hierarchical to:	No other components.
1794	Dependencies:	[FDP_ITC.1 Import of user data without security attributes,
1795		or
1796		FDP_ITC.2 Import of user data with security attributes, or
1797		FCS_CKM.1 Cryptographic key generation], not fulfilled s.
1798		Application Note 25
1799		FCS_CKM.4 Cryptographic key destruction
1800	Application Note 25:	Please note that for the key generation process an external
1801		security module is used during TOE production.
1802	Application Note 26:	The TOE encrypts its local TSF and user data while it is
1803		not in use (i.e. while stored in a persistent memory).
1804		It shall be noted that this kind of encryption cannot provide
1805		an absolute protection against physical manipulation and
1806		does not aim to. It however contributes to the security
1807		concept that considers the protection that is provided by
1808		the environment.

¹⁰² [assignment: *list of cryptographic operations*]

¹⁰³ [assignment: *cryptographic algorithm*]

¹⁰⁴ [assignment: *cryptographic key sizes*]

¹⁰⁵ [assignment: *list of standards*]

6.5 Class FDP: User Data Protection

6.5.1 Introduction to the Security Functional Policies

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

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

6.5.2 Gateway Access SFP

6.5.2.1 Access control policy (FDP_ACC)

6.5.2.1.1 FDP_ACC.2: Complete access control

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

subjects: external entities in WAN, HAN and LMN

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

the TOE and any information that is stored in the

TOE ¹⁰⁷ and all operations among subjects and

objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any

subject controlled by the TSF and any object controlled by

the TSF are covered by an access control SFP.

¹⁰⁶ [assignment: *access control SFP*]

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

1837	Hierarchical to:	FDP_ACC.1 Subset access control
1838	Dependencies:	FDP_ACF.1 Security attribute based access control
1839	6.5.2.1.2 FDP_ACF.1: Security attribute based access control	
1840	FDP_ACF.1.1	The TSF shall enforce the <i>Gateway access SFP</i> ¹⁰⁸ to
1841		objects based on the following:
1842		<i>subjects: external entities on the WAN, HAN or</i>
1843		<i>LMN side</i>
1844		<i>objects: any information that is sent to, from or via</i>
1845		<i>the TOE</i>
1846		<i>attributes: destination interface</i> ¹⁰⁹ .
1847	FDP_ACF.1.2	The TSF shall enforce the following rules to determine if
1848		an operation among controlled subjects and controlled
1849		objects is allowed:
1850		• <i>an authorised Consumer is only allowed to have</i>
1851		<i>read access to his own User Data via the interface</i>
1852		<i>IF_GW_CON,</i>
1853		• <i>an authorised Service Technician is only allowed to</i>
1854		<i>have read access to the system log via the interface</i>
1855		<i>IF_GW_SRV, the Service Technician must not be</i>
1856		<i>allowed to read, modify or delete any other TSF</i>
1857		<i>data,</i>
1858		• <i>an authorised Gateway Administrator is allowed to</i>
1859		<i>interact with the TOE only via IF_GW_WAN,</i>
1860		• <i>only authorised Gateway Administrators are</i>
1861		<i>allowed to establish a wake-up call,</i>
1862		• <i>additional rules governing access among controlled</i>
1863		<i>subjects and controlled objects using controlled</i>

¹⁰⁸ [assignment: *access control SFP*]

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

1864		<i>operations on controlled objects or none:</i>
1865		<i>none</i> ^{110, 111}
1866	FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to
1867		objects based on the following additional rules: <i>none</i> ¹¹² .
1868	FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects
1869		based on the following additional rules:
1870		• <i>the Gateway Administrator is not allowed to read</i>
1871		<i>consumption data or the Consumer Log,</i>
1872		• <i>nobody must be allowed to read the symmetric</i>
1873		<i>keys used for encryption</i> ¹¹³ .
1874	Hierarchical to:	No other components
1875	Dependencies:	FDP_ACC.1 Subset access control
1876		FMT_MSA.3 Static attribute initialisation
1877	6.5.3 Firewall SFP	
1878	6.5.3.1 Information flow control policy (FDP_IFC)	
1879	6.5.3.1.1 FDP_IFC.2/FW: Complete information flow control for	
1880	firewall	
1881	FDP_IFC.2.1/FW	The TSF shall enforce the <i>Firewall SFP</i> ¹¹⁴ on the TOE,
1882		<i>external entities on the WAN side, external entities on the</i>
1883		<i>LAN side and all information flowing between them</i> ¹¹⁵ and
1884		all operations that cause that information to flow to and
1885		from subjects covered by the SFP.

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

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

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

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

¹¹⁴ [assignment: *information flow control SFP*]

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

1886	FDP_IFC.2.2/FW	The TSF shall ensure that all operations that cause any
1887		information in the TOE to flow to and from any subject in
1888		the TOE are covered by an information flow control SFP.
1889	Hierarchical to:	FDP_IFC.1 Subset information flow control
1890	Dependencies:	FDP_IFF.1 Simple security attributes
1891	6.5.3.2 Information flow control functions (FDP_IFF)	
1892	6.5.3.2.1 FDP_IFF.1/FW: Simple security attributes for Firewall	
1893	FDP_IFF.1.1/FW	The TSF shall enforce the <i>Firewall SFP</i> ¹¹⁶ based on the
1894		following types of subject and information security
1895		attributes:
1896		<i>subjects: The TOE and external entities on the</i>
1897		<i>WAN, HAN or LMN side</i>
1898		<i>information: any information that is sent to, from or</i>
1899		<i>via the TOE</i>
1900		<i>attributes: destination_interface (TOE, LMN, HAN</i>
1901		<i>or WAN), source_interface (TOE, LMN, HAN or</i>
1902		<i>WAN), destination_authenticated,</i>
1903		<i>source_authenticated</i> ¹¹⁷ .
1904	FDP_IFF.1.2/FW	The TSF shall permit an information flow between a
1905		controlled subject and controlled information via a
1906		controlled operation if the following rules hold:
1907		<i>(if source_interface=HAN or</i>
1908		<i>source_interface=TOE) and</i>
1909		<i>destination_interface=WAN and</i>
1910		<i>destination_authenticated = true</i>
1911		<i>Connection establishment is allowed</i>
1912		

116 [assignment: *information flow control SFP*]

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

1913		<i>if source_interface=LMN and</i>
1914		<i>destination_interface= TOE and</i>
1915		<i>source_authenticated = true</i>
1916		<i>Connection establishment is allowed</i>
1917		
1918		<i>if source_interface=TOE and</i>
1919		<i>destination_interface= LMN and</i>
1920		<i>destination_authenticated = true</i>
1921		<i>Connection establishment is allowed</i>
1922		
1923		<i>if source_interface=HAN and</i>
1924		<i>destination_interface= TOE and</i>
1925		<i>source_authenticated = true</i>
1926		<i>Connection establishment is allowed</i>
1927		
1928		<i>if source_interface=TOE and</i>
1929		<i>destination_interface= HAN and</i>
1930		<i>destination_authenticated = true</i>
1931		<i>Connection establishment is allowed</i>
1932		<i>else</i>
1933		<i>Connection establishment is denied</i> ¹¹⁸ .
1934	FDP_IFF.1.3/FW	The TSF shall enforce the <i>establishment of a connection</i>
1935		<i>to a configured external entity in the WAN after having</i>
1936		<i>received a wake-up message on the WAN interface</i> ¹¹⁹ .

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

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

1937	FDP_IFF.1.4/FW	The TSF shall explicitly authorise an information flow
1938		based on the following rules: <i>none</i> ¹²⁰ .
1939	FDP_IFF.1.5/FW	The TSF shall explicitly deny an information flow based on
1940		the following rules: <i>none</i> ¹²¹ .
1941	Hierarchical to:	No other components
1942	Dependencies:	FDP_IFC.1 Subset information flow control
1943		FMT_MSA.3 Static attribute initialisation
1944	Application Note 27:	It should be noted that the FDP_IFF.1.1/FW facilitates
1945		different interfaces of the origin and the destination of an
1946		information flow implicitly requires the TOE to implement
1947		physically separate ports for WAN, LMN and HAN.
1948	6.5.4 Meter SFP	
1949	6.5.4.1 Information flow control policy (FDP_IFC)	
1950	6.5.4.1.1 FDP_IFC.2/MTR: Complete information flow control for	
1951	Meter information flow	
1952	FDP_IFC.2.1/MTR	The TSF shall enforce the <i>Meter SFP</i> ¹²² on the TOE,
1953		<i>attached Meters, authorized External Entities in the WAN</i>
1954		<i>and all information flowing between them</i> ¹²³ and all
1955		operations that cause that information to flow to and from
1956		subjects covered by the SFP.
1957	FDP_IFC.2.2/MTR	The TSF shall ensure that all operations that cause any
1958		information in the TOE to flow to and from any subject in
1959		the TOE are covered by an information flow control SFP.
1960	Hierarchical to:	FDP_IFC.1 Subset information flow control
1961	Dependencies:	FDP_IFF.1 Simple security attributes

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

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

¹²² [assignment: *information flow control SFP*]

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

1962	6.5.4.2 Information flow control functions (FDP_IFF)	
1963	6.5.4.2.1 FDP_IFF.1/MTR: Simple security attributes for Meter	
1964	information	
1965	FDP_IFF.1.1/MTR	The TSF shall enforce the <i>Meter SFP</i> ¹²⁴ based on the
1966		following types of subject and information security
1967		attributes:
1968		<ul style="list-style-type: none"> • <i>subjects: TOE, external entities in WAN, Meters located in LMN</i>
1969		
1970		<ul style="list-style-type: none"> • <i>information: any information that is sent via the TOE</i>
1971		
1972		<ul style="list-style-type: none"> • <i>attributes: destination interface, source interface (LMN or WAN), Processing Profile</i> ¹²⁵.
1973		
1974	FDP_IFF.1.2/MTR	The TSF shall permit an information flow between a
1975		controlled subject and controlled information via a
1976		controlled operation if the following rules hold:
1977		<ul style="list-style-type: none"> • <i>an information flow shall only be initiated if allowed by a corresponding Processing Profile</i> ¹²⁶.
1978		
1979	FDP_IFF.1.3/MTR	The TSF shall enforce the following rules:
1980		<ul style="list-style-type: none"> • Data received from Meters shall be processed as defined in the corresponding Processing Profiles,
1981		
1982		<ul style="list-style-type: none"> • Results of processing of Meter Data shall be submitted to external entities as defined in the Processing Profiles,
1983		
1984		
1985		<ul style="list-style-type: none"> • The internal system time shall be synchronised as follows:
1986		

¹²⁴ [assignment: *information flow control SFP*]

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

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

1987			○ <i>The TOE shall compare the system time to a</i>
1988			<i>reliable external time source every 24</i>
1989			<i>hours</i> ¹²⁷ .
1990			○ <i>If the deviation between the local time and the</i>
1991			<i>remote time is acceptable</i> ¹²⁸ , <i>the local system</i>
1992			<i>time shall be updated according to the remote</i>
1993			<i>time.</i>
1994			○ <i>If the deviation is not acceptable the TOE</i>
1995			<i>shall ensure that any following Meter Data is</i>
1996			<i>not used, stop operation</i> ¹²⁹ <i>and</i>
1997			<i>inform a Gateway Administrator</i> ¹³⁰ .
1998	FDP_IFF.1.4/MTR	The TSF shall explicitly authorise an information flow	
1999		based on the following rules: <i>none</i> ¹³¹ .	
2000	FDP_IFF.1.5/MTR	The TSF shall explicitly deny an information flow based on	
2001		the following rules: <i>The TOE shall deny any acceptance of</i>	
2002		<i>information by external entities in the LMN unless the</i>	
2003		<i>authenticity, integrity and confidentiality of the Meter Data</i>	
2004		<i>could be verified</i> ¹³² .	
2005	Hierarchical to:	No other components	
2006	Dependencies:	FDP_IFC.1 Subset information flow control	
2007		FMT_MSA.3 Static attribute initialisation	
2008	Application Note 28:	FDP_IFF.1.3 defines that the TOE shall update the local	
2009		system time regularly with reliable external time sources if	
2010		the deviation is acceptable. In the context of this	
2011		functionality two aspects should be mentioned:	

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

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

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

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

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

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

2012		Reliability of external source
2013		<p>There are several ways to achieve the reliability of the external source. On the one hand, there may be a source in the WAN that has an acceptable reliability on its own (e.g. because it is operated by a very trustworthy organisation (an official legal time issued by the calibration authority would be a good example for such a source¹³³)). On the other hand a developer may choose to maintain multiple external sources that all have a certain level of reliability but no absolute reliability. When using such sources the TOE shall contact more than one source and harmonize the results in order to ensure that no attack happened.</p>
2014		
2015		
2016		
2017		
2018		
2019		
2020		
2021		
2022		
2023		
2024		
2025		Acceptable deviation
2026		<p>For the question whether a deviation between the time source(s) in the WAN and the local system time is still acceptable, normative or legislative regulations shall be considered. If no regulation exists, a maximum deviation of 3% of the measuring period is allowed to be in conformance with [PP_GW]. It should be noted that depending on the kind of application a more accurate system time is needed. For doing so, the intervall for the comparison of the system time to a reliable external time source is configurable. But this aspect is not within the scope of this Security Target.</p>
2027		
2028		
2029		
2030		
2031		
2032		
2033		
2034		
2035		
2036		
2037		<p>Please further note that – depending on the exactness of the local clock – it may be required to synchronize the time more often than every 24 hours.</p>
2038		
2039		
2040	Application Note 29:	<p>In FDP_IFF.1.5/MTR the TOE is required to verify the authenticity, integrity and confidentiality of the Meter Data</p>
2041		

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

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

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

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

6.5.5 General Requirements on user data protection

6.5.5.1 Residual information protection (FDP_RIP)

6.5.5.1.1 FDP_RIP.2: Full residual information protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from ¹³⁴ all objects.

Hierarchical to: FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

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

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

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

2071 way that makes it impossible for an attacker to get access
2072 to is assuming a physical access to the memory of the
2073 TOE.

2074 6.5.5.2 Stored data integrity (FDP_SDI)

2075 **6.5.5.2.1 FDP_SDI.2: Stored data integrity monitoring and action**

2076 FDP_SDI.2.1 The TSF shall monitor user data stored in containers
2077 controlled by the TSF for *integrity errors*¹³⁵ on all objects,
2078 based on the following attributes: *cryptographical check*
2079 *sum*¹³⁶.

2080 FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall
2081 *create a system log entry*¹³⁷.

2082 Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

2083 Dependencies: No dependencies.

2084 **6.6 Class FIA: Identification and Authentication**

2085 **6.6.1 User Attribute Definition (FIA_ATD)**

2086 6.6.1.1 FIA_ATD.1: User attribute definition

2087 FIA_ATD.1.1 The TSF shall maintain the following list of security
2088 attributes belonging to individual users:

- 2089
- *User Identity*
 - *Status of Identity (Authenticated or not)*
 - *Connecting network (WAN, HAN or LMN)*
 - *Role membership*
 - *none*¹³⁸.
- 2090
2091
2092
2093

2094 Hierarchical to: No other components.

2095 Dependencies: No dependencies.

135 [assignment: *integrity errors*]
136 [assignment: *user data attributes*]
137 [assignment: *action to be taken*]
138 [assignment: *list of security attributes*]

2096 **6.6.2 Authentication Failures (FIA_AFL)**

2097 6.6.2.1 FIA_AFL.1: Authentication failure handling

2098 FIA_AFL.1.1 The TSF shall detect when 5¹³⁹ unsuccessful
 2099 authentication attempts occur related to *authentication*
 2100 *attempts at IF_GW_CON*¹⁴⁰.

2101 FIA_AFL.1.2 When the defined number of unsuccessful authentication
 2102 attempts has been met¹⁴¹, the TSF shall *block*
 2103 *IF_GW_CON for 5 minutes*¹⁴².

2104 Hierarchical to: No other components

2105 Dependencies: FIA_UAU.1 Timing of authentication

2106 **6.6.3 User Authentication (FIA_UAU)**

2107 6.6.3.1 FIA_UAU.2: User authentication before any action

2108 FIA_UAU.2.1 The TSF shall require each user to be successfully
 2109 authenticated before allowing any other TSF-mediated
 2110 actions on behalf of that user.

2111 Hierarchical to: FIA_UAU.1

2112 Dependencies: FIA_UID.1 Timing of identification

2113 **Application Note 31:** Please refer to [TR-03109-1] for a more detailed overview
 2114 on the authentication of TOE users.

2115 6.6.3.2 FIA_UAU.5: Multiple authentication mechanisms

2116 FIA_UAU.5.1 The TSF shall provide

- 2117 • *authentication via certificates at the IF_GW_MTR*
- 2118 *interface*
- 2119 • *TLS-authentication via certificates at the*
- 2120 *IF_GW_WAN interface*

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

140 [assignment: *list of authentication events*]

141 [selection: *met, surpassed*]

142 [assignment: *list of actions*]

2121		<ul style="list-style-type: none"> • <i>TLS-authentication via HAN-certificates at the</i>
2122		<i>IF_GW_CON interface</i>
2123		<ul style="list-style-type: none"> • <i>authentication via password at the IF_GW_CON</i>
2124		<i>interface</i>
2125		<ul style="list-style-type: none"> • <i>TLS-authentication via HAN-certificates at the</i>
2126		<i>IF_GW_SRV interface</i>
2127		<ul style="list-style-type: none"> • <i>authentication at the IF_GW_CLS interface</i>
2128		<ul style="list-style-type: none"> • <i>verification via a commands' signature</i> ¹⁴³
2129		to support user authentication.
2130	FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity
2131		according to the
2132		<ul style="list-style-type: none"> • <i>meters shall be authenticated via certificates at the</i>
2133		<i>IF_GW_MTR interface only</i>
2134		<ul style="list-style-type: none"> • <i>Gateway Administrators shall be authenticated via</i>
2135		<i>TLS-certificates at the IF_GW_WAN interface only</i>
2136		<ul style="list-style-type: none"> • <i>Consumers shall be authenticated via TLS-</i>
2137		<i>certificates or via password at the IF_GW_CON</i>
2138		<i>interface only</i>
2139		<ul style="list-style-type: none"> • <i>Service Technicians shall be authenticated via</i>
2140		<i>TLS-certificates at the IF_GW_SRV interface only</i>
2141		<ul style="list-style-type: none"> • <i>CLS shall be authenticated at the IF_GW_CLS only</i>
2142		<ul style="list-style-type: none"> • <i>each command of an Gateway Administrator shall</i>
2143		<i>be authenticated by verification of the commands'</i>
2144		<i>signature,</i>
2145		<ul style="list-style-type: none"> • <i>other external entities shall be authenticated via</i>
2146		<i>TLS-certificates at the IF_GW_WAN interface</i>
2147		<i>only</i> ¹⁴⁴ .

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

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

2148	Hierarchical to:	No other components.
2149	Dependencies:	No dependencies.
2150	Application Note 32:	Please refer to [TR-03109-1] for a more detailed overview
2151		on the authentication of TOE users.
2152	6.6.3.3 FIA_UAU.6: Re-authenticating	
2153	FIA_UAU.6.1	The TSF shall re-authenticate an external entity ¹⁴⁵ under
2154		the conditions
2155		<ul style="list-style-type: none"> • <i>TLS channel to the WAN shall be disconnected</i>
2156		<i>after 48 hours,</i>
2157		<ul style="list-style-type: none"> • <i>TLS channel to the LMN shall be disconnected after</i>
2158		<i>5 MB of transmitted information,</i>
2159		<ul style="list-style-type: none"> • <i>other local users shall be re-authenticated after at</i>
2160		<i>least 10 minutes</i> ¹⁴⁶ <i>of inactivity</i> ¹⁴⁷ .
2161	Hierarchical to:	No other components.
2162	Dependencies:	No dependencies.
2163	Application Note 33:	This requirement on re-authentication for external entities
2164		in the WAN and LMN is addressed by disconnecting the
2165		TLS channel even though a re-authentication is - strictly
2166		speaking - only achieved if the TLS channel is build up
2167		again.
2168	6.6.4 User identification (FIA_UID)	
2169	6.6.4.1 FIA_UID.2: User identification before any action	
2170	FIA_UID.2.1	The TSF shall require each user to be successfully
2171		identified before allowing any other TSF-mediated actions
2172		on behalf of that user.
2173	Hierarchical to:	FIA_UID.1
2174	Dependencies:	No dependencies.

¹⁴⁵ [refinement: *the user*]

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

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

2175 **6.6.5 User-subject binding (FIA_USB)**

2176 6.6.5.1 FIA_USB.1: User-subject binding

2177 FIA_USB.1.1 The TSF shall associate the following user security
 2178 attributes with subjects acting on the behalf of that user:
 2179 *attributes as defined in FIA_ATD.1 ¹⁴⁸.*

2180 FIA_USB.1.2 The TSF shall enforce the following rules on the initial
 2181 association of user security attributes with subjects acting
 2182 on the behalf of users:

- 2183 • *The initial value of the security attribute 'connecting*
 2184 *network' is set to the corresponding physical*
 2185 *interface of the TOE (HAN, WAN, or LMN).*
- 2186 • *The initial value of the security attribute 'role*
 2187 *membership' is set to the user role claimed on basis*
 2188 *of the credentials used for authentication at the*
 2189 *connecting network as defined in FIA_UAU.5.2. For*
 2190 *role membership 'Gateway Administrators',*
 2191 *additionally the remote network endpoint ¹⁴⁹used*
 2192 *and configured in the TSF data must be identical.*
- 2193 • *The initial value of the security attribute 'user*
 2194 *identity' is set to the identification attribute of the*
 2195 *credentials used by the subject. The security*
 2196 *attribute 'user identity' is set to the subject key ID of*
 2197 *the certificate in case of a certificate-based*
 2198 *authentication, the meter-ID for wired Meters and*
 2199 *the user name owner in case of a password-based*
 2200 *authentication at interface IF_GW_CON.*
- 2201 • *The initial value of the security attribute 'status of*
 2202 *identity' is set to the authentication status of the*
 2203 *claimed identity. If the authentication is successful*
 2204 *on basis of the used credentials, the status of*

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

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

2205 *identity is 'authenticated', otherwise it is*
 2206 *'not authenticated'* ¹⁵⁰.

2207 FIA_USB.1.3 The TSF shall enforce the following rules governing
 2208 changes to the user security attributes associated with
 2209 subjects acting on the behalf of users:

- 2210 • *security attribute 'connecting network' is not*
 2211 *changeable.*
- 2212 • *security attribute 'role membership' is not*
 2213 *changeable.*
- 2214 • *security attribute 'user identity' is not changeable.*
- 2215 • *security attribute 'status of identity' is not*
 2216 *changeable*¹⁵¹.

2217 Hierarchical to: No other components.

2218 Dependencies: FIA_ATD.1 User attribute definition

2219 **6.7 Class FMT: Security Management**

2220 **6.7.1 Management of the TSF**

2221 6.7.1.1 Management of functions in TSF (FMT_MOF)

2222 **6.7.1.1.1 FMT_MOF.1: Management of security functions** 2223 ***behaviour***

2224 FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour
 2225 of ¹⁵² the functions *for management as defined in*

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

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

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

2226		<i>FMT_SMF.1</i> ¹⁵³ to roles and criteria as defined in Table
2227		13 ¹⁵⁴ .
2228	Hierarchical to:	No other components.
2229	Dependencies:	FMT_SMR.1 Security roles
2230		FMT_SMF.1 Specification of Management Functions

Function	Limitation
Display the version number of the TOE Display the current time	The management functions must only be accessible for an authorised Consumer and only via the interface IF_GW_CON. An authorized Service Technician is also able to access the version number of the TOE and the current time of the TOE via interface IF_GW_SRV ¹⁵⁵ .
All other management functions as defined in FMT_SMF.1	The management functions must only be accessible for an authorised Gateway Administrator and only via the interface IF_GW_WAN ¹⁵⁶ .
Firmware Update	The firmware update must only be possible after the authenticity of the firmware update has been verified (using the services of the Security Module and the trust anchor of the Gateway developer) and if the version number of the new firmware is higher to the version of the installed firmware.
Deletion or modification of events from the Calibration Log	A deletion or modification of events from the calibration log must not be possible.

2231 **Table 13: Restrictions on Management Functions**

¹⁵³ [assignment: *list of functions*]
¹⁵⁴ [assignment: *the authorised identified roles*]
¹⁵⁵ The TOE displays the version number of the TOE and the current time of the TOE also to the authorized service technician via the interface IF_GW_SRV because the service technician must be able to determine if the current time of the TOE is correct or if the version number of the TOE is correct.
¹⁵⁶ This criterion applies to all management functions. The following entries in this table only augment this restriction further.

2232	6.7.1.2 Specification of Management Functions (FMT_SMF)	
2233	6.7.1.2.1 FMT_SMF.1: Specification of Management Functions	
2234	FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: <i>list of management functions as defined in Table 14 and Table 15 and additional functionalities: none</i> ¹⁵⁷ .
2235		
2236		
2237		
2238	Hierarchical to:	No other components.
2239	Dependencies:	No dependencies.

SFR	Management functionality
FAU_ARP.1/SYS	<ul style="list-style-type: none">The management (addition, removal, or modification) of actions ¹⁵⁸
FAU_GEN.1/SYS FAU_GEN.1/CON FAU_GEN.1/CAL	-
FAU_SAA.1/SYS	<ul style="list-style-type: none">Maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules ¹⁵⁸
FAU_SAR.1/SYS FAU_SAR.1/CON FAU_SAR.1/CAL	- ¹⁵⁹
FAU_STG.4/SYS FAU_STG.4/CON	<ul style="list-style-type: none">Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure ¹⁵⁸Size configuration of the audit trail that is available before the oldest events get overwritten ¹⁵⁸

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

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

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

FAU_STG.4/CAL	- 160
FAU_GEN.2	-
FAU_STG.2	<ul style="list-style-type: none"> Maintenance of the parameters that control the audit storage capability for the consumer log and the system log¹⁵⁸
FCO_NRO.2	<ul style="list-style-type: none"> The management of changes to information types, fields,¹⁵⁸ originator attributes and recipients of evidence
FCS_CKM.1/TLS	-
FCS_COP.1/TLS	<ul style="list-style-type: none"> Management of key material including key material stored in the Security Module
FCS_CKM.1/CMS	-
FCS_COP.1/CMS	<ul style="list-style-type: none"> Management of key material including key material stored in the Security Module
FCS_CKM.1/MTR	-
FCS_COP.1/MTR	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Management of key material
FDP_ACC.2	-
FDP_ACF.1	-
FDP_IFC.2/FW	-

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

FDP_IFF.1/FW	<ul style="list-style-type: none"> Managing the attributes used to make explicit access based decisions Add authorised units for communication (pairing) Management of endpoint to be contacted after successful wake-up call Management of CLS systems
FDP_IFC.2/MTR	-
FDP_IFF.1/MTR	<ul style="list-style-type: none"> Managing the attributes (including Processing Profiles) used to make explicit access based decisions
FDP_RIP.2	-
FDP_SDI.2	<ul style="list-style-type: none"> The actions to be taken upon the detection of an integrity error shall be configurable.¹⁵⁸
FIA_ATD.1	<ul style="list-style-type: none"> If so indicated in the assignment, the authorised Gateway Administrator might be able to define additional security attributes for users¹⁶¹.
FIA_AFL.1	<ul style="list-style-type: none"> Management of the threshold for unsuccessful authentication attempts¹⁵⁸ Management of actions to be taken in the event of an authentication failure¹⁵⁸
FIA_UAU.2	<ul style="list-style-type: none"> Management of the authentication data by an Gateway Administrator
FIA_UAU.5	- 162
FIA_UAU.6	<ul style="list-style-type: none"> Management of re-authentication time

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

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

FIA_UID.2	<ul style="list-style-type: none"> The management of the user identities
FIA_USB.1	<ul style="list-style-type: none"> An authorised Gateway Administrator can define default subject security attributes, if so indicated in the assignment of FIA_ATD.1.¹⁵⁸ An authorised Gateway Administrator can change subject security attributes, if so indicated in the assignment of FIA_ATD.1.¹⁵⁸
FMT_MOF.1	<ul style="list-style-type: none"> Managing the group of roles that can interact with the functions in the TSF
FMT_SMF.1	-
FMT_SMR.1	<ul style="list-style-type: none"> Managing the group of users that are part of a role
FMT_MSA.1/AC	<ul style="list-style-type: none"> Management of rules by which security attributes inherit specified values^{163,158}
FMT_MSA.3/AC	- ¹⁶⁴
FMT_MSA.1/FW	<ul style="list-style-type: none"> Management of rules by which security attributes inherit specified values^{165,158}
FMT_MSA.3/FW	- ¹⁶⁶
FMT_MSA.1/MTR	<ul style="list-style-type: none"> Management of rules by which security attributes inherit specified values^{167,158}

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

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

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

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

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

FMT_MSA.3/MTR	- 168
FPR_CON.1	<ul style="list-style-type: none"> Definition of the interval in FPR_CON.1.2 if definable within the operational phase of the TOE ¹⁵⁸
FPR_PSE.1	-
FPT_FLS.1	-
FPT_RPL.1	-
FPT_STM.1	<ul style="list-style-type: none"> Management a time source
FPT_TST.1	- 169
FPT_PHP.1	<ul style="list-style-type: none"> Management of the user or role that determines whether physical tampering has occurred ¹⁵⁸
FTP_ITC.1/WAN	- 170
FTP_ITC.1/MTR	- 171
FTP_ITC.1/USR	- 172

2240

Table 14: SFR related Management Functionalities

-
- ¹⁶⁸ As no role is allowed to specify alternative initial values within [PP_GW], the management functions as defined by [CC, part 2] do not apply.
- ¹⁶⁹ As the rules for TSF testing are fixed within [PP_GW], the management functions as defined by [CC, part 2] do not apply.
- ¹⁷⁰ As the configuration of the actions that require a trusted channel is fixed by [PP_GW], the management functions as defined in [CC, part 2] do not apply.
- ¹⁷¹ As the configuration of the actions that require a trusted channel is fixed by [PP_GW], the management functions as defined in [CC, part 2] do not apply.
- ¹⁷² As the configuration of the actions that require a trusted channel is fixed by [PP_GW], the management functions as defined in [CC, part 2] do not apply.

2241

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

2242

Table 15: Gateway specific Management Functionalities

2243

6.7.2 Security management roles (FMT_SMR)

2244

6.7.2.1 FMT_SMR.1: Security roles

2245

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

2246

2247

2248

2249

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

2250

Hierarchical to: No other components.

2251

Dependencies: No dependencies.

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

¹⁷⁴ [assignment: *the authorised identified roles*]

2252	6.7.3 Management of security attributes for Gateway access SFP	
2253	6.7.3.1 Management of security attributes (FMT_MSA)	
2254	6.7.3.1.1 FMT_MSA.1/AC: Management of security attributes for	
2255	Gateway access SFP	
2256	FMT_MSA.1.1/AC	The TSF shall enforce the <i>Gateway access SFP</i> ¹⁷⁵ to
2257		restrict the ability to <u>query, modify, delete, other</u>
2258		<u>operations: none</u> ¹⁷⁶ the security attributes <i>all relevant</i>
2259		<i>security attributes</i> ¹⁷⁷ to <i>authorised Gateway</i>
2260		<i>Administrators</i> ¹⁷⁸ .
2261	Hierarchical to:	No other components.
2262	Dependencies:	[FDP_ACC.1 Subset access control, or
2263		FDP_IFC.1 Subset information flow control], fulfilled by
2264		FDP_ACC.2
2265		FMT_SMR.1 Security roles
2266		FMT_SMF.1 Specification of Management Functions
2267	6.7.3.1.2 FMT_MSA.3/AC: Static attribute initialisation for Gateway	
2268	access SFP	
2269	FMT_MSA.3.1/AC	The TSF shall enforce the <i>Gateway access SFP</i> ¹⁷⁹ to
2270		provide <u>restrictive</u> ¹⁸⁰ default values for security attributes
2271		that are used to enforce the SFP.
2272	FMT_MSA.3.2/AC	The TSF shall allow the <i>no role</i> ¹⁸¹ to specify alternative
2273		initial values to override the default values when an object
2274		or information is created.

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

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

¹⁷⁷ [assignment: *list of security attributes*]

¹⁷⁸ [assignment: *the authorised identified roles*]

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

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

¹⁸¹ [assignment: *the authorised identified roles*]

2275	Hierarchical to:	No other components.
2276	Dependencies:	FMT_MSA.1 Management of security attributes
2277		FMT_SMR.1 Security roles
2278	6.7.4 Management of security attributes for Firewall SFP	
2279	6.7.4.1 Management of security attributes (FMT_MSA)	
2280	6.7.4.1.1 FMT_MSA.1/FW: Management of security attributes for	
2281	firewall policy	
2282	FMT_MSA.1.1/FW	The TSF shall enforce the <i>Firewall SFP</i> ¹⁸² to restrict the
2283		ability to <u>query, modify, delete, other operations: none</u> ¹⁸³
2284		the security attributes <i>all relevant security attributes</i> ¹⁸⁴ to
2285		<i>authorised Gateway Administrators</i> ¹⁸⁵ .
2286	Hierarchical to:	No other components.
2287	Dependencies:	[FDP_ACC.1 Subset access control, or
2288		FDP_IFC.1 Subset information flow control], fulfilled by
2289		FDP_IFC.2/FW
2290		FMT_SMR.1 Security roles
2291		FMT_SMF.1 Specification of Management Functions
2292	6.7.4.1.2 FMT_MSA.3/FW: Static attribute initialisation for Firewall	
2293	policy	
2294	FMT_MSA.3.1/FW	The TSF shall enforce the <i>Firewall SFP</i> ¹⁸⁶ to provide
2295		<u>restrictive</u> ¹⁸⁷ default values for security attributes that are
2296		used to enforce the SFP.

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

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

¹⁸⁴ [assignment: *list of security attributes*]

¹⁸⁵ [assignment: *the authorised identified roles*]

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

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

2297	FMT_MSA.3.2/FW	The TSF shall allow the <i>no role</i> ¹⁸⁸ to specify alternative
2298		initial values to override the default values when an object
2299		or information is created.
2300	Hierarchical to:	No other components.
2301	Dependencies:	FMT_MSA.1 Management of security attributes
2302		FMT_SMR.1 Security roles
2303	Application Note 34:	The definition of restrictive default rules for the firewall
2304		information flow policy refers to the rules as defined in
2305		FDP_IFF.1.2/FW and FDP_IFF.1.5/FW. Those rules apply
2306		to all information flows and must not be overwritable by
2307		anybody.
2308	6.7.5 Management of security attributes for Meter SFP	
2309	6.7.5.1 Management of security attributes (FMT_MSA)	
2310	6.7.5.1.1 FMT_MSA.1/MTR: Management of security attributes for	
2311	Meter policy	
2312	FMT_MSA.1.1/MTR	The TSF shall enforce the <i>Meter SFP</i> ¹⁸⁹ to restrict the
2313		ability to <u>change default, query, modify, delete, other</u>
2314		<u>operations: none</u> ¹⁹⁰ the security attributes <i>all relevant</i>
2315		<i>security attributes</i> ¹⁹¹ to <i>authorised Gateway</i>
2316		<i>Administrators</i> ¹⁹² .
2317	Hierarchical to:	No other components.
2318	Dependencies:	[FDP_ACC.1 Subset access control, or
2319		FDP_IFC.1 Subset information flow control], fulfilled by
2320		FDP_IFC.2/FW
2321		FMT_SMR.1 Security roles

¹⁸⁸ [assignment: *the authorised identified roles*]

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

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

¹⁹¹ [assignment: *list of security attributes*]

¹⁹² [assignment: *the authorised identified roles*]

2322		FMT_SMF.1 Specification of Management Functions
2323	6.7.5.1.2	<i>FMT_MSA.3/MTR: Static attribute initialisation for Meter</i>
2324		<i>policy</i>
2325	FMT_MSA.3.1/MTR	The TSF shall enforce the <i>Meter SFP</i> ¹⁹³ to provide
2326		<u>restrictive</u> ¹⁹⁴ default values for security attributes that are
2327		used to enforce the SFP.
2328	FMT_MSA.3.2/MTR	The TSF shall allow the <i>no role</i> ¹⁹⁵ to specify alternative
2329		initial values to override the default values when an object
2330		or information is created.
2331	Hierarchical to:	No other components.
2332	Dependencies:	FMT_MSA.1 Management of security attributes
2333		FMT_SMR.1 Security roles

2335 6.8 Class FPR: Privacy

2336	6.8.1	Communication Concealing (FPR_CON)
2337	6.8.1.1	FPR_CON.1: Communication Concealing
2338	FPR_CON.1.1	The TSF shall enforce the <i>Firewall SFP</i> ¹⁹⁶ in order to
2339		ensure that no personally identifiable information (PII) can
2340		be obtained by an analysis of <i>frequency, load, size or the</i>
2341		<i>absence of external communication</i> ¹⁹⁷ .
2342	FPR_CON.1.2	The TSF shall connect to <i>the Gateway Administrator,</i>
2343		<i>authorized External Entity in the WAN</i> ¹⁹⁸ in intervals as

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

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

195 [assignment: *the authorised identified roles*]

196 [assignment: *information flow policy*]

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

198 [assignment: *list of external entities*]

2344		follows <u>daily, other interval: none</u> ¹⁹⁹ to conceal the data
2345		flow ²⁰⁰ .
2346	Hierarchical to:	No other components.
2347	Dependencies:	No dependencies.
2348	6.8.2 Pseudonymity (FPR_PSE)	
2349	6.8.2.1 FPR_PSE.1 Pseudonymity	
2350	FPR_PSE.1.1	The TSF shall ensure that <i>external entities in the WAN</i> ²⁰¹
2351		are unable to determine the real user name bound to
2352		<i>information neither relevant for billing nor for a secure</i>
2353		<i>operation of the Grid sent to parties in the WAN</i> ²⁰² .
2354	FPR_PSE.1.2	The TSF shall be able to provide <i>aliases as defined by the</i>
2355		<i>Processing Profiles</i> ²⁰³ of the real user name for the
2356		Meter and Gateway identity ²⁰⁴ to <i>external entities in the</i>
2357		<i>WAN</i> ²⁰⁵ .
2358	FPR_PSE.1.3	The TSF shall <u>determine an alias for a user</u> ²⁰⁶ and verify
2359		that it conforms to the <i>alias given by the Gateway</i>
2360		<i>Administrator in the Processing Profile</i> ²⁰⁷ .
2361	Hierarchical to:	No other components.
2362	Dependencies:	No dependencies.
2363	Application Note 35:	When the TOE submits information about the consumption
2364		or production of a certain commodity that is not relevant for
2365		the billing process nor for a secure operation of the Grid,
2366		there is no need that this information is sent with a direct

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

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

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

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

203 [assignment: *number of aliases*]

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

205 [assignment: *list of subjects*]

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

207 [assignment: *alias metric*]

2367	link to the identity of the consumer. In those cases, the
2368	TOE shall replace the identity of the Consumer by a
2369	pseudonymous identifier. Please note that the identity of
2370	the Consumer may not be their name but could also be a
2371	number (e.g. consumer ID) used for billing purposes.
2372	A Gateway may use more than one pseudonymous
2373	identifier.
2374	A complete anonymisation would be beneficial in terms of
2375	the privacy of the consumer. However, a complete
2376	anonymous set of information would not allow the external
2377	entity to ensure that the data comes from a trustworthy
2378	source.
2379	Please note that an information flow shall only be initiated
2380	if allowed by a corresponding Processing Profile.
2381	

2382

6.9Class FPT: Protection of the TSF

2383

6.9.1 Fail secure (FPT_FLS)

2384

6.9.1.1 FPT_FLS.1: Failure with preservation of secure state

2385	FPT_FLS.1.1	The TSF shall preserve a secure state when the following
2386		types of failures occur:
2387		<ul style="list-style-type: none"> the deviation between local system time of the TOE
2388		and the reliable external time source is too large,
2389		<ul style="list-style-type: none"> TOE hardware / firmware integrity violation or
2390		<ul style="list-style-type: none"> TOE software application integrity violation ²⁰⁸.

2391	Hierarchical to:	No other components.
------	------------------	----------------------

2392	Dependencies:	No dependencies.
------	---------------	------------------

2393	Application Note 36:	The local clock shall be as exact as required by normative
2394		or legislative regulations. If no regulation exists, a

208

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

2395 maximum deviation of 3% of the measuring period is
2396 allowed to be in conformance with [PP_GW].

2397 **6.9.2 Replay Detection (FPT_RPL)**

2398 6.9.2.1 FPT_RPL.1: Replay detection

2399 FPT_RPL.1.1 The TSF shall detect replay for the following entities: *all*
2400 *external entities* ²⁰⁹.

2401 FPT_RPL.1.2 The TSF shall perform *ignore replayed data* ²¹⁰ when
2402 replay is detected.

2403 Hierarchical to: No other components.

2404 Dependencies: No dependencies.

2405 **6.9.3 Time stamps (FPT_STM)**

2406 6.9.3.1 FPT_STM.1: Reliable time stamps

2407 FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

2408 Hierarchical to: No other components.

2409 Dependencies: No dependencies.

2410

2411 **6.9.4 TSF self test (FPT_TST)**

2412 6.9.4.1 FPT_TST.1: TSF testing

2413 FPT_TST.1.1 The TSF shall run a suite of self tests during initial startup,
2414 at the request of a user and periodically during normal
2415 operation ²¹¹ to demonstrate the correct operation of the
2416 TSF ²¹².

209 [assignment: *list of identified entities*]

210 [assignment: *list of specific actions*]

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

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

2417 FPT_TST.1.2 The TSF shall provide authorised users with the capability
 2418 to verify the integrity of TSF data ²¹³.

2419 FPT_TST.1.3 The TSF shall provide authorised users with the capability
 2420 to verify the integrity of TSF ²¹⁴.

2421 Hierarchical to: No other components.

2422 Dependencies: No dependencies.

2423 **6.9.5 TSF physical protection (FPT_PHP)**

2424 6.9.5.1 FPT_PHP.1: Passive detection of physical attack

2425 FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical
 2426 tampering that might compromise the TSF.

2427 FPT_PHP.1.2 The TSF shall provide the capability to determine whether
 2428 physical tampering with the TSF's devices or TSF
 2429 elements has occurred.

2430 Hierarchical to: No other components.

2431 Dependencies: No dependencies.

2432

2433 **6.10 Class FTP: Trusted path/channels**

2434 **6.10.1 Inter-TSF trusted channel (FTP_ITC)**

2435 6.10.1.1 FTP_ITC.1/WAN: Inter-TSF trusted channel for WAN

2436 FTP_ITC.1.1/WAN The TSF shall provide a communication channel between
 2437 itself and another trusted IT product that is logically distinct
 2438 from other communication channels and provides assured
 2439 identification of its end points and protection of the channel
 2440 data from modification or disclosure.

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

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

2441	FTP_ITC.1.2/WAN	The TSF shall permit <u>the TSF</u> ²¹⁵ to initiate communication
2442		via the trusted channel.
2443	FTP_ITC.1.3/WAN	The TSF shall initiate communication via the trusted
2444		channel for <i>all communications to external entities in the</i>
2445		<i>WAN</i> ²¹⁶ .
2446	Hierarchical to:	No other components
2447	Dependencies:	No dependencies.
2448	6.10.1.2 FTP_ITC.1/MTR:	Inter-TSF trusted channel for Meter
2449	FTP_ITC.1.1/MTR	The TSF shall provide a communication channel between
2450		itself and another trusted IT product that is logically distinct
2451		from other communication channels and provides assured
2452		identification of its end points and protection of the channel
2453		data from modification or disclosure.
2454	FTP_ITC.1.2/MTR	The TSF shall permit the Meter and the TOE ²¹⁷ to initiate
2455		communication via the trusted channel.
2456	FTP_ITC.1.3/MTR	The TSF shall initiate communication via the trusted
2457		channel for <i>any communication between a Meter and the</i>
2458		<i>TOE</i> ²¹⁸ .
2459	Hierarchical to:	No other components.
2460	Dependencies:	No dependencies.
2461	Application Note 37:	The corresponding cryptographic primitives are defined by
2462		FCS_COP.1/MTR.
2463	6.10.1.3 FTP_ITC.1/USR:	Inter-TSF trusted channel for User
2464	FTP_ITC.1.1/USR	The TSF shall provide a communication channel between
2465		itself and another trusted IT product that is logically distinct
2466		from other communication channels and provides assured

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

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

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

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

2467		identification of its end points and protection of the channel
2468		data from modification or disclosure.
2469	FTP_ITC.1.2/USR	The TSF shall permit the Consumer, the Service
2470		Technician ²¹⁹ to initiate communication via the trusted
2471		channel.
2472	FTP_ITC.1.3/USR	The TSF shall initiate communication via the trusted
2473		channel for <i>any communication between a Consumer and</i>
2474		<i>the TOE and the Service Technician and the TOE</i> ²²⁰ .
2475	Hierarchical to:	No other components.
2476	Dependencies:	No dependencies.
2477		

2478 **6.11 Security Assurance Requirements for the TOE**

2479 The minimum Evaluation Assurance Level for this Security Target is **EAL 4 augmented**
2480 **by AVA_VAN.5 and ALC_FLR.2**. The following table lists the assurance components
2481 which are therefore applicable to this ST.

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

219 [selection: *the TSF, another trusted IT product*]
220 [assignment: *list of functions for which a trusted channel is required*]

Assurance Class	Assurance Component
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1
	ALC_FLR.2
Security Target Evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	AVA_VAN.5

2482 **Table 16: Assurance Requirements**

2483 **6.11.1 Refinement for ALC_DEL.1 for the following assurance elements**

2484 ALC_DEL.1.1D: The developer shall document and provide procedures for delivery of

2485 the TOE or parts of it to the **consumer MPO**.

2486 ALC_DEL.1.1C: The delivery documentation shall describe all procedures that are nec-

2487 essary to maintain security when distributing versions of the TOE to the **consumer MPO**.

2488 Application Note: "MPO" as the recipient of the TOE delivery is to be understood to also

2489 include service technicians or any other agent who act as a contractor on behalf of the

2490 MPO.

2491

2492 **6.12 Security Requirements rationale**

2493 **6.12.1 Security Functional Requirements rationale**

2494 6.12.1.1 Fulfilment of the Security Objectives

2495 This chapter proves that the set of security requirements (TOE) is suited to fulfil the

2496 security objectives described in chapter 4 and that each SFR can be traced back to the

2497 security objectives. At least one security objective exists for each security requirement.

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
FAU_ARP.1/SYS									X	
FAU_GEN.1/SYS									X	
FAU_SAA.1/SYS									X	
FAU_SAR.1/SYS									X	
FAU_STG.4/SYS									X	
FAU_GEN.1/CON									X	
FAU_SAR.1/CON									X	
FAU_STG.4/CON									X	

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
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.Manage-	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		

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
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 17: Fulfilment of Security Objectives

The following paragraphs contain more details on this mapping.

6.12.1.1.1 O.Firewall

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

- **FDP_IFC.2/FW** defines that the TOE shall implement an information flow policy for its firewall functionality.
- **FDP_IFF.1/FW** defines the concrete rules for the firewall information flow policy.

- 2505 • **FTP_ITC.1/WAN** defines the policy around the trusted channel to parties in the
2506 WAN.

2507 **6.12.1.1.2 O.SeparateIF**

2508 O.SeparateIF is met by a combination of the following SFRs:

- 2509 • **FDP_IFC.2/FW** and **FDP_IFF.1/FW** implicitly require the TOE to implement
2510 physically separate ports for WAN and LMN.
2511 • **FPT_TST.1** implements a self test that also detects whether the ports for WAN
2512 and LAN have been interchanged.

2513 **6.12.1.1.3 O.Conceal**

2514 O.Conceal is completely met by **FPR_CON.1** as directly follows.

2515 **6.12.1.1.4 O.Meter**

2516 O.Meter is met by a combination of the following SFRs:

- 2517 • **FDP_IFC.2/MTR** and **FDP_IFF.1/MTR** define an information flow policy to
2518 introduce how the Gateway shall handle Meter Data.
2519 • **FCO_NRO.2** ensure that all Meter Data will be signed by the Gateway (invoking
2520 the services of its Security Module) before being submitted to external entities.
2521 • **FPR_PSE.1** defines requirements around the pseudonymization of Meter
2522 identities for Status data.
2523 • **FTP_ITC.1/MTR** defines the requirements around the Trusted Channel that
2524 shall be implemented by the Gateway in order to protect information submitted
2525 via the Gateway and external entities in the WAN or the Gateway and a
2526 distributed Meter.

2527

2528 **6.12.1.1.5 O.Crypt**

2529 O.Crypt is met by a combination of the following SFRs:

- 2530 • **FCS_CKM.4** defines the requirements around the secure deletion of ephemeral
2531 cryptographic keys.
- 2532 • **FCS_CKM.1/TLS** defines the requirements on key negotiation for the TLS
2533 protocol.
- 2534 • **FCS_CKM.1/CMS** defines the requirements on key generation for symmetric
2535 encryption within CMS.
- 2536 • **FCS_COP.1/TLS** defines the requirements around the encryption and
2537 decryption capabilities of the Gateway for communications with external parties
2538 and to Meters.
- 2539 • **FCS_COP.1/CMS** defines the requirements around the encryption and
2540 decryption of content and administration data.
- 2541 • **FCS_CKM.1/MTR** defines the requirements on key negotiation for meter com-
2542 munication encryption.
- 2543 • **FCS_COP.1/MTR** defines the cryptographic primitives for meter
2544 communication encryption.
- 2545 • **FCS_COP.1/HASH** defines the requirements on hashing that are needed in the
2546 context of digital signatures (which are created and verified by the Security
2547 Module).
- 2548 • **FCS_COP.1/MEM** defines the requirements around the encryption of TSF data.
- 2549 • **FPT_RPL.1** ensures that a replay attack for communications with external
2550 entities is detected.

2551 **6.12.1.1.6 O.Time**

2552 O.Time is met by a combination of the following SFRs:

- 2553 • **FDP_IFC.2/MTR** and **FDP_IFF.1/MTR** define the required update functionality
2554 for the local time as part of the information flow control policy for handling Meter
2555 Data.
- 2556 • **FPT_STM.1** defines that the TOE shall be able to provide reliable time stamps.

2557

6.12.1.1.7 *O.Protect*

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

- **FCS_COP.1/MEM** defines that the TOE shall encrypt its TSF and user data as long as it is not in use.
- **FDP_RIP.2** defines that the TOE shall make information unavailable as soon as it is no longer needed.
- **FDP_SDI.2** defines requirements around the integrity protection for stored data.
- **FPT_FLS.1** defines requirements that the TOE falls back to a safe state for specific error cases.
- **FPT_TST.1** defines the self testing functionality to detect whether the interfaces for WAN and LAN are separate.
- **FPT_PHP.1** defines the exact requirements around the physical protection that the TOE has to provide.

6.12.1.1.8 *O.Management*

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

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

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

6.12.1.1.9 O.Log

O.Log defines that the TOE shall implement three different audit processes that are covered by the Security Functional Requirements as follows:

System Log

The implementation of the system log itself is covered by the use of **FAU_GEN.1/SYS**. **FAU_ARP.1/SYS** and **FAU_SAA.1/SYS** allow to define a set of criteria for automated analysis of the audit and a corresponding response. **FAU_SAR.1/SYS** defines the requirements around the audit review functions and that access to them shall be limited to authorised Gateway Administrators via the IF_GW_WAN interface and to authorised Service Technicians via the IF_GW_SRV interface. Finally, **FAU_STG.4/SYS** defines the requirements on what should happen if the audit log is full.

Consumer Log

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

Calibration Log

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

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

6.12.1.1.10 O.Access

FDP_ACC.2 and **FDP_ACF.1** define the access control policy as required to address O.Access. **FIA_UAU.5** ensures that entities that would like to communicate with the TOE are authenticated before any action whereby **FIA_UAU.6** ensures that external entities

2622 in the WAN are re-authenticated after the session key has been used for a certain
2623 amount of time.

2624 6.12.1.2 Fulfilment of the dependencies

2625 The following table summarises all TOE functional requirements dependencies of this
2626 ST and demonstrates that they are fulfilled.

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

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

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

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

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

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

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

Table 18: SFR Dependencies

6.12.1.3 Justification for missing dependencies

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

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

6.12.2 Security Assurance Requirements rationale

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

In order to keep evaluations according to this Security Target commercially feasible EAL 4 has been chosen as assurance level as this is the lowest level that provides the prerequisites for the use of AVA_VAN.5.

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

6.12.2.1 Dependencies of assurance components

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

7 TOE Summary Specification

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

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

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

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

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

The following elliptical curves are supported by the TOE

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

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

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

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

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

The following communication types are known to the TOE ²²²:

- a) WAN communication via IF_GW_WAN

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

- 2714 b) LMN communication via IF_GW_MTR (wireless or wired Meter)
- 2715 c) HAN communication via IF_GW_CON, IF_GW_CLS or IF_GW_SRV
- 2716 Except the communication with wireless meters at IF_GW_MTR, all communication
- 2717 types are TLS-based. In order to accept a TLS communication connection as being au-
- 2718 thenticated, the following conditions must be fulfilled:
- 2719 a) The TLS channel must have been established successfully with the required
- 2720 cryptographic mechanisms.
- 2721 b) The certificate of the external entity must be known and trusted through config-
- 2722 uration by the Gateway Administrator, and associated with the according com-
- 2723 munication type²²³.
- 2724 For the successfully authenticated external entity, the TOE performs an internal assign-
- 2725 ment of the communication type based on the certificate received at the external inter-
- 2726 face if applicable. The user identity is associated with the name of the certificate owner
- 2727 in case of a certificate-based authentication or with the user name in case of a password-
- 2728 based authentication at interface IF_GW_CON.
- 2729 For the LMN communication of the TOE with wireless (a.k.a. wM-Bus-based) meters,
- 2730 the external entity is authenticated by the use of the AES-CMAC algorithm and the me-
- 2731 ter-ID for wired Meters is used for association to the user identity (**FIA_USB.1**). This
- 2732 communication is only allowed for meters not supporting TLS-based communication
- 2733 scenarios.
- 2734 **FCS_CKM.1/TLS** is fulfilled by the TOE through the implementation of the pseudoran-
- 2735 dom function of the TLS protocol compliant to [RFC 5246] while the Security Module is
- 2736 used by the TOE for the generation of the cryptographic key material. The use of TLS
- 2737 according to [RFC 5246] and the use of the postulated cipher suites according to
- 2738 [RFC 5639] fulfill the requirement **FCS_COP.1/TLS**. The requirements
- 2739 **FCS_CKM.1/MTR** and **FCS_COP.1/MTR** are fulfilled by the use of AES-CMAC-secured
- 2740 communication for wireless meters. The requirement **FCS_CKM.4** is fulfilled by the de-
- 2741 scribed method of “zeroisation” when destroying cryptographic key material. The imple-
- 2742 mentation of the described mechanisms (especially the use of TLS and AES-CBC with
- 2743 CMAC) fulfills the requirements **FTP_ITC.1/WAN**, **FTP_ITC.1/MTR**, and

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

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

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

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

In case of wireless meter communication (via the wM-Bus protocol), the security attribute of the Meter is the meter-id authenticated by the CMAC, where the meter-id is the identity providing criterion that is used by the TOE. The identity of the Meter is associated to the

2779 successfully authenticated external entity by the TOE and linked to the respective role
2780 according to Table 5 and its active session. In this case, the identity providing criterion
2781 is also the meter-id.

2782 The TOE enforces an explicit and complete security policy protecting the data flow for
2783 all external entities (**FDP_IFC.2/FW**, **FDP_IFF.1/FW**, **FDP_IFC.2/MTR**,
2784 **FDP_IFF.1/MTR**). The security policy defines the accessibility of data for each external
2785 entity and additionally the permitted actions for these data. Moreover, the external enti-
2786 ties do also underlie restrictions for the operations which can be executed with the TOE
2787 (**FDP_ACF.1**). In case that it is not possible to authenticate an external entity success-
2788 fully (e.g. caused by unknown authentication credentials), no other action is allowed on
2789 behalf of this user and the concerning connection is terminated (**FIA_UAU.2**). Any com-
2790 munication is only possible after successful authentication and identification of the ex-
2791 ternal entity (**FIA_UID.2**, **FIA_USB.1**).

2792 The reception of the wake-up service data package is a special case that requests the
2793 TOE to establish a TLS authenticated and protected connection to the Gateway Admin-
2794 istrator. The TOE validates the data package due to its compliance to the structure de-
2795 scribed in [TR-03109-1] and verifies the ECDSA signature with the public key of the
2796 Gateway Administrator's certificate which must be known and trusted to the TOE. The
2797 TOE does not perform a revocation check or any validity check compliant to the shell
2798 model. The TOE verifies the electronic signature successfully when the certificate is
2799 known, trusted and associated to the Gateway Administrator. The TOE establishes the
2800 connection to the Gateway Administrator when the package has been validated due to
2801 its structural conformity, the signature has been verified and the integrated timestamp
2802 fulfills the requirements of [TR-03109-1]. Receiving the data package and the successful
2803 validation of the wake-up package does not mean that the Gateway Administrator has
2804 successfully been authenticated.

2805 If the Gateway Administrator could be successfully authenticated based on the certificate
2806 submitted during the TLS handshake phase, the role will be assigned by the TOE ac-
2807 cording to now approved identity based on the internal role model and the TLS channel
2808 will be established.

2809 **WAN roles**

2810 The TOE assigns the following roles in the WAN communication (**FMT_SMR.1**):

- 2811 • authorised Gateway Administrator,
- 2812 • authorised External Entity.

2813 The role assignment is based on the X.509 certificate used by the external entity during
2814 TLS connection establishment. The TOE has explicit knowledge of the Gateway Admin-
2815 istrator's certificate and the assignment of the role "Gateway Administrator" requires the
2816 successful authentication of the WAN connection.

2817 The assignment of the role "Authorized External Entity" requires the X.509 certificate
2818 that is used during the TLS handshake to be part of an internal trust list that is under
2819 control of the TOE.

2820 The role "Authorized External Entity" can be assigned to more than one external entity.

2821 **HAN roles**

2822 The TOE differentiates and assigns the following roles in the HAN communication
2823 (**FMT_SMR.1**):

- 2824 • authorised Consumer
- 2825 • authorised Service Technician

2826 The role assignment is based on the X.509 certificate used by the external entity for
2827 TLS-secured communication channels or on password-based authentication at interface
2828 IF_GW_CON if configured (**FIA_USB.1**).

2829 The assignment of roles in the HAN communication requires the successful identification
2830 of the external entity as a result of a successful authentication based on the certificate
2831 used for the HAN connection. The certificates used to authenticate the "Consumer" or
2832 the "Service Technician" are explicitly known to the TOE through configuration by the
2833 Gateway Administrator.

2834 **Multi-client capability in the HAN**

2835 The HAN communication might use more than one, parallel and independent authenti-
2836 cated communication channels. The TOE ensures that the certificates that are used for
2837 the authentication are different from each other.

2838 The role "Consumer" can be assigned to multiple, parallel sessions. The TOE ensures
2839 that these parallel sessions are logically distinct from each other by the use of different
2840 authentication information. This ensures that only the Meter Data associated with the
2841 authorized user are provided and Meter Data of other users are not accessible.

2842 **LMN roles**

2843 One of the following authentication mechanisms is used for Meters:

- 2844 a) authentication by the use of TLS according to [RFC 5246] for wired Meters
2845 a) authentication by the use of AES with CMAC authentication according to
2846 [RFC 3394] for wireless Meters.

2847 The TOE explicitly knows the identification credentials needed for authentication (X.509
2848 certificate when using TLS; meter-id in conjunction with CMAC and known K_{mac} when
2849 using AES) through configuration by the Gateway Administrator. If the Meter could be
2850 successfully authenticated and the claimed identity could thus be proved, the according
2851 role “Authorised External Entity” is assigned by the TOE for this Meter at IF_GW_MTR
2852 based on the internal role model.

2853 **LMN multi-client capabilities**

2854 The LMN communication can be run via parallel, logically distinct and separately au-
2855 thenticated communication channels. The TOE ensures that the authentication creden-
2856 tials of each separate channel are different.

2857 The TOE’s internal policy for access to data and objects under control of the TOE is
2858 closely linked with the identity of the external entity at IF_GW_MTR according to the
2859 TOE-internal role model. Based on the successfully verified authentication data, a per-
2860 mission catalogue with security attributes is internally assigned, which defines the al-
2861 lowed actions and access permissions within a communication channel.

2862 The encapsulation of the TOE processes run by this user is realized through the mech-
2863 anisms offered by the TOE’s operating system and very restrictive user rights for each
2864 process. Each role is assigned to a separate, limited user account in the TOE’s operating
2865 system. For all of these accounts, it is only allowed to read, write or execute the files
2866 absolutely necessary for implementing the program logic. For each identity interacting
2867 with the TOE, a separate operating system process is started. Especially, the databases
2868 used by the TOE and the logging service are adequately separated for enforcement of
2869 the necessary security domain separation (**FDP_ACF.1**). The allowed actions and ac-
2870 cess permissions and associated objects are assigned to the successfully approved
2871 identity of the user based on the used authentication credentials and the resulting asso-
2872 ciated role. The current session is unambiguously associated with this user. No interac-
2873 tion (e.g. access to Meter Data) is possible without an appropriate permission catalogue
2874 (**FDP_ACC.2**). The freeing of the role assignment and associated resources are ensured
2875 through the monitoring of the current session.

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

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

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

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

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

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

Closely linked with the deposition of the Meter Data is the assignment of an unambiguous and reliable timestamp on these data. The reliability grounds on the regular use of an external time source offering a sufficient exactness (**FPT_STM.1**) which is used to synchronize the operating system of the TOE. A maximum deviation of 3% of the measuring period is allowed to be in conformance with [PP_GW]. The data set (Meter Data and tariff data) is associated with the timestamp in an inseparably manner because each Meter Data entry in the database includes the corresponding time stamp and the database is cryptographically protected through the encrypted file system. For details about database encryption please see page 152).

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

The TOE does also foresee the case that the data is encrypted for an external entity that is not directly assigned to the external entity holding the active communication channel. The electronic signature is created through the utilization of the Security Module whereas

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

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

7.3SF.3: Administration, Configuration and SW Update

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

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

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

2977 A complete overview of the possible management functions is given in Table 14 and
2978 Table 15 (**FMT_SMF.1**). Beside the possibility for a successfully authenticated Service
2979 Technician to view the system log via interface IF_GW_SRV, administrative or configu-
2980 ration measures on the TOE can only be taken by the successfully authenticated Gate-
2981 way Administrator.

2982 In order to perform these measures, the TOE has to establish a TLS secured channel
2983 to the Gateway Administrator and must authenticate the Gateway Administrator suc-
2984 cessfully. There are two possibilities:

- 2985 a) The TOE independently contacts the Gateway Administrator at a certain time
2986 specified in advance by the Gateway Administrator.
- 2987 b) Through a message sent to the wake-up service, the TOE is requested to con-
2988 tact the Gateway Administrator.

2989 In the second case, the wake-up data packet is received by the TOE from the WAN and
2990 checked by the TOE for structural correctness according to [TR-03109-1]. Afterwards,
2991 the TOE verifies the correctness of the electronic signature applied to the wake-up mes-
2992 sage data packet using the certificate of the Gateway Administrator stored in the TSF
2993 data. Afterwards, a TLS connection to the Gateway Administrator is established by the
2994 TOE and the above mentioned operations can be performed.

2995 Software/firmware updates always have to be signed by the TOE manufacturer.

2996 Software/firmware updates can be of different content:

- 2997 a) The whole boot image of the TOE is changed.
- 2998 b) Only individual components of the TOE are changed. These components can
2999 be the boot loader plus the static kernel or the SMGW application.

3000 The update packet is realized in form of an archive file enveloped into a CMS signature
3001 container according to [RFC 5652]. The electronic signature of the update packet is cre-
3002 ated using signature keys from the TOE manufacturer. The verification of this signature
3003 is performed by the TOE using the TOE's Security Module using the trust anchor of the
3004 TOE manufacturer. If the signature of the transferred data could not be successfully
3005 verified by the TOE or if the version number of the new firmware is not higher than the
3006 version number of the installed firmware, the received data is rejected by the TOE and
3007 not used for further processing. Any administrator action is entered in the System Log of
3008 the TOE. Additionally, an authorised Consumer can interact with the TOE via the

3009 interface IF_GW_CON to get the version number and the current time displayed
3010 (**FMT_MOF.1**).

3011 The signature of the update packet is immediately verified after receipt. After successful
3012 verification of the update packet the update process is immediately performed. In each
3013 case, the Gateway Administrator gets notified by the TOE and an entry in the TOE's
3014 system log will be written.

3015 All parameters that can be changed by the Gateway Administrator are preset with re-
3016 strictive values by the TOE. No role can specify alternative initial values to override these
3017 restrictive default values (**FMT_MSA.3/AC**, **FMT_MSA.3/FW**, **FMT_MSA.3/MTR**).

3018 This mechanism is supported by the TOE-internal resource monitor that internally mon-
3019 itors existing connections, assigned roles and operations allowed at a specific time.

3020

3021 **7.4 SF.4: Displaying Consumption Data**

3022 The TOE offers the possibility of displaying consumption data to authenticated Consum-
3023 ers at interface IF_GW_CON. Therefore, the TOE contains a web server that implements
3024 TLS-based communication with mutual authentication (**FTP_ITC.1/USR**). If the Con-
3025 sumer requests a password-based authentication from the GWA according to [TR-
3026 03109-1] and the GWA activates this authentication method for this Consumer, the TOE
3027 uses TLS authentication with server-side authentication and HTTP digest access au-
3028 thentication according to [RFC 7616]. In both cases, the requirement **FCO_NRO.2** is
3029 fulfilled through the use of TLS-based communication and through encryption and digital
3030 signature of the (tariffed) Meter Data to be displayed using **FCS_COP.1/HASH**.

3031 To additionally display consumption data, a connection at interface IF_GW_CON must
3032 be established and the role "(authorised) Consumer" is assigned to the user with his
3033 used display unit by the TOE. Different Consumer can use different display units. The
3034 amount of allowed connection attempts at IF_GW_CON is set to 5. In case the amount
3035 of allowed connection attempts is reached, the TOE blocks IF_GW_CON (**FIA_AFL.1**).
3036 The display unit has to technically support the applied authentication mechanism and
3037 the HTTP protocol version 1.1 according to [RFC 2616] as communication protocol. Data
3038 is provided as HTML data stream and transferred to the display unit. In this case, further
3039 processing of the transmitted data stream is carried out by the display unit.

3040 According to [TR-03109-1], the TOE exclusively transfers Consumer specific consump-
3041 tion data to the display unit. The Consumer can be identified in a clear and unambiguous

manner due to the applied authentication mechanism. Moreover, the TOE ensures that exclusively the data actually assigned to the Consumer is provided at the display unit via IF_GW_CON (**FIA_USB.1**).

7.5 SF.5: Audit and Logging

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

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

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

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

If possible, each log entry is assigned to an identity that is known to the TOE. For audit events resulting from actions of identified users resp. roles, the TOE associates the

3074 generated log information to the identified users while generating the audit information
3075 (**FAU_GEN.2**).

3076 Generated audit and log data are stored in a cryptographically secured storage. For this
3077 purpose, a file-based SQL database system is used securing its' data using an AES-
3078 XTS-128 encrypted file system (AES in XTS mode with 128-bit keys) according to
3079 [FIPS Pub. 197] and [NIST 800-38E]. This is achieved by using device-specific AES
3080 keys so that the secure environment can only be accessed with the associated symmet-
3081 ric key available. Using an appropriately limited access of this symmetric, the TOE im-
3082 plements the necessary rules so that it can be ensured that unauthorised modification
3083 or deletion is prohibited (**FAU_STG.2**).

3084 Audit and log data are stored in separate locations: One location is used to store Con-
3085 sumer-specific log data (Consumer-Log) whereas device status data and metrological
3086 data are stored in a separate location: status data are stored in the System-Log and
3087 metrological data are stored in the Calibration-Log. Each of these logs is located in phys-
3088 ically separate databases secured by different cryptographic keys. In case of several
3089 external meters, a separate database is created for each Meter to store the respective
3090 consumption and log data (**FAU_GEN.2**).

3091 If the audit trail of the System-Log or the Consumer-Log is full (so that no further data
3092 can be added), the oldest entries in the audit trail are overwritten (**FAU_STG.2**,
3093 **FAU_STG.4/SYS**, **FAU_STG.4/CON**). If the Consumer-Log's oldest audit record must
3094 be kept because the period of billing verification (of usually 15 months) has not been
3095 reached, the TOE's metrological activity is paused until the oldest audit record gets
3096 deletable. Thereafter, the TOE's metrological activity is started again through an internal
3097 timer. Moreover, the mechanism for storing log entries is designed in a way that these
3098 entries are cryptographically protected against unauthorized deletion. This is especially
3099 achieved by assigning cryptographic keys to each of the individual databases for the
3100 System-Log, Consumer-Log and Calibration-Log.

3101 If the Calibration-Log cannot store any further data, the operation of the TOE is stopped
3102 through the termination of its metering services and the TOE informs the Gateway Ad-
3103 ministrator by creating an entry in the System-Log, so that additional measures can be
3104 taken by the Gateway Administrator. Calibration-Log entries are never overwritten by
3105 the TOE (**FAU_STG.2**, **FAU_STG.4/CAL**, **FMT_MOF.1**).

3106 The TOE anonymizes the data in a way that no conclusions about a specific person or
3107 user can be drawn from the log or recorded not billing relevant data. Stored consumption

data are exclusively intended for accounting with the energy supplier. The data stored in the System-Log are used for analysis purposes concerning necessary technical analyses and possible security-related information.

7.6 SF.6: TOE Integrity Protection

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

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

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

3140 of the device, and the further use of the TOE for the purpose of gathering Meter Data is
3141 not allowed (**FPT_FLS.1**).

3142 Basically, if an integrity violation is detected, the TOE will create an entry in the System
3143 Log to document this status for the authorised Gateway Administrator on interface
3144 IF_GW_WAN resp. for the authorised Service Technician on interface IF_GW_SRV, and
3145 will inform the Gateway Administrator on this incident (**FAU_ARP.1/SYS**,
3146 **FAU_GEN.1/SYS**, **FAU_SAR.1/SYS**, **FPT_TST.1**).

3147 **7.7 TSS Rationale**

3148 The following table shows the correspondence analysis for the described TOE security
3149 functionalities and the security functional requirements.

	SE.1	SE.2	SE.3	SE.4	SE.5	SE.6
FAU_ARP.1/SYS					X	(X)
FAU_GEN.1/SYS					X	(X)
FAU_SAA.1/SYS					X	
FAU_SAR.1/SYS					X	(X)
FAU_STG.4/SYS					X	
FAU_GEN.1/CON					X	
FAU_SAR.1/CON					X	
FAU_STG.4/CON					X	
FAU_GEN.1/CAL					X	
FAU_SAR.1/CAL					X	
FAU_STG.4/CAL					X	
FAU_GEN.2					X	

	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6
FAU_STG.2					X	
FCO_NRO.2		X		X		
FCS_CKM.1/TLS	X					
FCS_COP.1/TLS	X					
FCS_CKM.1/CMS		X				
FCS_COP.1/CMS		X				
FCS_CKM.1/MTR	X	X				
FCS_COP.1/MTR	X	X				
FCS_CKM.4	X	X				
FCS_COP.1/HASH		X				
FCS_COP.1/MEM		X				
FDP_ACC.2	X					
FDP_ACF.1	X					
FDP_IFC.2/FW	X					
FDP_IFF.1/FW	X					
FDP_IFC.2/MTR	X					
FDP_IFF.1/MTR	X					
FDP_RIP.2	X	X				
FDP_SDI.2		X			X	

	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6
FIA_ATD.1	X					
FIA_AFL.1				X		
FIA_UAU.2	X					
FIA_UAU.5	X					
FIA_UAU.6	X					
FIA_UID.2	X					
FIA_USB.1	X			X		
FMT_MOF.1			X		X	
FMT_SMF.1			X			
FMT_SMR.1	X					
FMT_MSA.1/AC			X			
FMT_MSA.3/AC			X			
FMT_MSA.1/FW			X			
FMT_MSA.3/FW			X			
FMT_MSA.1/MTR			X			
FMT_MSA.3/MTR			X			
FPR_CON.1		X				
FPR_PSE.1		X				
FPT_FLS.1						X

	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6
FPT_RPL.1	X	X				X
FPT_STM.1		X				
FPT_TST.1						X
FPT_PHP.1						X
FTP_ITC.1/WAN	X					
FTP_ITC.1/MTR	X					
FTP_ITC.1/USR	X			X		

3150 **Table 19: Rationale for the SFR and the TOE Security Functionalities** ²²⁴

²²⁴ Please note that SFRs marked with “(X)” only have supporting effect on the fulfilment of the TSF.

8 List of Tables

TABLE 1: SMART METER GATEWAY PRODUCT CLASSIFICATIONS..... 10

TABLE 2: COMMUNICATION FLOWS BETWEEN DEVICES IN DIFFERENT NETWORKS 23

TABLE 3: MANDATORY TOE EXTERNAL INTERFACES..... 28

TABLE 4: CRYPTOGRAPHIC SUPPORT OF THE TOE AND ITS SECURITY MODULE 29

TABLE 5: ROLES USED IN THE SECURITY TARGET 35

TABLE 6: ASSETS (USER DATA) 37

TABLE 7: ASSETS (TSF DATA) 38

TABLE 8: RATIONALE FOR SECURITY OBJECTIVES 55

TABLE 9: LIST OF SECURITY FUNCTIONAL REQUIREMENTS 66

TABLE 10: OVERVIEW OVER AUDIT PROCESSES 68

TABLE 11: EVENTS FOR CONSUMER LOG 73

TABLE 12: CONTENT OF CALIBRATION LOG 78

TABLE 13: RESTRICTIONS ON MANAGEMENT FUNCTIONS..... 107

TABLE 14: SFR RELATED MANAGEMENT FUNCTIONALITIES 112

TABLE 15: GATEWAY SPECIFIC MANAGEMENT FUNCTIONALITIES 113

TABLE 16: ASSURANCE REQUIREMENTS..... 124

TABLE 17: FULFILMENT OF SECURITY OBJECTIVES 128

TABLE 18: SFR DEPENDENCIES 138

TABLE 19: RATIONALE FOR THE SFR AND THE TOE SECURITY FUNCTIONALITIES 157

9 List of Figures

FIGURE 1: THE TOE AND ITS DIRECT ENVIRONMENT 12

FIGURE 2: THE LOGICAL INTERFACES OF THE TOE 14

FIGURE 3: THE PRODUCT WITH ITS TOE AND NON-TOE PARTS 16

FIGURE 4: THE TOE'S PROTOCOL STACK..... 18

FIGURE 5: CRYPTOGRAPHIC INFORMATION FLOW FOR DISTRIBUTED METERS AND GATEWAY
..... 31

10 Appendix

10.1 Mapping from English to German terms

English term	German term
billing-relevant	abrechnungsrelevant
CLS, Controllable Local System	dezentral steuerbare Verbraucher- oder Erzeugersysteme
Consumer	Anschlussnutzer; Letztverbraucher (im verbrauchenden Sinne); u.U. auch Einspeiser
Consumption Data	Verbrauchsdaten
Gateway	Kommunikationseinheit
Grid	Netz (für Strom/Gas/Wasser)
Grid Status Data	Zustandsdaten des Versorgungsnetzes
LAN, Local Area Network	Lokales Kommunikationsnetz
LMN, Local Metrological Network	Lokales Messeinrichtungsnetz
Meter	Messeinrichtung (Teil eines Messsystems)
Processing Profiles	Konfigurationsprofile
Security Module	Sicherheitsmodul (z.B. eine Smart Card)
Service Provider	Diensteanbieter
Smart Meter, Smart Metering System ²²⁵	Intelligente, in ein Kommunikationsnetz eingebundene, elektronische Messeinrichtung (Messsystem)
TOE	EVG (E valuierungs g egenstand)

²²⁵ Please note that the terms "Smart Meter" and "Smart Metering System" are used synonymously within this document.

WAN, Wide Area Network	Weitverkehrsnetz (für Kommunikation)
------------------------	--------------------------------------

3182

3183 **10.2 Glossary**

Term	Description
Authenticity	property that an entity is what it claims to be (according to [SD_6])
Block Tariff	Tariff in which the charge is based on a series of different energy/volume rates applied to successive usage blocks of given size and supplied during a specified period. (according to [CEN])
BPL	<i>Broadband Over Power Lines</i> , a method of power line communication
CA	Certification Authority, an entity that issues digital certificates. CLS config
CDMA	<i>Code Division Multiple Access</i>
CLS config (secondary asset)	See chapter 3.2
CMS	Cryptographic Message Syntax
Confidentiality	the property that information is not made available or disclosed to unauthorised individuals, entities, or processes (according to [SD_6])
Consumer	End user of electricity, gas, water or heat (according to [CEN]). See chapter 3.1
DCP	<i>Data Co-Processor</i> , security hardware of the CPU
DLMS	Device Language Message Specification
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level

Term	Description
Energy Service Provider	Organisation offering energy related services to the Consumer (according to [CEN])
ETH	Ethernet
external entity	See chapter 3.1
firmware update	See chapter 3.2
Gateway Administrator (GWA)	See chapter 3.1
Gateway config (secondary asset)	See chapter 3.2
Gateway time	See chapter 3.2
G.hn	Gigabit Home Networks
GPRS	<i>General Packet Radio Service</i> , a packet oriented mobile data service
Home Area Network (HAN)	In-house data communication network which interconnects domestic equipment and can be used for energy management purposes (adopted according to [CEN]).
Integrity	property that sensitive data has not been modified or deleted in an unauthorised and undetected manner (according to [SD_6])
IT-System	Computersystem
Local Area Network (LAN)	Data communication network, connecting a limited number of communication devices (Meters and other devices) and covering a moderately sized geographical area within the premises of the consumer. In the context of this ST, the term LAN is used as a hypernym for HAN and LMN (according to [CEN], adopted).

Term	Description
Local attacker	See chapter 3.4
LTE	<i>Long Term Evolution</i> mobile broadband communication standard
Meter config (secondary asset)	See chapter 3.2
Local Metrological Network (LMN)	In-house data communication network which interconnects metrological equipment.
Meter Data	See chapter 3.2
Meter Data Aggregator (MDA)	Entity which offers services to aggregate metering data by grid supply point on a contractual basis. NOTE: The contract is with a supplier. The aggregate is of all that supplier's consumers connected to that particular grid supply point. The aggregate may include both metered data and data estimated by reference to standard load profiles (adopted from [CEN])
Meter Data Collector (MDC)	Entity which offers services on a contractual basis to collect metering data related to a supply and provide it in an agreed format to a data aggregator (that can also be the DNO). NOTE: The contract is with a supplier or a pool. The collection may be carried out by manual or automatic means. ([CEN])
Meter Data Management System (MDMS)	System for validating, storing, processing and analysing large quantities of Meter Data. ([CEN])
Metrological Area Network	In-house data communication network which interconnects metrological equipment (i.e. Meters)
OEM	Original Equipment Manufacturer
OMS	Open Metering System

Term	Description
OCOTP	On-Chip One-time-programmable
Personally Identifiable Information (PII)	Personally Identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
RJ45	registered jack #45; a standardized physical network interface
RMII	Reduced Media Independent Interface
RTC	Real Time Clock
Service Technician	Human entity being responsible for diagnostic purposes.
Smart Metering System	The Smart Metering System consists of a Smart Meter Gateway and connected to one or more meters. In addition, CLS (i.e. generation plants) may be connected with the gateway for dedicated communication purposes.
SML	Smart Message Language
Tariff	Price structure (normally comprising a set of one or more rates of charge) applied to the consumption or production of a product or service provided to a Consumer (according to [CEN]).
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security protocol according to [RFC 5246]
TOE	Target of Evaluation - set of software, firmware and/or hardware possibly accompanied by guidance
TSF	TOE security functionality
UART	Universal Asynchronous Receiver Transmitter

Term	Description
WAN attacker	See chapter 3.4
WLAN	Wireless Local Area Network

3184 11 Literature

- 3185 [CC] Common Criteria for Information Technology Security
3186 Evaluation –
3187 Part 1: Introduction and general model, April 2017, ver-
3188 sion 3.1, Revision 5, CCMB-2017-04-001,
3189 [https://www.commoncriteriapor-](https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf)
3190 [tal.org/files/ccfiles/CCPART1V3.1R5.pdf](https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf)
3191 Part 2: Security functional requirements, April 2017, ver-
3192 sion 3.1, Revision 5, CCMB-2017-04-002,
3193 [https://www.commoncriteriapor-](https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf)
3194 [tal.org/files/ccfiles/CCPART2V3.1R5.pdf](https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf)
3195 Part 3: Security assurance requirements, April 2017, ver-
3196 sion 3.1, Revision 5, CCMB-2017-04-003,
3197 [https://www.commoncriteriapor-](https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf)
3198 [tal.org/files/ccfiles/CCPART3V3.1R5.pdf](https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf)
3199 [CEN] SMART METERS CO-ORDINATION GROUP (SM-CG)
3200 Item 5. M/441 first phase deliverable – Communication –
3201 Annex: Glossary (SMCG/Sec0022/DC)
3202 [PP_GW] Protection Profile for the Gateway of a Smart Metering
3203 System (Smart Meter Gateway PP), Schutzprofil für die
3204 Kommunikationseinheit eines intelligenten Messsystems
3205 für Stoff- und Energiemengen, SMGW-PP, v.1.3, Bundes-
3206 amt für Sicherheit in der Informationstechnik, 31.03.2014
3207 [SecModPP] Protection Profile for the Security Module of a Smart Me-
3208 ter Gateway (Security Module PP), Schutzprofil für das
3209 Sicherheitsmodul der Kommunikationseinheit eines intelli-
3210 genten Messsystems für Stoff- und Energiemengen,
3211 SecMod-PP, Version 1.0.2, Bundesamt für Sicherheit in
3212 der Informationstechnik, 18.10.2013
3213 [SD_6] ISO/IEC JTC 1/SC 27 N7446, Standing Document 6
3214 (SD6): Glossary of IT Security Terminology 2009-04-29,
3215 available at

3216		http://www.teletrust.de/uploads/me-
3217		dia/ISOIEC_JTC1_SC27_IT_Security_Glossary_Tele-
3218		TrusT_Documentation.pdf
3219	[TR-02102]	Technische Richtlinie BSI TR-02102, Kryptographische
3220		Verfahren: Empfehlungen und Schlüssellängen, Bundes-
3221		amt für Sicherheit in der Informationstechnik, Version
3222		2022-01
3223	[TR-03109]	Technische Richtlinie BSI TR-03109, Version 1.1, Bun-
3224		desamt für Sicherheit in der Informationstechnik,
3225		22.09.2021
3226	[TR-03109-1]	Technische Richtlinie BSI TR-03109-1, Anforderungen an
3227		die Interoperabilität der Kommunikationseinheit eines
3228		Messsystems, Version 1.1, Bundesamt für Sicherheit in
3229		der Informationstechnik, 17.09.2021
3230	[TR-03109-1-I]	Technische Richtlinie BSI TR-03109-1 Anlage I, CMS-
3231		Datenformat für die Inhaltsdatenverschlüsselung und -
3232		signatur, Version 1.0.9, Bundesamt für Sicherheit in der
3233		Informationstechnik, 18.03.2013
3234	[TR-03109-1-VI]	Technische Richtlinie BSI TR-03109-1 Anlage VI, Be-
3235		triebsprozesse, Version 1.0, Bundesamt für Sicherheit in
3236		der Informationstechnik, 18.03.2013
3237	[TR-03109-2]	Technische Richtlinie BSI TR-03109-2, Smart Meter Ga-
3238		teway – Anforderungen an die Funktionalität und In-
3239		teroperabilität des Sicherheitsmoduls, Version 1.1, Bun-
3240		desamt für Sicherheit in der Informationstechnik,
3241		15.12.2014
3242	[TR-03109-3]	Technische Richtlinie BSI TR-03109-3, Kryptographische
3243		Vorgaben für die Infrastruktur von intelligenten Messsys-
3244		temen, Version 1.1, Bundesamt für Sicherheit in der Infor-
3245		mationstechnik, 17.04.2014
3246	[TR-03109-4]	Technische Richtlinie BSI TR-03109-4, Smart Metering
3247		PKI - Public Key Infrastruktur für Smart Meter Gateways,

3248		Version 1.2.1, Bundesamt für Sicherheit in der Informati-
3249		onstechnik, 09.08.2017
3250	[TR-03109-6]	Technische Richtlinie BSI TR-03109-6, Smart Meter Ga-
3251		teway Administration, Version 1.0, Bundesamt für Sicher-
3252		heit in der Informationstechnik, 26.11.2015
3253	[TR-03111]	Technische Richtlinie BSI TR-03111, Elliptic Curve Cryp-
3254		tography (ECC), Version 2.1, 01.06.2018
3255	[TR-03116-3]	Technische Richtlinie BSI TR-03116-3, Kryptographische
3256		Vorgaben für Projekte der Bundesregierung, Teil 3 - Intel-
3257		ligente Messsysteme, Stand 2023, Bundesamt für Sicher-
3258		heit in der Informationstechnik, 06.12.2022
3259	[AGD_Consumer]	Handbuch für Verbraucher, Smart Meter Gateway, Ver-
3260		sion 4.12, 15.12.2023, Power Plus Communications AG
3261	[AGD_Techniker]	Handbuch für Service-Techniker, Smart Meter Gateway,
3262		Version 5.8, 01.02.2024, Power Plus Communications
3263		AG
3264	[AGD_GWA]	Handbuch für Hersteller von Smart-Meter Gateway-Admi-
3265		nistrations-Software, Smart Meter Gateway, Version 4.15,
3266		26.01.2024, Power Plus Communications AG
3267	[AGD_SEC]	Auslieferungs- und Fertigungsprozeduren, Anhang Si-
3268		chere Auslieferung, Version 1.15, 02.12.2024, Power
3269		Plus Communications AG
3270	[SMGW_Logging]	Logmeldungen, SMGW Version 1.3 & 2.1 & 2.1.1, Version
3271		3.4, 23.06.2023, Power Plus Communications AG
3272	[FIPS Pub. 140-2]	NIST, FIPS 140-3, Security Requirements for crypto-
3273		graphic modules, 2019
3274	[FIPS Pub. 180-4]	NIST, FIPS 180-4, Secure Hash Standard, 2015
3275	[FIPS Pub. 197]	NIST, FIPS 197, Advances Encryption Standard (AES),
3276		2001
3277	[IEEE 1901]	IEEE Std 1901-2010, IEEE Standard for Broadband over
3278		Power Line Networks: Medium Access Control and Physi-
3279		cal Layer Specifications, 2010

3280	[IEEE 802.3]	IEEE Std 802.3-2008, IEEE Standard for Information
3281		technology, Telecommunications and information ex-
3282		change between systems, Local and metropolitan area
3283		networks, Specific requirements, 2008
3284	[ISO 10116]	ISO/IEC 10116:2006, Information technology -- Security
3285		techniques -- Modes of operation for an n-bit block cipher,
3286		2006
3287	[NIST 800-38A]	NIST Special Publication 800-38A, Recommendation for
3288		Block Cipher Modes of Operation: Methods and Tech-
3289		niques, December 2001, http://nvl-
3290		pubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublica-
3291		tion800-38a.pdf
3292	[NIST 800-38D]	NIST Special Publication 800-38D, Recommendation for
3293		Block Cipher Modes of Operation: Galois/Counter Mode
3294		(GCM) and GMAC, M. Dworkin, November 2007,
3295		http://csrc.nist.gov/publications/nistpubs/800-38D/SP-
3296		800-38D.pdf
3297	[NIST 800-38E]	NIST Special Publication 800-38E, Recommendation for
3298		Block Cipher Modes of Operation: The XTS-AES Mode
3299		for Confidentiality on Storage Devices, M. Dworkin, Janu-
3300		ary, 2010, http://csrc.nist.gov/publications/nistpubs/800-
3301		38E/nist-sp-800-38E.pdf
3302	[RFC 2104]	RFC 2104, HMAC: Keyed-Hashing for Message Authenti-
3303		cation, M. Bellare, R. Canetti und H. Krawczyk, February
3304		1997, http://rfc-editor.org/rfc/rfc2104.txt
3305	[RFC 2616]	RFC 2616, Hypertext Transfer Protocol - HTTP/1.1, R.
3306		Fielding, J. Gettys, J. Mogul, H. Frystyk, P. Masinter, P.
3307		Leach, T. Berners-Lee, June 1999, http://rfc-edi-
3308		tor.org/rfc/rfc2616.txt
3309	[RFC 7616]	RFC 7616, HTTP Digest Access Authentication, R.
3310		Shekh-Yusef, D. Ahrens, S. Bremer, September 2015,
3311		http://rfc-editor.org/rfc/rfc7616.txt

3312	[RFC 3394]	RFC 3394, Schaad, J. and R. Housley, Advanced En-
3313		cryption Standard (AES) Key Wrap Algorithm, September
3314		2002, http://rfc-editor.org/rfc/rfc3394.txt
3315	[RFC 3565]	RFC 3565, J. Schaad, Use of the Advanced Encryption
3316		Standard (AES) Encryption Algorithm in Cryptographic
3317		Message Syntax (CMS), July 2003, http://rfc-editor.org/rfc/rfc3565.txt
3318		
3319	[RFC 4493]	IETF RFC 4493, The AES-CMAC Algorithm, J. H. Song, J.
3320		Lee, T. Iwata, June 2006, http://www.rfc-editor.org/rfc/rfc4493.txt
3321		
3322	[RFC 5083]	RFC 5083, R. Housley, Cryptographic Message Syntax
3323		(CMS)
3324		Authenticated-Enveloped-Data Content Type, November
3325		2007, http://www.ietf.org/rfc/rfc5083.txt
3326	[RFC 5084]	RFC 5084, R. Housley, Using AES-CCM and AES-GCM
3327		Authenticated Encryption in the Cryptographic Message
3328		Syntax (CMS), November 2007,
3329		http://www.ietf.org/rfc/rfc5084.txt
3330	[RFC 5114]	RFC 5114, Additional Diffie-Hellman Groups for Use with
3331		IETF Standards, M. Lepinski, S. Kent, January 2008,
3332		http://www.ietf.org/rfc/rfc5114.txt
3333	[RFC 5246]	RFC 5246, T. Dierks, E. Rescorla, The Transport Layer
3334		Security (TLS) Protocol Version 1.2, August 2008,
3335		http://www.ietf.org/rfc/rfc5246.txt
3336	[RFC 5289]	RFC 5289, TLS Elliptic Curve Cipher Suites with SHA-
3337		256/384 and AES Galois Counter Mode (GCM), E.
3338		Rescorla, RTFM, Inc., August 2008,
3339		http://www.ietf.org/rfc/rfc5289.txt
3340	[RFC 5639]	RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool
3341		Standard Curves and Curve Generation, M. Lochter, BSI,
3342		J. Merkle, secunet Security Networks, March 2010,
3343		http://www.ietf.org/rfc/rfc5639.txt

3344	[RFC 5652]	RFC 5652, Cryptographic Message Syntax (CMS), R.
3345		Housley, Vigil Security, September 2009,
3346		http://www.ietf.org/rfc/rfc5652.txt
3347	[EIA RS-485]	EIA Standard RS-485, Electrical Characteristics of Gener-
3348		ators and Receivers for Use in Balanced Multipoint Sys-
3349		tems, ANSI/TIA/EIA-485-A-98, 1983/R2003
3350	[EN 13757-1]	M-Bus DIN EN 13757-1: Kommunikationssysteme für
3351		Zähler und deren Fernablesung Teil 1: Datenaustausch
3352	[EN 13757-3]	M-Bus DIN EN 13757-3, Kommunikationssysteme für
3353		Zähler und deren Fernablesung Teil 3: Spezielle Anwen-
3354		dungsschicht
3355	[EN 13757-4]	M-Bus DIN EN 13757-4, Kommunikationssysteme für
3356		Zähler und deren Fernablesung Teil 4: Zählerauslesung
3357		über Funk, Fernablesung von Zählern im SRD-Band von
3358		868 MHz bis 870 MHz
3359	[IEC-62056-5-3-8]	Electricity metering – Data exchange for meter reading,
3360		tariff and load control – Part 5-3-8: Smart Message Lan-
3361		guage SML, 2012
3362	[IEC-62056-6-1]	IEC-62056-6-1, Datenkommunikation der elektrischen
3363		Energiemessung, Teil 6-1: OBIS Object Identification Sys-
3364		tem, 2017, International Electrotechnical Commission
3365	[IEC-62056-6-2]	IEC-62056-6-2, Datenkommunikation der elektrischen
3366		Energiemessung - DLMS/COSEM, Teil 6-2: COSEM Inter-
3367		face classes, 2017, International Electrotechnical Commis-
3368		sion
3369	[IEC-62056-21]	IEC-62056-21, Direct local data exchange - Mode C, 2011,
3370		International Electrotechnical Commission
3371	[LUKS]	LUKS On-Disk Format Specification Version 1.2.1, Clem-
3372		ens Fruhwirth, October 16th, 2011
3373	[PACE]	The PACE-AA Protocol for Machine Readable Travel Doc-
3374		uments, and its Security, Jens Bender, Ozgur Dagdelen,

3375		Marc Fischlin and Dennis Kügler, http://fc12.ifca.ai/pre-proceedings/paper_49.pdf
3376		
3377	[X9.63]	ANSI X9.63, Public Key Cryptography for the Financial
3378		Services Industry: Key Agreement and Key Transport Us-
3379		ing Elliptic Curve Cryptography, 2011
3380	[G865]	DVGW-Arbeitsblatt G865 Gasabrechnung, 11/2008
3381	[VDE4400]	VDE-AR-N 4400:2011-09, Messwesen Strom, VDE-An-
3382		wendungsregel, 01.09.2011
3383	[DIN 43863-5]	DIN: Herstellerübergreifende Identifikationsnummer für
3384		Messeinrichtungen, 2012
3385	[USB]	Universal Serial Bus Specification, Revision 2.0, April 27,
3386		2000, USB Communications CLASS Specification for
3387		Ethernet Devices, http://www.usb.org/develop-
3388		ers/docs/usb20_docs/#usb20spec
3389	[ITU G.hn]	G.996x Unified high-speed wireline-based home network-
3390		ing transceivers, 2018
3391	[MSB-LK]	Anforderungskatalog zur MSB-Lieferkette, Version 1.0,
3392		Bundesamt für Sicherheit in der Informationstechnik



Power Plus Communications AG

Dudenstraße 6, 68167 Mannheim

Tel. 00 49 621 40165 100 | Fax. 00 49 621 40165 111

info@ppc-ag.de | www.ppc-ag.de