TECHNICAL SPECIFICATION

SECURITY TARGET
SMART GRID HUB - SECURE

IDENTIFIER:	ASE_ST
ISSUE:	V1.23, 22.12.2023
TARGET:	German Smart Meter Gateway
AUTHOR:	EFR GmbH
TOE REFERENCE:	SGH-S v1.01

Content

1 ST Introduction 5
1.1 TOE Reference 5
1.2 TOE Components And Identification 5
1.3 TOE Overview 7
1.3.1 Introduction 7
1.3.2 Overview of the Gateway in a Smart Metering System 7
1.3.3 TOE description 10
1.3.4 TOE type 10
1.3.5 TOE physical boundary 10
1.3.6 TOE logical boundary 12
1.3.7 The logical interfaces of the TOE 18
1.3.8 The cryptography of the TOE and its Security Module 19
1.3.9 TOE life-cycle 23
2 Conformance Claim (ASE_CCL) 23
2.1 Conformance statement 23
2.2 ST Conformance Claims 23
2.3 Conformance claim rationale 23
2.4 Package Claim 23
3 Security Problem Definition (ASE_SPD) 24
3.1 External entities 24
3.2 Assets 24
3.3 Assumptions 26
3.4 Threats 27
3.5 Organizational Security Policies 29
4 Security Objectives (ASE_OBJ) 30
4.1 Security objectives for the TOE 30
4.2 Security objectives for the operational environment 33
4.3 Security objectives rationale 34
4.3.1 Overview 34
4.3.2 Countering the threats 35
4.3.3 Coverage of organizational security policies 38
4.3.4 Coverage of assumptions 38

4.4 Security objectives conclusion 39
5 Extended Components definition 39
5.1 Communication concealing (FPR_CON) 39
5.1.1 Family behavior 39
5.1.2 Component levelling 39
5.1.3 Management 39
5.1.4 Audit 40
5.1.5 Communication concealing (FPR_CON.1) 40
6 Security Requirements 40
6.1 Overview 40
6.2 Class FAU: Security Audit 42
6.2.1 Introduction 42
6.2.2 Security Requirements for the System Log 44
6.2.3 Security Requirements for the Consumer Log 45
6.2.4 Security Requirements for the Calibration Log 47
6.2.5 Security Requirements that apply to all logs 49
6.3 Class FCO: Communication 50
6.3.1 Non-repudiation of origin (FCO_NRO) 50
6.4 Class FCS: Cryptographic support 51
6.4.1 Cryptographic support for TLS 51
6.4.2 Cryptographic support for CMS 52
6.4.3 Cryptographic support for Meter communication encryption 54
6.4.4 General Cryptographic support 57
6.5 Class FDP: User Data Protection 58
6.5.1 Introduction to the Security Functional Policies 58
6.5.2 Gateway Access SFP 59
6.5.3 Firewall SFP 60
6.5.4 Meter SFP 62
6.5.5 General Requirements on user data protection 64
6.6 Class FIA: Identificatiofmn and Authentication 65
6.6.1 User Attribute Definition (FIA_ATD) 65
6.6.2 Authentication Failure handling (FIA_AFL) 65
6.6.3 User Authentication (FIA_UAU) 65
6.6.4 User Identification (FIA_UID) 67
6.6.5 User-subject binding (FIA_USB) 67

6.7 Class FMT: Security Management 68
6.7.1 Management of the TSF 68
6.7.2 Security management roles (FMT_SMR) 71
6.7.3 Management of security attributes for Gateway access SFP 71
6.7.4 Management of security attributes for Firewall SFP 72
6.7.5 Management of security attributes for Meter SFP 73
6.8 Class FPR: Privacy 73
6.8.1 Communication Concealing (FPR_CON) 73
6.8.2 Pseudonymity (FPR_PSE) 74
6.9 Class FPT: Protection of the TSF 75
6.9.1 Fail secure (FPT_FLS) 75
6.9.2 Replay detection (FPT_RPL) 75
6.9.3 Time stamps (FPT_STM) 75
6.9.4 TSF self-test (FPT_TST) 76
6.10 Class FTP: Trusted path/channel 77
6.10.1 Inter-TSF trusted channel (FTP_ITC) 77
6.11 Security Assurance Requirements for the TOE 78
6.12 Security Requirements rationale 79
6.12.1 Security Functional Requirements rationale 79
6.12.2 Security Assurance Requirements rationale 86
7 TOE Summary Specification (TSS) 87
7.1 Cryptographic functionality and TLS handling 87
7.1.1 Cryptographic primitives and certificate generation 87
7.1.2 TLS handling 88
7.2 Identification, authentication and authorization 88
7.3 Self protection and security management 89
7.3.1 Self protection 89
7.3.2 Security management 90
8 Appendix 91
8.1 Glossary Supplement 91
8.2 References Supplement 92
9 Bibliography 92

1 ST INTRODUCTION

1.1 TOE REFERENCE

The TOE is referenced by the be underlying TOE-Reference. Any update of the components given in Chapter 1.2 will increase the TOE's version.

Developer Name:	EFR GmbH
TOE-Reference:	SGH-S v1.01

Table 1: TOE-Reference

1.2 TOE COMPONENTS AND IDENTIFICATION

The TOE is comprised of a hardware board and an application software, other hardware such as the hardwired security module or the communication modem is not part of the TOE.
Version 1.01 of the TOE consists of the following components:

Name:	**Component**	**Identification**
Bootloader	c2e15873	Identification via Component
Root File System	9ac7c6ce03	
Operating System	93ef40da7c8f	
SMGW-App	6.1.1-b955543b4	
Hardware	SGH-S-AL1-B-100 SGH-S-AM1-B-100	Imprint on the SMGW's housing
User Documents	Produkthandbuch SGH-S für den GWA V1.23.pdf	SHA256: 81aa69969092c55af673462aec2a7da489dda5e22b4029e8ef5be222e52310bc
	Servicetechniker Handbuch für Installation und Inbetriebnahme V1.20.pdf	SHA256: c3a564f6274dc54b0e2cfc91a2e363bd50e8d20edd3b4f00d52735ee2827989d
	Handbuch SGH-S für Endnutzer V1.08.pdf	SHA256: 229b6c74729bd19a62318e7e7488bb715ba1547e2aa7faf6949c8c1044142757

Table 1: TOE components

Depending on the type of communication and power supply of the non-TOE relevant part, the nameplate of the TOE relevant case can be one of the following suffixes:

SGH-S-				-		-				Secure Gateway „Smart Grid Hub-Secure"
	A									Wechselspannungsanschluss 230V AC
		L								Mobilfunk CAT1 LTE 800/900/1800/2100/2600 MHz sowie 2G 900/1800 (zusätzlich zur Ethernet-WAN Schnittstelle)
		M								Mobilfunk CAT M1/NB2 LTE 450/700/800/900/1800/2100 MHz (zusätzlich zur Ethernet-WAN Schnittstelle)
			1							Ethernet-Switch HAN-CLS
				-	**B**					Variante mit Sicherheitsmodul, mit CC Zertifizierung und PTB A 50.8 Zulassung
						-	**1**	**0**	**0**	Hardware-Identification [1.00 – 9.99]

Table 2: TOE variants and features

1.3 TOE Overview

1.3.1 Introduction

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

1.3.2 Overview of the Gateway in a Smart Metering System

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

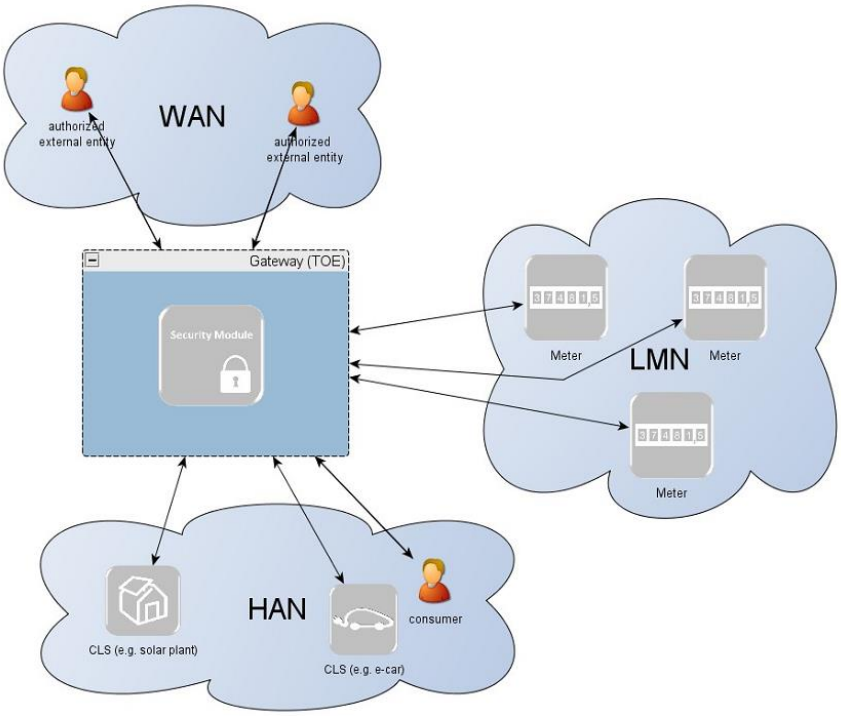


Figure 1: the TOE and its direct environment

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

- The **Gateway** (as defined in this ST) serves as the communication component between the components in the LAN of the consumer (such as meters and added generation plants) and the outside world. The Gateway allows the SMGW-Administrator secure access to the SMGW functionalities. 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 authorized parties have access to them or derivatives thereof. Before sending relevant

information, the information will be signed and encrypted using the services of a Security Module. The Gateway features a mandatory user interface, enabling authorized 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) in defined intervals and submits those records to the Gateway. The Meter Data has to be signed before transfer in order to ensure its authenticity and integrity unless the transmission is physically protected due to the Meter and the Gateway being implemented within one device and utilizing a wired or optical connection. The Meter is comparable to a classical meter and has comparable security requirements; it will be sealed according to the standards of today's classical meters according to the regulations of [PTB-A50.7]. The Meter further supports the encryption of its connection to the Gateway.
- The Gateway utilizes the services of a **Security Module** (e.g., a smart card) as a cryptographic service provider and as a secure storage for confidential assets. The Security Module will be evaluated separately according to the requirements in the corresponding Protection Profile (c.f. [BSI-CC-PP-0077-2015]).

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

The following figure introduces the external interfaces of the TOE and their cardinality.

Please note that the arrows of the interfaces within the Smart Metering System as shown in Figure 2 indicate the flow of information. However, it does not indicate that a communication flow can be initiated bi-directionally. Indeed, the following chapters of this ST will place dedicated requirements on the way an information flow can be initiated.

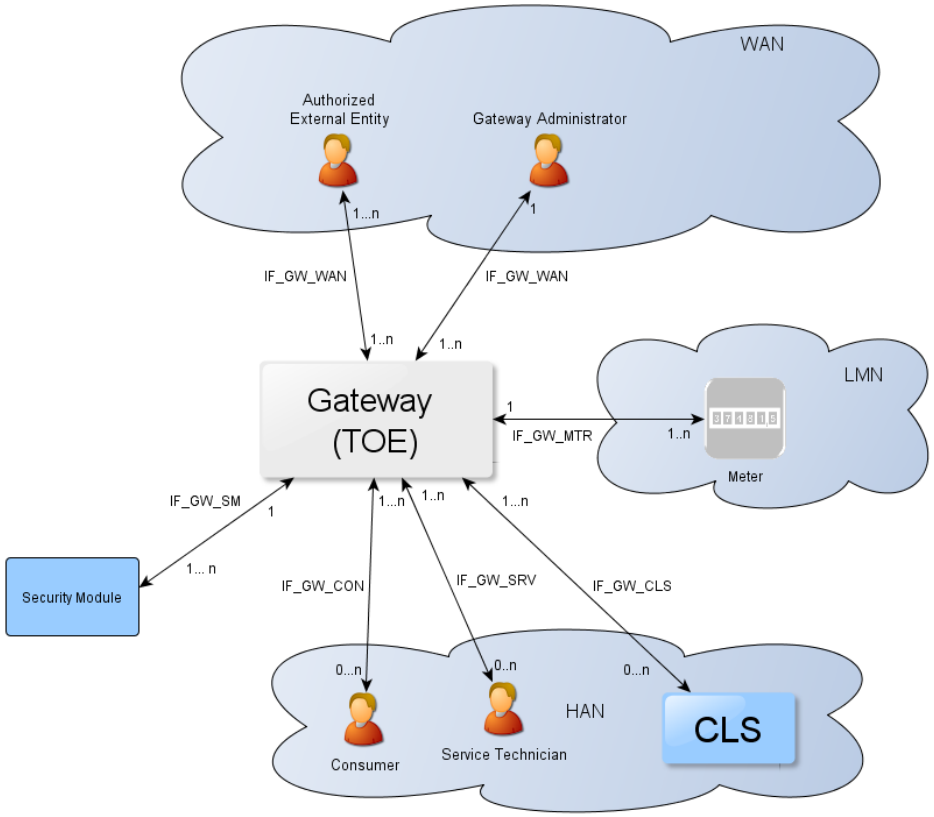


Figure 2: the logical interfaces of the TOE

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.
- 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 CLSs 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 GW Security Module

provides for security critical operations such that the conformance requirements put on the Gateway relate only to a minimum of security functions. The Security Module is evaluated separately.
It should be noted that this Security Target does not aim to imply any concrete system architecture or product design as long as the security requirements from this Security Target are fulfilled. Only in cases where the implementation of the Security Functional Requirements will definitely require certain architecture, this architecture is described in this ST in a mandatory way. It will also be possible to combine the functionalities of Gateway and Meter into one or more modules and devices. To underline this approach this ST will further refer to the term “unit” whenever the TOE or another part of the Smart Metering System is described from a functional perspective and only use the term “component” or “device” when a real physical device is described. The used form of implementing the units of a Smart Metering System in components are described in chapter 1.3.5.2.

1.3.3 TOE DESCRIPTION

The Smart Meter Gateway (in the following short: Gateway or TOE) may serve as the communication unit between devices of private and commercial consumers and service providers of a commodity industry (e.g., electricity, gas, water, etc.). It also collects, processes and stores Meter Data and is responsible for the distribution of this data to external entities.
Typically, the Gateway will be placed in the household or premises of the consumer of the commodity and enables access to local Meter(s) (i.e. the unit(s) used for measuring the consumption or production of electric power, gas, water, heat etc.) and may enable access to Controllable Local Systems (e.g., power generation plants, controllable loads such as air condition and intelligent household appliances). Roles respectively External Entities in the context of the Gateway are introduced in chapter 3.1.
The TOE has a fail-safe design that specifically ensures that any malfunction cannot impact the delivery of a commodity, e.g., energy, gas or water.

1.3.4 TOE TYPE

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

1.3.5 TOE PHYSICAL BOUNDARY

1.3.5.1 Introduction

The TOE comprises the hardware and firmware that is relevant for the security functionality of the Gateway as defined in this ST. The Security Module that is utilized by the TOE is considered being not part of the TOE.

1.3.5.2 TOE design: A Gateway and multiple Meters

The following figure shows the implementation of the Gateway as described in this ST from a physical perspective.
The Gateway is implemented in one device comprising:

- the security relevant parts (i.e. TOE security functionality (TSF)) of the TOE,
- the non-security relevant parts of the Gateway (e.g., the unit for communication), and

- the Security Module that is a target of a separate evaluation but is physically located in the device.

The Gateway communicates with one or more Meters (in the LMN), provides an interface to the WAN and provides interfaces to the HAN.

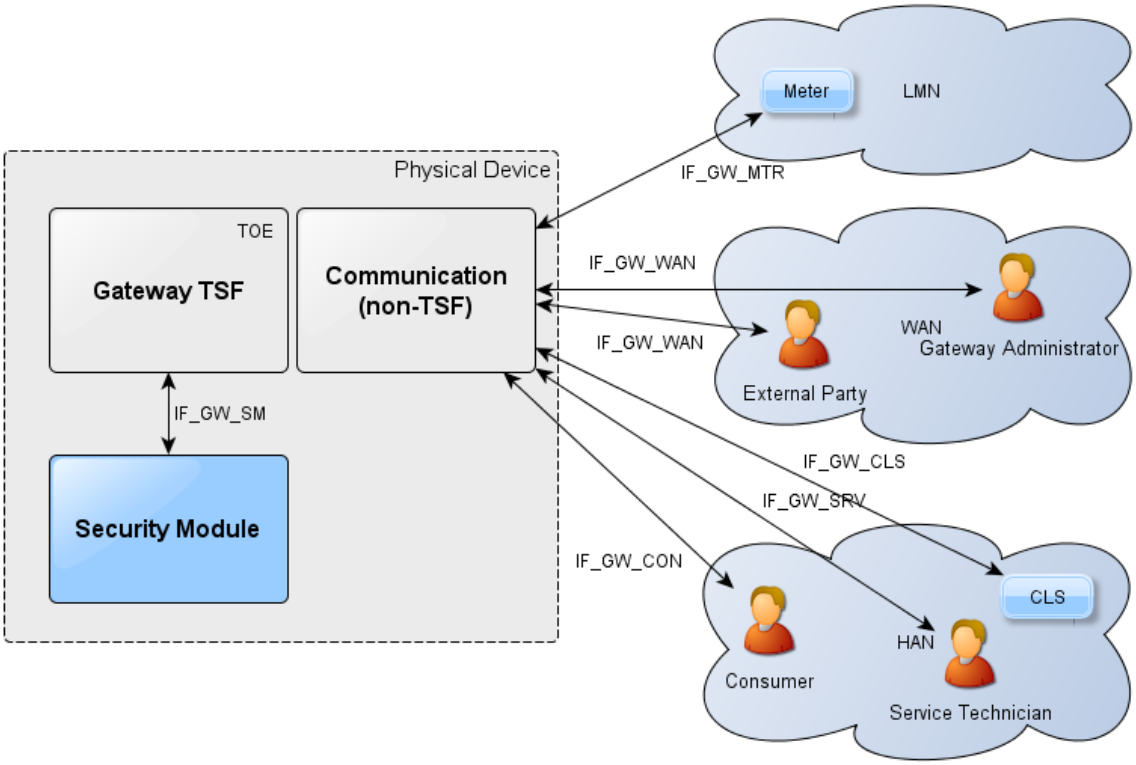


Figure 3: TOE design: A Gateway and multiple meters

Furthermore a 2-port IP switch is integrated in the Gateway to either

a) distribute the WAN interface into two physical Ethernet interfaces IF_GW_WAN-1 and IF_GW_WAN-2
b) distribute the HAN interface into two physical Ethernet interface IF_GW_CLS and IF_GW_CON/IF_GW_SRV

The integrated IP switch only distributes the IP communication of a single physical Ethernet interface into two physical Ethernet interfaces and does no modification on communication stream. Therefore it can be seen as an external transparent communication component which does not influence the secured communication.
For a secure delivery and installation, the following documentations are part of the TOE:

- Servicetechniker Handbuch für Installation und Inbetriebnahme

1.3.5.3 Non-TOE components

The SMGW is composed of TOE relevant and non-relevant components. Non-relevant components are:

- Security Module (separate certificated, [BSI-DSZ-CC-1003-2018])
- Antenna systems
- Communication Module for wMBUS (on Power Supply PCB)
- Communication Module for LTE (on Power Supply PCB)
- Power Supply PCB

1.3.6 TOE LOGICAL BOUNDARY

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

- **Handling of Meter Data**, collection and processing of Meter data, submission to authorized 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 authorized 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.

1.3.6.1 Handling of Meter Data

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 utilizes Processing Profiles to determine which data are sent to which component or external entity A Processing Profile defines:

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

The Processing Profiles are not only the basis for the security features of the TOE; they also contain functional aspects as they indicate to the Gateway how the Meter Data shall be processed. Further Processing Profiles are used to allocate and connect Meter located in the LMN to the SMGW.
More details on the Processing Profiles can be found in [BSI-TR-3109].

The TOE enforces more than one Processing Profile, specifically if the communication and the contractual requirement for multiple external entities have to be handled.

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

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

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

These functionalities will

- prevent that the Gateway accepts data from or sends data to unauthorized 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 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 (e.g., by using SSL/TLS) and ensures that consumers only get access to their own data.

Accessing of this interface by the consumer may happen via different technologies as long as the security requirements are fulfilled. The interface IF_GW_CON may be used by a remote display dedicated to this purpose or may be accessed by standard technologies (e.g., via a PC-based web browser).

1.3.6.2 Confidentiality protection

The TOE protects data from unauthorized 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.

Furthermore, all data, which no longer have to be stored in the TOE, 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 prevents that an unauthorized party is able to disclose any of the data transferred in and from the Smart Metering System (e.g., Meter Data, configuration settings).

1.3.6.3 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 utilizes 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 TOE and have not been changed during transmission. The TOE utilizes 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 authorized external entity and have not been changed during transmission. The TOE utilizes the services of its Security Module for aspects of this functionality.

These functionalities will:

- prevent within the Smart Metering System 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 Meter Data from forged components (with the aim to cause damage to the Smart Grid) will be accepted in the system.

1.3.6.4 Information flow control and firewall

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

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

These functionalities will:

- 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 data are transmitted to the wrong external entity, and that data are transmitted without being confidentiality/authenticity/integrity-protected,
- protect the Smart Metering System and a corresponding large-scale infrastructure in two ways: by preventing that conquered components will send forged Meter Data (with the aim to cause damage to the Smart Grid), and by preventing that widely distributed Smart Metering Systems can be abused as a platform for malicious software to attack other systems in the WAN (e.g., a WAN attacker who would be able to install a botnet on components of the Smart Metering System).

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

Source (1st column) Destination (2nd 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	No connection establishment allowed	(See following list)

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 not connected to any other network,
3. Devices in the **HAN** may communicate with each other. However, the Gateway is not involved in this communication. If devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is assumed to be appropriately protected. It should be noted that for the case that a TOE connects to more than one HAN communications between devices within different HAN via the TOE are only allowed if explicitly configured by a Gateway Administrator.

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

1. The Gateway accepts the submission of Meter Data from the LMN,
2. The Gateway offers a wake-up service at the WAN side as described in chapter 1.3.6.5,
3. The Gateway offers a user interface to the HAN that allows CLS or consumers to connect to the Gateway in order to read relevant information.

1.3.6.5 Wake-up service

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 are only be established by the Gateway itself (e.g., when the Gateway delivers Meter data or contacts the Gateway Administrator to check for updates) or by devices in the HAN.

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 and to offer a so-called wake-up service.

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

1. The Gateway verifies the wake-up packet. This comprises
   a) a check if the header identification is correct
   b) the recipient is the Gateway
   c) the wake-up packet has been sent/received within an acceptable period of time in order to prevent replayed messages
   d) the wake-up message has not been received before

2. If the wake-up message could not be verified as described in step #1 the message will be dropped/ignored. No further operations will be initiated and no feedback is provided.
3. If the message could be verified as described in step #1 the signature of the wake-up message will be verified. The Gateway 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 [BSI-TR-3109].

1.3.6.6 Privacy Preservation

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

This contains two aspects:
The Processing Profiles that the TOE obeys facilitate an approach in which only a minimum amount of data has to be submitted to external entities and therewith leave the scope of control of the consumer. The mechanisms “encryption” and “pseudonymization” 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 authorized 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 allows a consumer access to the data only in the consumer log that is related to their own consumption or production. The following paragraphs provide more details on the information that are included in this log:

Monitoring of Data Transfers
The TOE is able to keep track of each data transmission in the consumer log and allow the consumer to see details on which information have been and will be sent (based on the previous and current settings) to which external entity.

Configuration Reporting
The TOE 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).

1.3.6.7 Management of Security Functions

The Gateway provides authorized Gateway Administrators with functionality to manage the behavior of the security functions and to update the TOE.
The Gateway support the following Management functionalities:

- Pairing of the meter
- Firmware update
- Display the current version number of the TOE
- Display the current time
- Certificates handling for external entities in WAN
- Reset of the TOE when the it stops in critical situations

Further, it is defined that only authorized 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 is only possible from the WAN side interface.

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

1.3.6.8 Identification and Authentication

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

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

1.3.7 THE LOGICAL INTERFACES OF THE TOE

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

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

table 3: Mandatory TOE external interfaces

1.3.8 THE CRYPTOGRAPHY OF THE TOE AND ITS SECURITY MODULE

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

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

Aspect	TOE	Security Module
Communication with external entities	• Encryption • Decryption • Hashing • Key Derivation • MAC generation • MAC verification • Secure storage of the TLS certificates	Key Negotiation: • Support of the authentication of the external entity • Secure storage of the private key • Random Number Generation • Digital signature verification and generation
Communication with the consumer	• Encryption • Decryption • Hashing • Key Derivation •MAC generation •MAC verification • Secure storage of the TLS certificates	Key Negotiation: • Support of the authentication of the consumer • Digital signature verification and generation • Secure storage of the private key • Random Number Generation
Communication with the Meter	• Encryption • Decryption • Hashing • Key Derivation •MAC generation •MAC verification • Secure storage of the TLS certificates	Key Negotiation (in case of TLS connection): • Support of the authentication of the meter • Secure storage of the private key • Digital signature verification and generation • Random Number Generation
Signing data before submission to an external entity	• Hashing	Signature creation: • Secure Storage of the private key
Content data encryption and integrity protection	• Encryption • Decryption • MAC generation • Key Derivation • Secure storage of the Public Key	Key Negotiation: • Secure storage of the private key • Random Number Generation

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

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

1.3.8.1 Content data encryption vs. an encrypted channel

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

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

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

This concept of encryption on two layers facilitates use cases in which the external 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 figures introduce 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 4:

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

    or

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

7. The processed and signed Meter Data may be stored for a certain amount of time.
8. The processed Meter Data is finally submitted to an authorized external entity in the WAN via an encrypted and mutually authenticated channel.

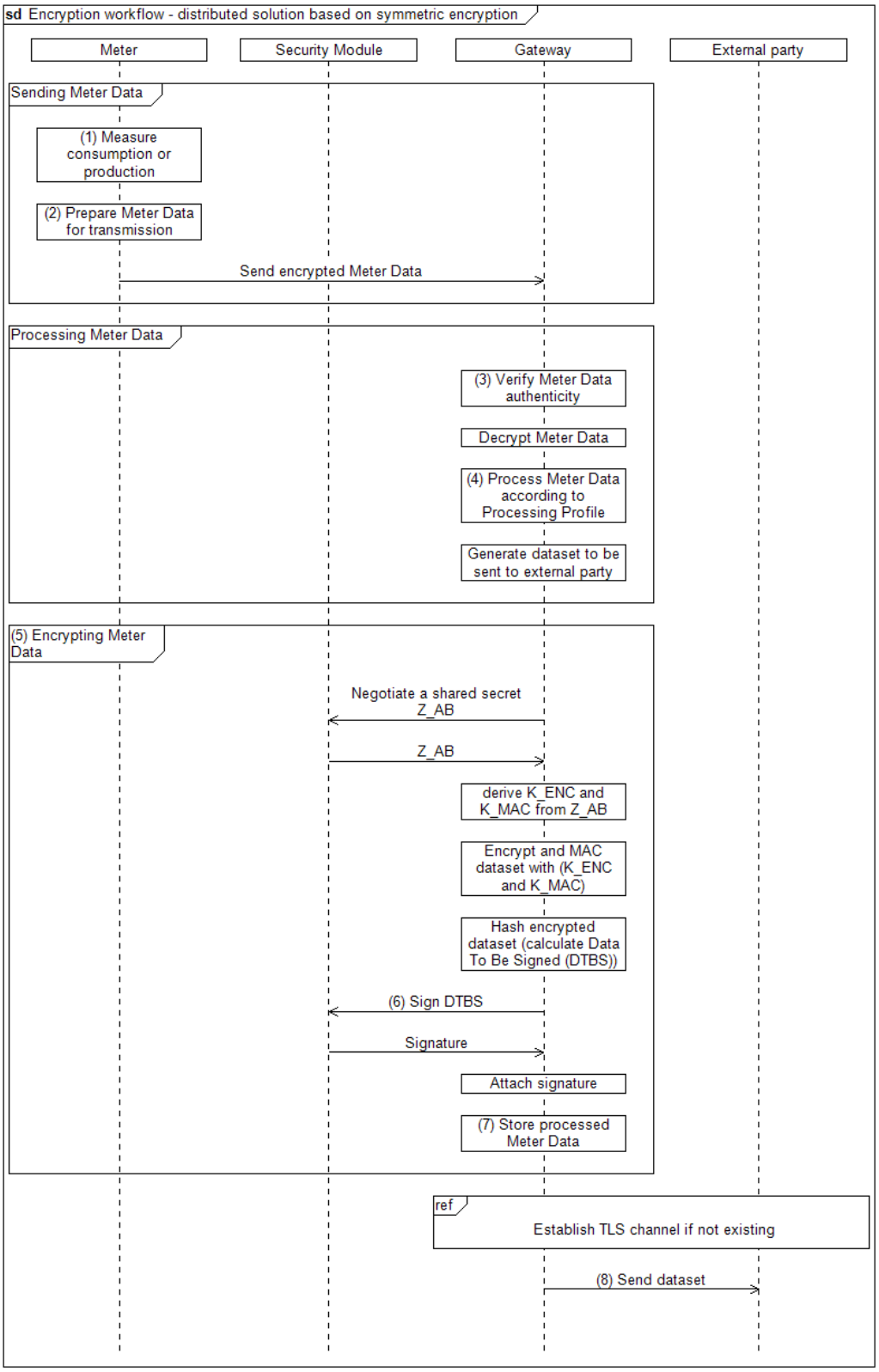


Figure 4: Cryptographic workflow for Meter, Gateway and the Security Module

1.3.9 TOE LIFE-CYCLE

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

1. Development
2. Production
3. Pre-personalization at the developer's (without Security Module)
4. Pre-personalization and integration of Security Module
5. Installation and start of operation
6. Personalization
7. Normal operation

A detailed description of the different phases is provided in [BSI-TR-03109-1-VI].

The process of programming of the TOE's secure operating system and the final application will take place in a secured room according to BSI requirements and will be done only by skilled staff. After the temporary configuration program in the TOE has started, the integration and pre-personalisation 1 and 2 will executed. There exists a VPN channel from secure room to SUB-CA for Key and Certificate exchange. The configuration program in the TOE will terminated for ever in the TOE after usage.
At the end of the personalisation process the TOE and the security module are in the operational mode.

2 CONFORMANCE CLAIM (ASE_CCL)

2.1 CONFORMANCE STATEMENT

This ST claims strict conformance to the PP [BSI-CC-PP-0073-2014] (Smart Meter Gateway).

2.2 ST CONFORMANCE CLAIMS

This ST has been developed using Version 3.1 Revision 4 of Common Criteria [CC]
This ST claims conformance to Common Criteria [CC] part 2 extended due to the use of FPR_CON.1.
This ST claims conformance to Common Criteria [CC] part 3; no extended assurance components have been defined.

2.3 CONFORMANCE CLAIM RATIONALE

The Smart Meter Gateway protection profile is the dedicate fit for this device class and covers all TSF. Therefore no other protection profile has been considered.

2.4 PACKAGE CLAIM

This ST claims an assurance package EAL4 augmented by AVA_VAN.5 and ALC_FLR.2.

3 Security Problem Definition (ASE_SPD)

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 authorized 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 authorized individual that is responsible for diagnostic purposes
Authorized External Entity/ User	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary. In the context of this ST the term user or external entity serve as a hypernym for all entities mentioned before.

table 5: Roles used in the Security Target

3.2 Assets

The following table introduces the relevant assets for this Protection Profile. The table focuses 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.

Asset	Description	Need for Protection
Meter data	Meter readings that allow calculation of the quantity of a commodity, e.g., electricity, gas, water or heat consumed over a period. Meter Data comprise Consumption or Production Data (billing-relevant) and grid status data (not billing-relevant). While billing-relevant data needs to have a relation to the consumer grid status data do not have to be directly related to a consumer.	• According to their specific need (see below)
System log data	Log data from the system log.	• Integrity • Confidentiality (only authorized SMGW administrators and Service Technicians may read the log data)
Consumer log data	Log data from the consumer log.	• Integrity

		• Confidentiality (only authorized Consumers may read the log data)
Calibration log data	Log data from the calibration log.	• Integrity • Confidentiality (only authorized SMGW administrators may read the log data)
Consumption data	Billing-relevant part of Meter Data. Please note that the term Consumption Data implicitly includes Production Data.	• Integrity and authenticity (comparable to the classical meter and its security requirements) • Confidentiality (due to privacy concerns)
Status data	Grid status data, subset of Meter Data that is not billing-relevant.	• Integrity and authenticity (comparable to the classical meter and its security requirements) • Confidentiality (due to privacy concerns)
Supplementary data	The Gateway may be used for communication purposes by devices in the LMN or HAN. It may be that the functionality of the Gateway that is used by such a device is limited to pure (but secure) communication services. Data that is transmitted via the Gateway but that does not belong to one of the aforementioned data types is named Supplementary Data.	• Integrity and authenticity (comparable to the classical meter and its security requirements) • Confidentiality in the WAN (due to privacy concerns)
Data/ user data	The terms Data or User Data are used as a hypernym for Meter Data and Supplementary Data.	• According to their specific need
Gateway time	Date and time of the real-time clock of the Gateway. Gateway Time is used in Meter Data records sent to external entities.	• Integrity • Authenticity (when time is adjusted to an external reference time)
Personally Identifiable Information (PII)	Personally Identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.	• Confidentiality
Meter config (secondary asset)	Configuration data of the Meter to control its behavior including the Meter identity.	• Integrity and authenticity • Confidentiality

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

table 6: Assets (TSF data)

3.3 ASSUMPTIONS

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

A.ExternalPrivacy
It is assumed that authorized 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 unauthorized 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 authorized 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 authorized to provide the update is trustworthy and will not introduce any malware into a firmware update.

A.Network
It is assumed that

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

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

Application Note 1 : This ST acknowledges that the Gateway cannot be completely protected against unauthorized 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 [BSI-TR-03109-1]

Application Note 2 : The Processing Profiles that are used for information flow control as referred to by A.ProcessProfile are an essential factor for the preservation of the privacy of the consumer. The Processing Profiles are used to determine which data shall be sent to which entity at which frequency and how data are processed, e.g., whether the data needs to be related to the consumer (because it is used for billing purposes) or whether the data shall be pseudonymised.
The Processing Profiles shall be visible for the consumer to allow a transparent communication.
It is essential that Processing Profiles correctly define the amount of information that must be sent to an external entity. Exact regulations regarding the Processing Profiles and the Gateway Administrator are beyond the scope of this document.

3.4 THREATS

The following sections identify the threats that are posed against the assets handled by the Smart Meter Gateway. Those threats are the result of a threat model that has been developed for the whole Smart Metering System first and then has been focussed on the threats against the Gateway.

It should be noted that the threats in the following paragraphs consider two different kinds of attackers:

- Attackers having physical access to Meter, Gateway, or a connection between these components or local logical access to any of the interfaces (local attacker), trying to disclose or alter assets while stored in Meter or Gateway or while transmitted between meters in the LMN and the Gateway. Please note that the following threat model assumes that the local attacker has less motivation than the WAN attacker as a successful attack of a local attacker

will always only impact one Gateway. Please further note that the local attacker includes the authorized individuals like consumers.

- An attacker located in the WAN (WAN attacker) trying to compromise the confidentiality and/or integrity of the processed Meter Data and or configuration data transmitted via the WAN, or attacker trying to conquer a component of the infrastructure (i.e. Meter, Gateway or Controllable Local System) via the WAN to cause damage to a component itself or to the corresponding grid (e.g., by sending forged Meter Data to an external entity).

The definition of the following threats acknowledges that the local attacker (facilitating physical access) has less motivation for an attack than a remote attacker.

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

T.DataModificationLocal
A local attacker may try to modify (i.e. alter, delete, insert, replay or redirect) Meter Data when transmitted between Meter and Gateway, Gateway and consumer, or Gateway and external entities. The objective of the attacker may be to alter billing-relevant information or grid status information. The attacker may perform the attack via any interface (LMN, HAN, or WAN).
In order to achieve the modification, the attacker may also try to modify secondary assets like the firmware or configuration parameters of the Gateway.

T.DataModificationWAN
A WAN attacker may try to modify (i.e. alter, delete, insert, replay or redirect) Meter Data, Gateway config data, Meter config data, CLS config data or a firmware update when transmitted between the Gateway and an external entity in the WAN.
When trying to modify Meter Data it is the objective of the WAN attacker to modify billing-relevant information or grid status data.
When trying to modify config data or a firmware update the WAN attacker tries to circumvent security mechanisms of the TOE or tries to get control over the TOE or a device in the LAN that is protected by the TOE.

T.TimeModification
A local attacker or WAN attacker may try to alter the Gateway time. The motivation of the attacker could be e.g., to change the relation between date/time and measured consumption or production values in the Meter Data records (e.g., to influence the balance of the next invoice).

T.DisclosureWAN
A WAN attacker may try to violate the privacy of the consumer by disclosing Meter Data or configuration data (Meter config, Gateway config or CLS config) or parts of it when transmitted between Gateway and external entities in the WAN.

T.DisclosureLocal

A Local Attacker may try to violate the privacy of the consumer by disclosing Meter Data transmitted between the TOE and the Meter. This threat is of specific importance if Meters of more than one consumer are served by one Gateway.

T.Infrastructure
A WAN attacker may try to obtain control over Gateways, Meters or CLS via the TOE, which enables the WAN Attacker to cause damage to consumers or external entities or the grids used for commodity distribution (e.g., by sending wrong data to an external entity).
A WAN attacker may also try to conquer a CLS in the HAN first in order to logically attack the TOE from the HAN side.

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

T.ResidentData
A WAN or local attacker may try to access (i.e. read, alter, delete) information to which they don't have permission to while the information is stored in the TOE. While the WAN attacker only uses the logical interface of the TOE that is provided into the WAN the local attacker may also physically access the TOE.

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

3.5 Organizational Security Policies

This section lists the organizational security policies (OSP) that the Gateway complies 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 requirements according to [SecMod-PP] and shall be used in accordance with its relevant guidance documentation.

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

1. A system log of relevant events in order to allow an authorized Gateway Administrator to analyse the status of the TOE. The TOE shall also analyse the system log automatically for an accumulation of security relevant events.
2. A consumer log that contains information about the information flows that have been initiated to the WAN and information about the Processing Profiles causing this information flow as well as the billing-relevant information.
3. A calibration log (as defined in chapter 6.2) 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 be only allowed for an authorized Gateway Administrator via IF_GW_WAN of the TOE and an authorized Service Technician via IF_GW_SRV.
2. Access to the information in the calibration log shall be only allowed for an authorized Gateway Administrator via the IF_GW_WAN interface of the TOE.
3. Access to the information in the consumer log shall be only allowed for an authorized 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 (ASE_OBJ)

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 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 detects during its self-test whether connections (wired or wireless), if any, are wrongly connected.

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

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

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

- the TOE shall ensure that the communication to the Meter(s) is established in a Gateway Administrator-definable interval or an interval as defined by the Meter,
- the TOE shall enforce encryption and integrity protection for the communication with the meter
- the TOE shall verify the integrity and authenticity of the data received from a Meter before handling it further,
- the TOE shall process the data according to the definition in the corresponding Processing Profile,
- the TOE shall encrypt the processed Meter Data for the final recipient, sign the data and
- deliver the encrypted data to authorized external entities as defined in the corresponding Processing Profiles facilitating an encrypted channel,
- the TOE shall store processed Meter Data if an external entity cannot be reached and re-try to send the data until a configurable number of unsuccessful retries has been reached,
- the TOE shall pseudonymise the data for parties that do not need the relation between the processed Meter Data and the identity of the consumer.

O.Crypt
The TOE shall provide cryptographic functionality as follows:

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

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

The TOE shall not provide a Random Number generator but use the the Random Number Generator of the Security Module instead.

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

O.Protect
The TOE shall implement functionalities to protect its security functions against malfunctions and tampering.
Specifically, the TOE shall

- encrypts its TSF and user data as long as it is not in use
- overwrites any information that is no longer needed to ensure that it is no longer available via the external interfaces of the TOE,
- monitors user data and the TOE firmware for integrity errors,
- contains a test that detects whether the interfaces for WAN and LAN are separate,
- implements self-tests to verify the integrity of the TOE security functions and its data,
- has a fail-safe design that specifically ensures that no malfunction can impact the delivery of a commodity (e.g., energy, gas, heat or water),
- make any physical manipulation within the scope of the intended environment detectable for the consumer and Gateway Administrator.

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

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

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

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

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

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

1. Access to the information in the system log shall only allowed for an authorized Gateway Administrator via IF_GW_WAN or for the TOE and an authorized Service Technician via IF_GW_SRV.
2. Access to the information in the consumer log shall only allowed for an authorized consumer via the IF_GW_CON interface of the TOE and via a secured (i.e. confidentiality and integrity protected) connection. The consumer shall only access to their own information.
3. Read-only access to the information in the calibration log is shall only allowed for an authorized Gateway Administrator via the WAN interface of the TOE.

The system log may overwrite the oldest events in case that the audit trail gets full.
For the consumer log the TOE shall ensure that a sufficient amount of events is available (in order to allow a consumer to verify an invoice) but may overwrite older events in case that the audit trail gets full.
For the calibration log however, the TOE shall ensure the availability of all events over the lifetime of the TOE.

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

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

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

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

OE.Profile
The Processing Profiles that are used when handling data shall be obtained from a trustworthy and reliable source only.

OE.SM
The environment shall provide the services of a certified Security Module for

- Verification of digital signatures,
- Generation of digital signatures,
- Key agreement

- Key transport
- Key storage
- Random Number Generation.

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

OE.Update
The firmware updates for the Gateway that can be provided by an authorized external entity shall undergo a certification process according to this Security Target before they are issued to show that the update is implemented correctly. The external entity that is authorized to provide the update shall be trustworthy and ensure that no malware is introduced via a firmware update.

OE.Network
It shall be ensured that

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

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

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 OVERVIEW

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

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access	OE.SM	OE.ExternalPrivacy	OE.TrustedAdmins	OE.PhysicalProtection	OE.Profile	OE.Update	OE.Network	OE.Keygen
T.DataModificationLocal				X	X		X	X					X	X				
T.DataModificationWAN	X				X		X	X					X					
T.TimeModification					X	X	X	X					X	X				
T.DisclosureWAN	X		X		X		X	X					X					
T.DisclosureLocal				X	X		X	X					X	X				
T.Infrastructure	X	X		X	X		X	X					X					
T.ResidualData							X	X					X					
T.ResidentData	X				X		X	X		X			X	X				
T.Privacy	X		X	X	X		X	X					X		X			
OSP.SM					X		X	X			X		X					
OSP.Log							X	X	X	X			X					
A.ExternalPrivacy												X						
A.TrustedAdmins													X					
A.PhysicalProtection														X				
A.ProcessProfile															X			
A.Update																X		
A.Network																	X	
A.Keygen																		X

7: Rationale for Security Objectives

4.3.2 COUNTERING THE THREATS

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

4.3.2.1 General objectives

The security objectives O.Protect, O.Management and OE.TrustedAdmins contribute to counter each threat and contribute to each OSP.
O.Management is indispensable as it defines the requirements around the management of the Security Functions. Without a secure management no TOE can be secure. Also **OE.TrustedAdmins** contributes to this aspect as it provides the requirements on the availability of a trustworthy Gateway Administrator and Service Technician. **O.Protect** is present to ensure that all security functions are working as specified.
Those general objectives will not be addressed in detail in the following paragraphs.

4.3.2.2 T.DataModificationLocal

The threat **T.DataModificationLocal** is countered by a combination of the security objectives **O.Meter**, **O.Crypt** and **OE**.**PhysicalProtection**.
O.Meter defines that the TOE will enforce the encryption of communication when receiving Meter Data from the Meter. O.Crypt defines the required cryptographic functionality. The objectives together ensure that the communication between the Meter and the TOE cannot be modified or released.
OE.PhysicalProtection is of relevance as it ensures that access to the TOE is limited.

4.3.2.3 T.DataModificationWAN

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

4.3.2.4 T.TimeModification

The threat **T.TimeModification** is countered by a combination of the security objectives **O.Time, O.Crypt** and **OE.PhysicalProtection**.
O.Time defines that the TOE needs a reliable time stamp mechanism that is also updated from reliable sources regularly in the WAN. O.Crypt defines the required cryptographic functionality for the communication to external entities in the WAN. Therewith, **O.Time** and **O.Crypt** are the core objective to counter the threat **T.TimeModification**.
OE.PhysicalProtection is of relevance as it ensures that access to the TOE is limited.

4.3.2.5 T.DisclosureWAN

The threat **T.DisclosureWAN** is countered by a combination of the security objectives **O.Firewall, O.Conceal** and **O.Crypt**.
O.Firewall defines the connections for the devices within the LAN to external entities within the WAN and shall provide firewall functionality in order to protect the devices of the LMN and HAN (as long as they use the Gateway) and itself against threats from the WAN side. **O.Crypt** defines the required cryptographic functionality. Both objectives together ensure that the communication between the Meter and the TOE cannot be disclosed.
O.Conceal ensures that no information can be disclosed based on additional characteristics of the communication like frequency, load or the absence of a communication.

4.3.2.6 T.DisclosureLocal

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

O.Meter defines that the TOE will enforce the encryption and integrity protection of communication when polling or receiving Meter Data from the Meter. **O.Crypt** defines the required cryptographic functionality. Both objectives together ensure that the communication between the Meter and the TOE cannot be disclosed.

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

4.3.2.7 T.Infrastructure

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

O.Firewall is the core objective that counters this threat. It ensures that all communication flows to the WAN are initiated by the TOE. The fact that the TOE does not offer any services to the WAN side and will not react to any requests (except the wakeup 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 deletes 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 is primarily addressed by the security objectives **O.Meter**, **O.Crypt** and **O.Firewall** as these objective ensures that the TOE will only distribute Meter Data to external entities in the WAN as defined in the corresponding Processing Profiles and that the data will be protected for the transfer. **OE.Profile** is present to ensure that the Processing Profiles are obtained from a

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

4.3.3 COVERAGE OF ORGANIZATIONAL 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 utilizes 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 utilizes for as defined in **OSP.SM** and also requires a certified Security Module. **O.Crypt** defines the cryptographic functionalities for the TOE itself. In this context it has to be ensured that the Security Module is operated in accordance with its guidance documentation.

4.3.3.2 OSP.Log

The Organizational Security Policy **OSP.Log** that mandates that the TOE maintains an audit log is directly addressed by the security objective for the TOE **O.Log**.
O.Access contributes to the implementation of the OSP as it defines that also Gateway Administrators are not allowed to read/modify all data. This is of specific importance to ensure the confidentiality and integrity of the log data as is required by the **OSP.Log**.

4.3.4 COVERAGE OF ASSUMPTIONS

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

4.3.4.1 A.ExternalPrivacy

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

4.3.4.2 A.TrustedAdmins

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

4.3.4.3 A.PhysicalProtection

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

4.3.4.4 A.ProcessProfile

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

4.3.4.5 A.Update

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

4.3.4.6 A.Network

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

4.3.4.7 A.Keygen

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

4.4 SECURITY OBJECTIVES CONCLUSION

Based on the security objectives and the security objectives rationale, the following conclusion can be drawn:
If all security objectives are achieved then the security problem as defined in Security problem definition (ASE_SPD) is solved. All threats are countered, all OSPs are enforced, and all assumptions are upheld.

5 EXTENDED COMPONENTS DEFINITION

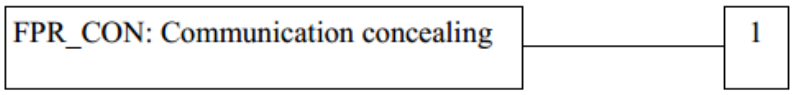
5.1 COMMUNICATION CONCEALING (FPR_CON)

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.

5.1.1 FAMILY BEHAVIOR

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.

5.1.2 COMPONENT LEVELLING



5.1.3 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.
b. Default interval is daily.

5.1.4 AUDIT

There are no auditable events foreseen.

5.1.5 COMMUNICATION CONCEALING (FPR_CON.1)

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

FPR_CON.1.1 The TSF shall enforce the [assignment: *information flow policy]* in order to ensure that no Personally Identifiable Information (PII) can be obtained by an analysis of [assignment: *characteristics of the information flow that need to be concealed*].

FPR_CON.1.2 The TSF shall connect to [assignment*: list of external entities*] in intervals as follows [selection: *weekly, daily or hourly*, *[assignment: other intervals]*] to conceal the data flow.

6 SECURITY REQUIREMENTS

6.1 OVERVIEW

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

- **Refinement** operation (denoted by **bold text**): is used to add details to a requirement, and thus further restricts a requirement. In case that a word has been deleted from the original text this refinement is indicated by **~~crossed-out bold~~** text.
- **Selection** operation (denoted by underlined text): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized 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 summarizes 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 behavior
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 initialization for Gateway access policy
FMT_MSA.1/FW	Management of security attributes for firewall policy
FMT_MSA.3/FW	Static attribute initialization for Firewall policy
FMT_MSA.1/MTR	Management of security attributes for Meter policy
FMT_MSA.3/MTR	Static attribute initialization for Meter policy
Class FPR: Privacy	
FPR_CON.1	Communication Concealing
FPR_PSE.1	Pseudonymity
Class FPT: Protection of the TSF	
FPT_FLS.1	Failure with preservation of secure state

FPT_RPL.1	Replay Detection
FPT_STM.1	Reliable time stamps
FPT_TST.1	TSF testing
FPT_PHP.1	Passive detection of physical attack
Class FTP: Trusted path/channels	
FTP_ITC.1/WAN	Inter-TSF trusted channel for WAN
FTP_ITC.1/MTR	Inter-TSF trusted channel for Meter
FTP_ITC.1/USR	Inter-TSF trusted channel for User

table 8: List of Security Functional Requirements

6.2 CLASS FAU: SECURITY AUDIT

6.2.1 INTRODUCTION

The TOE implements three different audit logs as defined in OSP.Log and O.Log. The following table provides an overview over the three audit logs before the following chapters introduce the SFRs related to those audit logs.

	System-Log	Consumer-Log	Calibration-Log
Purpose	• Inform the Gateway Administrator about security relevant events • Log all events as defined by Common Criteria for the used SFR • Log all system relevant events on specific functionality • Automated alarms in case of a cumulation of certain events • Inform the service technician about the status of the Gateway	• Inform the consumer about all information flows to the WAN • Inform the consumer about the Processing Profiles • Inform the consumer about other metering data (not billing-relevant) • Inform the consumer about all billing-relevant data needed to verify an invoice	• Track changes that are relevant for the calibration of the TOE
Data	• As defined in FAU_GEN.1.1/SYS • Augmented by specific events for the security functions	• Information about all information flows to the WAN • Information about the current and the previous Processing Profiles • Non-billing-relevant Meter Data	• Calibration relevant data only

		• Information about the system status (including relevant errors) • Billing relevant data needed to verify an invoice	
Access	• Access by authorized Gateway Administrator and via IF_GW_WAN only • Events may only be deleted by an authorized Gateway Administrator via IF_GW_WAN • Read access by authorized service technician via IF_GW_SRV only	• Read access by authorized consumer and via IF_GW_CON only to the data related to the current consumer	• Read access by authorized Gateway Administrator and via IF_GW_WAN only
Deletion	• Ring buffer. • The availability of data has to be ensured for a sufficient amount of time • Overwriting old events is possible if the memory is full	• Ring buffer. • The availability of data has to be ensured for a sufficient amount of time • Overwriting old events is possible if the memory is full • Retention period is set by authorized Gateway Administrator on request by consumer, data older than this are deleted.	• The availability of data has to be ensured over the lifetime of the TOE.

table 9: overview over audit processes

Application Note 4 : It shall be noted that no mechanic is implemented which allows an authorized Gateway Administrator the deletion of System Log data. The retention period for Consumer Log data is fixed and cannot be changed by an authorized Gateway Administrator. A consumer cannot issue a delete request on consumer data.

6.2.2 SECURITY REQUIREMENTS FOR THE SYSTEM LOG

6.2.2.1 Security audit automatic response (FAU_ARP)

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

FAU_ARP.1/SYS
The TSF shall ~~take~~ *inform an authorized Gateway Administrator and create a log entry within the System Log* upon detection of a potential security violation.

Hierarchical to: No other components
Dependencies: FAU_SAA.1 Potential violation analysis

6.2.2.2 Security audit data generation (FAU_GEN)

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

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

a. Start-up and shutdown of the audit functions;
b. All auditable events for the basic level of audit; and
c. *none*

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

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *none*.

Hierarchical to: No other components
Dependencies: FPT_STM.1

6.2.2.3 Security audit analysis (FAU_SAA)

6.2.2.3.1 FAU_SAA.1/SYS: Potential violation analysis for system log

FAU_SAA.1.1/SYS
The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

Application note 5 : All failures in FPT_FLS.1 are potential violations.

FAU_SAA.1.2/SYS
The TSF shall enforce the following rules for monitoring audited events:

a. Accumulation or combination of
    - *Repeated detection of undervoltage level,*

- *cryptographic errors*
- *invalid or duplicate wake-up packets*

known to indicate a potential security violation;

b. *none*

Hierarchical to: No other components
Dependencies: FAU_GEN.1

Application Note 6 : The specific events that are analyzed in the system audit log in order to ensure a correct operation of the TOE highly depend on specific implementation and application of the TOE; as such the authors of the ST has completed the operations in FAU_SAA.1/SYS. At least all types of failures in the TSF as listed in FPT_FLS.1 are recognized as potential violation by the TOE.

6.2.2.4 Security audit review (FAU_SAR)

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

FAU_SAR.1.1/SYS
The TSF shall provide *only authorized Gateway Administrators via the IF_GW_WAN interface and authorized Service Technicians via the IF_GW_SRV interface* with the capability to read *all information* from the **system** audit records.

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

Hierarchical to: No other components
Dependencies: FAU_GEN.1

6.2.2.5 Security audit event storage (FAU_STG)

6.2.2.5.1 FAU_STG.4/SYS: Prevention of audit data loss for the system log

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

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

Application Note 7 : The size of the audit trail that is available before the oldest events get overwritten is ~~configurable for the Gateway Administrator~~ set to 100.000 entries.

6.2.3 SECURITY REQUIREMENTS FOR THE CONSUMER LOG

6.2.3.1 Security audit data generation (FAU_GEN)

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

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

a. Start-up and shutdown of the audit functions;
b. All auditable events for the not specified level of audit; and
c. *All audit events as listed in **Table 10** and none*

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

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the ST*, additional information as listed in **Table 10** and none*.

Hierarchical to: No other components
Dependencies: FPT_STM.1

Application Note 8 : The possibility for the ST author to specify additional events in FAU_GEN.1.1/CON has been specifically introduced to allow that a more detailed set of information about the consumption or production of a certain commodity is audited (e.g., to allow a consumer to control the consumption or production on a granular level). Such information is primarily be captured in the consumer log as this log has the appropriate permissions associated to ensure that only the consumer can review the events.

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 10 Events of the Consumer log

6.2.3.2 Security audit review (FAU_SAR)

6.2.3.2.1 FAU_SAR.1/CON Audit Review for consumer log

FAU_SAR.1.1/CON
The TSF shall provide *only authorized consumer via the IF_GW_CON interface* with the capability to read *all information that are related to them* from the **consumer** audit records.

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

Hierarchical to: No other components
Dependencies: FAU_GEN.1

Application Note 9 : FAU_SAR.1.2/CON ensures that the consumer is able to interpret the information that is provided to him in a way that allows him to verify the invoice.

6.2.3.3 Security audit event storage (FAU_STG)

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

FAU_STG.4.1/CON
The TSF shall overwrite the oldest stored audit records and *inform the Gateway Administrator* if the **consumer** audit trail is full.

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

Application Note 10 : ~~The size of the audit trail that is available before the oldest events get overwritten is configurable for the Gateway Administrator.~~ The audit trail stores values for at least 15 months before deletion.

6.2.4 SECURITY REQUIREMENTS FOR THE CALIBRATION LOG

6.2.4.1 Security audit data generation (FAU_GEN)

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

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

a. Start-up and shutdown of the audit functions;
b. All auditable events for the not specified level of audit; and
c. All calibration-relevant information: see. Table 11

Event	Additional Information
Start of operation of the SMGW	Start of operation as well as the responsible calibration authority
Start of a self test	-
Adding and removal of a Meter	-
Adding and removal of a processing profile	-
A change of a processing profile	Parameters of a processing profile for which a change leads to an entry: • Device IDs of the Meters used for this processing

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

Table 11 Relevant information for calibration log according to [PTB-A50.8]

FAU_GEN.1.2/CAL

The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP~~/ST, *date of start of operation, installation and registration of a new meter, removal of a meter, change of configuration, software and firmware update, and error messages of connected meters, self test initiation, self test detected errors and unique error status code*.

Hierarchical to: No other components
Dependencies: FPT_STM.1

Application Note 11 : The calibration log serves to fulfil national requirements in the context of the calibration of the TOE. The concrete implementation of those requirements depends on the concrete implementation of the TOE.
Therefore the assignments in FAU_GEN.1.1/CAL and FAU_GEN.1.2/CAL base on the standard [PTB-A50-8]

6.2.4.2 Security audit review (FAU_SAR)

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

FAU_SAR.1.1/CAL
The TSF shall provide *only authorized Gateway Administrators via the IF_GW_WAN interface* with the capability to read *all information* from the **calibration** audit records.

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

Hierarchical to: No other components
Dependencies: FAU_GEN.1

6.2.4.3 Security audit event storage (FAU_STG)

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

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

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

Application Note 12 : As outlined in the introduction it has to be ensured that the events of the Calibration Log are available over the lifetime of the TOE.

6.2.5 SECURITY REQUIREMENTS THAT APPLY TO ALL LOGS

6.2.5.1 Security audit data generation (FAU_GEN)

6.2.5.1.1 FAU_GEN.2: User identity association

FAU_GEN.2.1
For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Hierarchical to: No other components
Dependencies: FAU_GEN.1
FIA_UID.1

Application Note 13 : Please note that FAU_GEN.2 applies to all audit logs, the system log, the calibration log, and the consumer log.

6.2.5.2 Security audit event storage (FAU_STG)

6.2.5.2.1 FAU_STG.2: Guarantees of audit data availability

FAU_STG.2.1
The TSF shall protect the stored audit records in ~~**the**~~ **all** audit trail**s** from unauthorized deletion.

FAU_STG.2.2
The TSF shall be able to prevent unauthorized modifications to the stored audit records in ~~**the**~~ **all** audit trail**s**.

FAU_STG.2.3
The TSF shall ensure that

- *all records from the calibration log,*
- *all records of a fixed period of 15 months from the consumer log,*
- *and the 100 000 latest records from the system log*

will be maintained when the following conditions occur: audit storage exhaustion or failure.

Hierarchical to: FAU_STG.1 Protected audit trail storage
Dependencies: FAU_GEN.1 Audit data generation

Application Note 14 : Please note that FAU_STG.2 applies to all audit logs, the system log, the calibration log, and the consumer log.

Application Note 15 : The ST author has considered the regulations from the national calibration authority [TR-03109-1] in order to decide about the amount of information that needs to be available for the requirement in FAU_STG.2.3 for each Audit log.

6.3 CLASS FCO: COMMUNICATION

6.3.1 NON-REPUDIATION OF ORIGIN (FCO_NRO)

6.3.1.1 FCO_NRO.2: Enforced proof of origin

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

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

FCO_NRO.2.3

The TSF shall provide a capability to verify the evidence of origin of information to recipient and *consumer* given *limitations of the digital signature according to [BSI-TR-03109-1]*

FCO_NRO.2

Hierarchical to: FCO_NRO.1 Selective proof of origin

Dependencies: FIA_UID.1 Timing of identification

Application Note 16 : FCO_NRO.2 requires that the TOE calculates a signature over Meter Data that is submitted to external entities. Therefore the TOE creates 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.

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

and specified cryptographic key sizes of
128 bit, or
256 bit

Cryptographic operation	Cryptographic algorithm	Standard
Key generation	*TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 or TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*	*[RFC-5289] [RFC-5246](AES)*

Table 12 Cryptographic standards for Key generation / agreement in TLS

Hierarchical to: No other components.

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

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

Application Note 18 : The TOE only uses cryptographic specifications and algorithms as described in [BSI-TR-03116-3].

Application Note 19 : Based on [BSI-TR-03109-3] the ST author has exactly referenced the applied cryptographic key generation algorithm for TLS.

6.4.1.2 Cryptographic operations (FCS_COP)

6.4.1.2.1 FCS_COP.1/TLS: Cryptographic operations for TLS

FCS_COP.1.1/TLS
The TSF shall perform *TLS encryption, decryption, and integrity protection* in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES) in GCM or CBC-HMAC-mode* and cryptographic key sizes *of 128 or 256 bit* that meet the following:

Cryptographic operation	Cryptographic algorithm	Standard
Symmetric encryption, integrity protection	*TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 or TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*	*[RFC-5289] [RFC-5246], [FIPS-197](AES) [NIST-SP800-38D](AES-GCM) [NIST-SP800-38A](AES_CBC) [RFC-2104](HMAC)*

Table 13 Cryptographic standards for Encryption algorithms using TLS

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1/TLS Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Application Note 20 : The TOE *only* uses cryptographic specifications and algorithms as described in [BSI-TR-03109-3].

Application Note 21 : Based on [BSI-TR-03109-3] the ST author has exactly referenced the applied cryptographic algorithm.

6.4.2 CRYPTOGRAPHIC SUPPORT FOR CMS

6.4.2.1 Cryptographic key management (FCS_CKM)

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

FCS_CKM.1.1/CMS
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [
ElGamal Key Agreement (ECKA-EG):
ecka-eg X963KDF-SHA256
ecka-eg X963KDF-SHA384
ecka-eg X963KDF-SHA512
combined with a specified key encryption algorithm:
id-aes128-wrap

id-aes192-wrap
id-aes256-wrap
and specified cryptographic key sizes [of:
128 bit
192 bit
256 bit
]
that meet the following:

Cryptographic operations	Cryptographic algorithms	Standard
ECKA-EG key agreement and key derivation	ecka-eg X963KDF-SHAxxx	[BSI-TR-03111], §4.1.3, [BSI-TR-03111], $4.3.3 by usage of the security modules services
AES key wrap/unwrap	id-aesxxx-wrap	[RFC-3394]
Key generation	Generation of symmetric AES keys	TRNG Class 3 / Security module not part of the TOE

Table 14 Cryptographic standards for Key generation / Key agreement in CMS

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

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

Application Note 23 : Based on [BSI-TR-03109-3] and [BSI-TR-03109-1-I] the ST author has exactly referenced the applied cryptographic key generation algorithm for CMS.

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

6.4.2.2 Cryptographic operation (FCS_COP)

6.4.2.2.1 FCS_COP.1/CMS: Cryptographic operation for CMS

FCS_COP.1.1/CMS
The TSF shall perform *symmetric encryption, decryption, and integrity protection* in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES)* in *CBC-CMAC- or GCM mode* and cryptographic key sizes *of 128, 192 and 256 bit* that meet the following:

Cryptographic operations	Cryptographic algorithm	Key size [bits]	Standard

encryption + Integrity protection	AES_GCM	128, 192 and 256	[FIPS-197], [NIST-SP800-38D], [RFC-5084]
decryption + Integrity protection	Choice of: AES_GCM, AES_CBC_CMAC	128, 192 and 256	[FIPS-197], [NIST-SP800-38D], [RFC-5652]

Table 15 Cryptographic standards for FCS_COP.1/CMS

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1/CMS Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Application Note 25 : The TOE shall only use cryptographic specifications and algorithms as described in [BSI-TR-03109-3].

Application Note 26 : As the TOE can chose an AES operation mode for symmetrical encryption, AES-GCM shall be used as default mode.

Application Note 27 : Based on [BSI-TR-03109-3] and [BSI-TR-03109-1-I] the ST author does exactly reference the applied cryptographic algorithm for CMS.

6.4.3 CRYPTOGRAPHIC SUPPORT FOR METER COMMUNICATION ENCRYPTION

6.4.3.1 Cryptographic key management (FCS_CKM)

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

FCS_CKM.1.1/MTR
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm

- *Key*-generation *of the shared secret via TRNG of the security module,*
- *Key derivation of MK' for symmetrical encryption/decryption and integrity protection via AES-CMAC,*
- *Key-generation for the TLS session according to* ***FCS_CKM.1.1/TLS***

And specified cryptographic key sizes

- *MK `and keys for symmetrical encryption/decryption: 128 bit*
- *TLS: According to* ***FCS_CKM.1.1/TLS***

that meet the following:

Cryptographic operations	Cryptographic algorithm	Key size [bits]	Standard
Key generation for MK`	TRNG Class 3 / Security module not part of the TOE	128	-

Symmetrical encryption /decryption and integrity protection	AES-CMAC	128	[BSI-TR 03116-3] §7.2 [RFC-4493]

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

Application Note 28 : Based on [BSI-TR-03109-3] the ST author does exactly reference the applied cryptographic key generation algorithm for Meter communication encryption.

Application Note 29 : The TOE does use cryptographic specifications and algorithms as described in [BSI-TR-03109-3].

Application Note 30 : Applies for bidirectional meters only:
The TOE uses the MK key of 128 bit length for the initial pairing between a meter and the TOE. This initial key is brought into the TOE via a management function (see FMT_SMF.1) to create a symmetrical encrypted session. The ONLY purpose of this session is the transmission of the meter`s TLS private key and certificate as well as the TLS certificate of the TOE.
After this information is exchanged, the TOE and a meter create a TLS encrypted session for all further communication. The TOE will now generate a secret which will be shared between TOE and meter for generation of a new key MK` using AES-CMAC and the method described in [BSI-TR-03116-3] §7.1.1.

Application Note 31 : Applies for bidirectional meters only:
Even though TLS is used as the standard communication between the TOE and meters, symmetrical encryption is required to allow management operations issued by the GWA when establishing a TLS session.

Application Note 32 : Applies for unidirectional meters only:
For derivation of the symmetrical decryption key and the key for integrity protection, AES-CMAC and the methods described in [BSI-TR-03116-3] §7.2 are applied.

6.4.3.2 Cryptographic operations (FCS_COP)

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

FCS_COP.1.1/MTR
The TSF shall perform *symmetric encryption, decryption, and integrity protection* in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES)* in *CBC-CMAC-mode* and cryptographic key sizes *of 128 bit* that meet the following:

Cryptographic operations	Cryptographic algorithm	Key size [bits]	Standard
encryption, decryption	AES_CBC	128	[FIPS-197], [ISO/IEC-18033-2:2006]
Integrity protection	AES-CMAC	128	[FIPS-197], [RFC-4493]

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1/MTR Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Application Note 33 : The three different scenarios of key generation for Meter communication encryption are**:**

1. If a TLS encryption is being used the key generation/negotiation is as defined by **FCS_CKM.1/TLS**.
   This is the common communication use case.
2. If AES encryption is being used,
   a. a secret is generated by the Gateway periodically according to [BSI-TR-03109-3] as defined by FCS_CKM.1/MTR and sent to the Meter via encrypted TLS-channel for key generation as defined by FCS_COP.1/TLS. *This use case allows execution of methods between meter and TOE without usage of a TLS encrypted channel.*
   b. a key has been brought into the Gateway via a management function ~~during~~ *before starting* the initial pairing process for the Meter (see FMT_SMF.1) and defined by FCS_COP.1/MTR. *This is the default use case for unidirectional meters.*
   For bidirectional meters it is used only once for initial pairing between TOE and meter.

All three scenarios are supported by the TOE as requested in **Ref_15.4.**

Application Note 34 : If the connection between the Meter and TOE is unidirectional, the communication between the Meter and the TOE is secured via AES encryption.
If a bidirectional connection between the Meter and the TOE is established, the communication is, depending on the communication scenario, secured by a TLS channel as described in chapter 6.4.1 or secured via symmetric AES encryption. As the TOE is interoperable with all kind of Meters it requires the implementation of both kinds of encryption.

Application Note 35 : Based on [BSI-TR-03109-3] the ST author has exactly referenced the applied cryptographic algorithm.

Application Note 36 : The TOE *only* uses cryptographic specifications and algorithms as described in [BSI-TR-03109-3].

6.4.4 General Cryptographic support

6.4.4.1 Cryptographic key management (FCS_CKM)

6.4.4.1.1 FCS_CKM.4: Cryptographic key destruction

FCS_CKM.4.1
The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *key overwriting and NV memory zeroization* that meets the following:
None

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1/TLS Cryptographic key generation, or
FCS_CKM.1/MTR Cryptographic key generation, or
FCS_CKM.1/CMS Cryptographic key generation]

Application Note 37 : Please note that as against the requirement FDP_RIP.2 the mechanisms implementing the requirement from FCS_CKM.4 is suitable to avoid attackers with physical access to the TOE from accessing the keys after they are no longer used.

6.4.4.2 Cryptographic operations (FCS_COP)

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

FCS_COP.1.1/HASH
The TSF shall perform *hashing for signature creation and verification* **and integrity checks and key derivation** in accordance with a specified cryptographic algorithm *Secure Hash Algorithm 2 (SHA-2)* and cryptographic key size [*none*] that meet the following:

Cryptographic operations	Cryptographic algorithm	Standard
Strong Hash	SHA-256, SHA-384, SHA-512	[FIPS-180-4]

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Application Note 38 : The TOE is only responsible for hashing of data in the context of digital signatures. The actual signature operation and the handling (i.e. protection) of the cryptographic keys in this context is performed by the Security Module.

Application Note 39 : The TOE *only* uses cryptographic specifications and algorithms as described in [BSI-TR-03109-3].

Application Note 40 : Based on [BSI-TR-03109-3] the ST author has exactly referenced the applied cryptographic algorithm.

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

FCS_COP.1.1/MEM
The TSF shall perform *TSF and user data encryption* in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES)* and cryptographic key sizes *256 bit each* that meet the following:

Cryptographic operations	Cryptographic algorithm	Key size [bits]	Standard
encryption, decryption	AES_256_XTS	2 keys each 256	[IEEE-1619]

Hierarchical to: No other components.
Dependencies: [~~FDP_ITC.1 Import of user data without security attributes, or~~
FDP_ITC.2 Import of user data with security attributes~~, or~~
~~FCS_CKM.1/CMS Cryptographic key generation~~]
FCS_CKM.4 Cryptographic key destruction

Application Note 41 : Please note that for the key generation process an external security module is used during TOE production.

Application Note 42 : The TOE encrypts its local TSF and user data while it is not in use (i.e.while stored in a persistent memory).
It shall be noted that this kind of encryption cannot provide an absolute protection against physical manipulation and does not aim to. It however contributes to the security concept that considers the protection that is provided by the environment.

Application Note 43 : [BSI-TR-02102] is considered when a cryptographic algorithm is chosen.

6.5 Class FDP: User Data Protection

6.5.1 Introduction to the Security Functional Policies

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

- The Gateway access SFP is an access control policy to control the access to objects under the control of the TOE. The details of this access control policy highly depend on the concrete

application of the TOE. The access control policy is described in more detail in [BSI-TR-03109-1].

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

6.5.2 GATEWAY ACCESS SFP

6.5.2.1 Access control policy (FDP_ACC)

6.5.2.1.1 FDP_ACC.2: Complete access control

FDP_ACC.2.1
The TSF shall enforce the *Gateway access SFP* on
subjects: external entities in WAN, HAN and LMN
objects: any information that is sent to, from or via the TOE and any information that is stored in the TOE and all operations among subjects and objects covered by the SFP.

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

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

6.5.2.1.2 FDP_ACF.1: Security attribute based access control

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

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

- *an authorized Consumer is only allowed to have read access to his own User Data via the interface IF_GW_CON,*
- *an authorized Service Technician is only allowed to have read access to the system log via the interface IF_GW_SRV, the service technician must not be allowed to read, modify or delete any other TSF data,*
- *an authorized Gateway Administrator is allowed to interact with the TOE only via IF_GW_WAN,*
- *only authorized Gateway Administrators are allowed to establish a wake-up call,*

- *Transmission of meter data is only allowed via the interface IF_GW_MTR*

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

FDP_ACF.1.4
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
- *the Gateway Administrator is not allowed to read consumption data or the Consumer Log,*
- *Nobody must be allowed to read the symmetric keys used for encryption.*

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

Application Note 44 : The ST author has considered the regulations from [BSI-TR-03109-1] for additional rules regarding the Gateway access SFP.

6.5.3 FIREWALL SFP

6.5.3.1 Information flow control policy (FDP_IFC)

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

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

FDP_IFC.2.2/FW
The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Hierarchical to: FDP_IFC.1 Subset information flow control
Dependencies: FDP_IFF.1 Simple security attributes

6.5.3.2 Information flow control functions (FDP_IFF)

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

FDP_IFF.1.1/FW
The TSF shall enforce the *Firewall SFP* based on the following types of subject and information security attributes:
subjects: *The TOE and external entities on the WAN, HAN or LMN side*
information: *any information that is sent to, from or via the TOE*

attributes: *destination_interface (TOE, LMN, HAN or WAN),*
source_interface (TOE, LMN, HAN or WAN),
destination_authenticated,
source_authenticated.

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

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

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

(else if source_interface=TOE) and
destination_interface=HAN and
destination_authenticated=true
Connection establishment is allowed

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

(else if source_interface=WAN) and
destination_interface=TOE and
source_authenticated=true (by a verified Wake-Up packet)
Connection establishment is allowed

else
Connection establishment is denied

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

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

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

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

Application Note 45 : It should be noted that the FDP_IFF.1.1/FW facilitates different interfaces of the origin and the destination of an information flow implicitly requires the TOE to implement physically separate ports for WAN, LMN and HAN.

Application Note 46 : The assignment in FDP_IFF.1.2/FW is used by the ST author to specify additional rules (e.g., connections between devices in different HANs if the TOE is attached to more than one HAN) as long as those rules do not contradict the rest of the SFP. Specifically the TOE do not accept any connections from the WAN side.

6.5.4 METER SFP

6.5.4.1 Information flow control policy (FDP_IFC)

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

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

FDP_IFC.2.2/MTR
The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Hierarchical to: FDP_IFC.1 Subset information flow control
Dependencies: FDP_IFF.1 Simple security attributes

6.5.4.2 Information flow control functions (FDP_IFF)

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

FDP_IFF.1.1/MTR
The TSF shall enforce the *Meter SFP* based on the following types of subject and information security attributes:
subjects: *The TOE and external entities on the WAN or LMN side*
information: *any information that is sent via the TOE*
attributes: *destination interface, source interface (LMN or WAN), Processing Profile*

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

- *An information flow shall only be initiated if allowed by a corresponding Processing Profile.*

FDP_IFF.1.3/MTR

The TSF shall enforce the *following rules*:

- *Data received from Meters shall be processed as defined in the corresponding Processing Profile,*
- *Results of processing Meter Data shall be submitted to external entities as defined in the Processing Profiles,*
- *The internal system time shall be synchronised as follows:*
  - *The TOE shall compare the system time to a reliable external time source every 24 hours*
  - *If the deviation between the local time and the remote time is acceptable, the local system time shall be updated according to the remote time.*
  - *If the deviation is not acceptable, the TOE*
    - *shall ensure that any following Meter Data is not used,*
    - *stop operation and*
    - *inform a Gateway Administrator.*

FDP_IFF.1.4/MTR
The TSF shall explicitly authorise an information flow based on the following rules:
All local meters defined in the corresponding meter profile are authorized to communicate with the TOE.

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

Hierarchical to: No other components
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

Application Note 47 : FDP_IFF.1.3 defines that the TOE updates the local system time regularly with a reliable external time sources if the deviation is acceptable. In the context of this functionality two aspects should be mentioned:
Reliability of external source
The GWA provides a time source that has an acceptable reliability (operated by a trustworthy organization).
Acceptable deviation
Questioning whether a deviation between the time source in the WAN and the local system time is still acceptable, the implementation follows normative regulations based on [PTB_A50.8.

Application Note 48 : According to FDP_IFF.1.3: The operation of the TOE will not be stopped, instead all received meter values will be marked as invalid and the TOE tries to contact the NTP service.

Application Note 49 : FDP_IFF.1.5/MTR requires from the TOE to verify the authenticity, integrity and confidentiality of the Meter Data received from the Meter. Meter Data is considered as trustworthy when:

1. Using a wired meter:
Being received inside a channel between the Meter and the TOE using the functionality as described in FCS_COP.1/TLS.
2. Using a wireless meter:
Decrypted and verified according to FCS_COP.1/MTR.

6.5.5 GENERAL REQUIREMENTS ON USER DATA PROTECTION

6.5.5.1 Residual information protection (FDP_RIP)

6.5.5.1.1 FDP_RIP.2: Full residual information protection

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

Hierarchical to: FDP_RIP.1 Subset residual information protection
Dependencies: No dependencies.

Application Note 50 : 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 is ensured that this information is no longer available via an external interface (even if an access control or information flow policy would fail). However, this does not necessarily mean that the information is overwritten in a way that makes it impossible for an attacker to get access to is assuming a physical access to the memory of the TOE.

6.5.5.2 Stored data integrity (FDP_SDI)

6.5.5.2.1 FDP_SDI.2: Stored data integrity monitoring and action

FDP_SDI.2.1
The TSF shall monitor user data stored in containers controlled by the TSF for *integrity errors* on all objects, based on the following attributes:

- *Checksums for file system integrity.*
- *Structural integrity check for data containers.*
- *Signed checksums for measurement values and data of the calibration log.*

Application note 51 : The structural integrity is verified during daily system check.

FDP_SDI.2.2
Upon detection of a data integrity error, the TSF shall *inform the authorized Gateway Administrator*.

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring
Dependencies: No dependencies.

6.6 CLASS FIA: IDENTIFICATIOFMN AND AUTHENTICATION

6.6.1 USER ATTRIBUTE DEFINITION (FIA_ATD)

6.6.1.1 FIA_ATD.1: User attribute definition

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

- *User Identity*
- *Status of Identity (Authenticated or not)*
- *Connecting network (WAN, HAN or LMN)*
- *Role membership*
- *none*

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

6.6.2 AUTHENTICATION FAILURE HANDLING (FIA_AFL)

6.6.2.1 FIA_AFL.1: User authentication before any action

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

FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been met, the TSF shall *create a System Log entry and block IF_GW_CON for 5 minutes.*

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

6.6.3 USER AUTHENTICATION (FIA_UAU)

6.6.3.1 FIA_UAU.2: User authentication before any action

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

Hierarchical to: FIA_UAU.1
Dependencies: FIA_UID.1 Timing of identification

Application Note 52 : Please refer to [BSI-TR-03109-1] for a more detailed overview on the authentication of the TOE users.

6.6.3.2 FIA_UAU.5: Multiple authentication mechanisms

FIA_UAU.5.1
The TSF shall provide

- *authentication via certificates at the IF_GW_MTR interface*
- *TLS-authentication via certificates at the IF_GW_WAN interface*
- *TLS-authentication via HAN-certificates at the IF_GW_CON interface*
- *authentication via password at the IF_GW_CON interface*
- *TLS-authentication via HAN-certificates at the IF_GW_SRV interface*
- *TLS authentication at the IF_GW_CLS interface*
- *verification via a commands' signature*

to support user authentication.

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

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

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

Application Note 53 : Please refer to [BSI-TR-03109-1] for a more detailed overview on the authentication of the TOE users.

6.6.3.3 FIA_UAU.6: Re-authentication

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

- *TLS channel to the WAN shall be disconnected after 48 hours,*
- *TLS channel to the LMN shall be disconnected after 5 MB of transmitted information,*
- *Other local users shall be re-authenticated after 10 minutes of inactivity*

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

Application Note 54 : This requirement on re-authentication for external entities in the WAN and LMN is addressed by disconnecting the TLS channel even though a re-authentication is – strictly speaking -only achieved if the TLS channel is built up again.

6.6.4 User Identification (FIA_UID)

6.6.4.1 FIA_UID.2: User identification before any action

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

Hierarchical to: FIA_UID.1
Dependencies: No dependencies.

6.6.5 User-subject binding (FIA_USB)

6.6.5.1 FIA_USB.1: User-subject binding

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

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

- *User Identity:* *Defined in the communication profiles.*
- *Status of Identity:* *Authenticated or Non-authenticated.*
- *Connecting network:* *WAN or HAN network*
- *Role membership:* *Consumer, External Entity, Gateway Admin, Service Technician*

Application Note 55 : The TOE restricts the security attributes. The roles Gateway Admin, External entity are strictly bound to the WAN network, Consumer, Service Technician are bound to the HAN network.

FIA_USB.1.3
The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *none*

Application Note 56 : Changes to user security attributes are not allowed.

Hierarchical to: No other components.
Dependencies: FIA_ATD.1 User attributes definition

6.7 CLASS FMT: SECURITY MANAGEMENT

6.7.1 MANAGEMENT OF THE TSF

6.7.1.1 Management of functions in TSF

6.7.1.1.1 FMT_MOF.1: Management of security functions behavior

FMT_MOF.1.1
The TSF shall restrict the ability to modify the behavior of the functions *for management as defined in FMT_SMF.1* to *roles and criteria as defined in* ***table 16***.

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

table 16: Restrictions on Management Functions

6.7.1.2 Specification of Management Functions (FMT_SMF)

6.7.1.2.1 FMT_SMF.1: Specification of Management Functions

FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: *list of management functions as defined in table 17: SFR related Management Functionalities and* ***table 18****: Gateway specific Management Functionalities and none*.

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

SFR	Management functionality
FAU_ARP.1/SYS	~~The management (addition, removal, or modification) of actions.~~
FAU_GEN.1/SYS FAU_GEN.1/CON FAU_GEN.1/CAL	-
FAU_SAA.1/SYS	~~Maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.~~
FAU_SAR.1/SYS FAU_SAR.1/CON FAU_SAR.1/CAL	-
FAU_STG.4/SYS FAU_STG.4/CON	~~• Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.~~ • ~~Size configuration of the audit trail that is available before the oldest events get overwritten.~~
FAU_STG.4/CAL	-
FAU_GEN.2	-
FAU_STG.2	~~Maintenance of the parameters that control the audit storage capability for the consumer log and the system log.~~
FCO_NRO.2	The management of changes to ~~information types, fields, originator attributes and~~ recipients of evidence.
FCS_CKM.1/TLS	-
FCS_COP.1/TLS	Management of key material including key material stored in the Security Module
FCS_CKM.1/CMS	-
FCS_COP.1/CMS	Management of key material including key material stored in the Security Module
FCS_CKM.1/MTR	-
FCS_COP.1/MTR	Management of key material stored in the Security Module and key material brought into the gateway during the pairing process.
FCS_CKM.4	-
FCS_COP.1/HASH	-
FCS_COP.1/MEM	~~Management of key material~~
FDP_ACC.2	-
FDP_ACF.1	-
FDP_IFC.2/FW	-
FDP_IFF.1/FW	~~• Managing the attributes used to make explicit access based decisions.~~ • Add authorized units for communication (pairing). • Management of endpoint to be contacted after successful wake up call. • Management of CLS systems.

FDP_IFC.2/MTR	-
FDP_IFF.1/MTR	Managing the attributes (including Processing Profiles) used to make explicit access based decisions.
FDP_RIP.2	-
FDP_SDI.2	~~The actions to be taken upon the detection of an integrity error shall be configurable.~~
FIA_ATD.1	~~If so indicated in the assignment, the authorized Gateway Administrator might be able to define additional security attributes for users.~~
FIA_AFL.1	• ~~Management of the threshold for unsuccessful authentication attempts;~~ • ~~Management of actions to be taken in the event of an authentication failure.~~
FIA_UAU.2	~~Management of the authentication data by an Gateway Administrator~~
FIA_UAU.5	-
FIA_UAU.6	-
FIA_UID.2	The management of the user identities.
FIA_USB.1	• ~~An authorized Gateway Administrator can define default subject security attributes, if so indicated in the assignment of FIA_ATD.1.~~ • ~~An authorized Gateway Administrator can change subject security attributes, if so indicated in the assignment of FIA_ATD.1.~~
FMT_MOF.1	~~Managing the group of roles that can interact with the functions in the TSF.~~
FMT_SMF.1	-
FMT_SMR.1	Managing the group of users that are part of a role.
FMT_MSA.1/AC	~~Management of rules by which security attributes inherit specified values.~~
FMT_MSA.3/AC	-
FMT_MSA.1/FW	~~Management of rules by which security attributes inherit specified values.~~
FMT_MSA.3/FW	-
FMT_MSA.1/MTR	~~Management of rules by which security attributes inherit specified values.~~
FMT_MSA.3/MTR	-
FPR_CON.1	~~Definition of the interval in FPR_CON.1.2 if definable within the operational phase of the TOE~~
FPR_PSE.1	-
FPT_FLS.1	-
FPT_RPL.1	-
FPT_STM.1	Management of a time source.
FPT_TST.1	-
FPT_PHP.1	~~Management of the user or role that determines whether physical tampering has occurred.~~
FTP_ITC.1/WAN	-
FTP_ITC.1/MTR	-

FTP_ITC.1/USR	-

table 17: SFR related Management Functionalities

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

table 18: Gateway specific Management Functionalities

6.7.2 SECURITY MANAGEMENT ROLES (FMT_SMR)

6.7.2.1 FMT_SMR.1: Security roles

FMT_SMR.1.1
The TSF shall maintain the roles
- *authorized Consumer,*
- *authorized Gateway Administrator,*
- *authorized Service Technician*,
- *authorized External Entity and*
- *authorized CLS*

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

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

6.7.3 MANAGEMENT OF SECURITY ATTRIBUTES FOR GATEWAY ACCESS SFP

6.7.3.1 Management of security attributes (FMT_MSA)

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

FMT_MSA.1.1/AC
The TSF shall enforce the *Gateway access SFP* to restrict the ability to query, modify, delete *and none* the security attributes *all relevant security attributes* to *authorized Gateway Administrators*.

Hierarchical to: No other components.
Dependencies: [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

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

FMT_MSA.3.1/AC
The TSF shall enforce the *Gateway access SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

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

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

6.7.4 MANAGEMENT OF SECURITY ATTRIBUTES FOR FIREWALL SFP

6.7.4.1 Management of security attributes (FMT_MSA)

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

FMT_MSA.1.1/FW
The TSF shall enforce the *Firewall SFP* to restrict the ability to query, modify, delete *and none* the security attributes *all relevant security attributes* to *authorized Gateway Administrators*.

Hierarchical to: No other components.
Dependencies: [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

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

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

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

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

Application Note 57 : The definition of restrictive default rules for the firewall information flow policy refers to the rules as defined in FDP_IFF.1.2/FW and FDP_IFF.1.5/FW.

Those rules apply to all information flows and are not be overwritable by anybody.

6.7.5 MANAGEMENT OF SECURITY ATTRIBUTES FOR METER SFP

6.7.5.1 Management of security attributes (FMT_MSA)

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

FMT_MSA.1.1/MTR
The TSF shall enforce the *Meter SFP* to restrict the ability to change default, query, modify, delete and *none* the security attributes *all relevant security attributes* to *authorized Gateway Administrators*.

Hierarchical to:	No other components.
Dependencies:	[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

6.7.5.2 FMT_MSA.3/MTR: Static attribute initialization for Meter policy

FMT_MSA3.1/MTR
The TSF shall enforce the *Meter SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA3.2/MTR
The TSF shall allow the *no role* to specify alternative initial values to override the default values when an object or information is created.

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

6.8 CLASS FPR: PRIVACY

6.8.1 COMMUNICATION CONCEALING (FPR_CON)

6.8.1.1 FPR_CON.1: Communication Concealing

FPR_CON.1.1
The TSF shall enforce the *Firewall SFP* in order to ensure that no PII (Personal Identity Information) can be obtained by an analysis of *all characteristics of the information flow that need to be concealed*.

FPR_CON.1.2

The TSF shall connect to *the Gateway Administrator* in intervals as follows: *daily* to conceal the data flow.

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

Application Note 58 :	Concealment shall be achieved via a daily Time-synchronization and a notification about the self-integrity-test. The self-integrity-test is triggered randomly during low usage of the TOE resources.

6.8.2 PSEUDONYMITY (FPR_PSE)

6.8.2.1 FPR_PSE.1 Pseudonymity

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

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

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

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

Application Note 59 :	When the TOE submits information about the consumption or production of a certain commodity that is not relevant for the billing process nor for a secure operation of the Grid, there is no need that this information is sent with a direct link to the identity of the consumer. In those cases, the TOE shall replace the identity of the consumer by a pseudonymous identifier. Please note that the identity of the consumer may not be its name but could also be a number (e.g., consumer ID) used for billing purposes. A Gateway may use more than one pseudonymous identifier delivered by the GWA. A complete anonymisation would be beneficial in terms of the privacy of the consumer. However, a complete anonymous set of information would not allow the external entity to ensure that the data comes from a trustworthy source. Please note that an information flow is only initiated if allowed by a corresponding Processing Profile.

6.9 CLASS FPT: PROTECTION OF THE TSF

6.9.1 FAIL SECURE (FPT_FLS)

6.9.1.1 FPT_FLS.1: Failure with preservation of secure state

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

- *the deviation between local system time of the TOE and the reliable external time source is too large*
- *the flash memory is exhausted*
- *database integrity error*
- *hardware initialization error*

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

Application Note 60 : The local clock is exact as required by normative or legislative regulations based on [PTB_A 50.8].

Application Note 61 : The TOE will return to normal operation as soon as the local system time is considered valid again.

6.9.2 REPLAY DETECTION (FPT_RPL)

6.9.2.1 FPT_RPL.1: Replay detection

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

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

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

6.9.3 TIME STAMPS (FPT_STM)

6.9.3.1 FPT_STM.1: Reliable time stamps

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

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

Application Note 62 : The time stamps as defined by FPT_STM.1 shall be of sufficient exactness. Therefore, the local system time of the TOE is synchronised regularly with a reliable external time source. Radio controlled clocks shall not be used. However, the local clock also needs a sufficient exactness as the synchronisation will fail if the deviation is too large (the TOE will preserve a secure state according to FPT_FLS.1).
Therefore the local clock shall be as exact as required by normative or legislative regulations. If no regulation exists, a maximum deviation of 3% of the measuring period is allowed to be in conformance with the Protection Profile.

6.9.4 TSF SELF-TEST (FPT_TST)

6.9.4.1 FPT_TST.1: TSF testing

FPT_TST.1.1
The TSF shall run a suite of self-tests during initial start-up, at the request of a user and periodically during normal operation to demonstrate the correct operation of the TSF.

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

FPT_TST.1.3
The TSF shall provide authorized users with the capability to verify the integrity of TSF.

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

Application Note 63 : The self-test suite as defined in FPT_TST.1 contains a test that detects whether the interfaces for WAN and LAN are separate. It should be noted that the possibility of the Gateway to detect such a misconfiguration are limited. The classical way would be that the Gateway tries to reach a known source in the WAN via a LAN interface. If such a request succeeds the test fails. Further, to the test the TSF, the self-test suite contains a test to verify the integrity of the TOE firmware.

6.9.4.2 FPT_PHP.1: Passive detection of physical attack

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

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

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

Application Note 64 : A passive detection of a physical attack is classically achieved by a seal and an appropriate physical design of the TOE that allows the consumer (or any other party) to verify the physical integrity of the TOE.
The level of protection that is required by FPT_PHP.1 is the same level of protection that is expected for classical meters. Exact requirements can be found in the regulations of the national calibration authority [TR-03109-1].

6.10 CLASS FTP: TRUSTED PATH/CHANNEL

6.10.1 INTER-TSF TRUSTED CHANNEL (FTP_ITC)

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

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

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

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

Hierarchical to: No other components
Dependencies: No dependencies.

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

FTP_ITC1.1/MTR
The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

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

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

Hierarchical to: No other components.
Dependencies: No dependencies

Application Note 65 : The corresponding cryptographic primitives are defined by FCS_COP.1/MTR.

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

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

FTP_ITC.1.2/USR
The TSF shall permit **the consumer, the service technician** to initiate communication via the trusted channel.

FTP_ITC.1.3/USR
The TSF shall initiate communication via the trusted channel for *any communication between a consumer and the TOE or the service technician and the TOE*.

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

Application Note 66 : The TOE do not possess a local display.

6.11 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

The minimum Evaluation Assurance Level for this Security Target is **EAL 4 augmented by AVA_VAN.5 and ALC_FLR.2**.

The following table lists the assurance components which are therefore applicable to this ST.

Assurance Class	Assurance Component
Development	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1
	ALC_FLR.2
Security Target Evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1

	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	AVA_VAN.5

table 19: Assurance Requirements

6.12 SECURITY REQUIREMENTS RATIONALE

6.12.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

6.12.1.1 Fulfilment of the Security Objectives

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

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access
FAU_ARP.1/SYS									**X**	
FAU_GEN.1/SYS									X	
FAU_SAA.1/SYS									X	
FAU_SAR.1/SYS									X	
FAU_STG.4/SYS									X	
FAU_GEN.1/CON									X	
FAU_SAR.1/CON									X	
FAU_STG.4/CON									X	
FAU_GEN.1/CAL									X	
FAU_SAR.1/CAL									X	
FAU_STG.4/CAL									X	
FAU_GEN.2									X	
FAU_STG.2									X	
FCO_NRO.2				X						
FCS_CKM.1/TLS					X					
FCS_COP.1/TLS					X					
FCS_CKM.1/CMS					X					
FCS_COP.1/CMS					X					

FCS_CKM.1/MTR					X					
FCS_COP.1/MTR					X					
FCS_CKM.4					X					
FCS_COP.1/HASH					X					
FCS_COP.1/MEM					X		X			
FDP_ACC.2										X
FDP_ACF.1										X
FDP_IFC.2/FW	X	X								
FDP_IFF.1/FW	X	X								
FDP_IFC.2/MTR				X		X				
FDP_IFF.1/MTR				X		X				
FDP_RIP.2							X			
FDP_SDI.2							X			
FIA_ATD.1								X		
FIA_AFL.1								X		
FIA_UAU.2								X		
FIA_UAU.5										X
FIA_UAU.6										X
FIA_UID.2								X		
FIA_USB.1								X		
FMT_MOF.1								X		
FMT_SMF.1								X		
FMT_SMR.1								X		
FMT_MSA.1/AC								X		
FMT_MSA.3/AC								X		
FMT_MSA.1/FW								X		
FMT_MSA.3/FW								X		
FMT_MSA.1/MTR								X		
FMT_MSA.3/MTR								X		
FPR_CON.1			X							
FPR_PSE.1				X						
FPT_FLS.1							X			
FPT_RPL.1					X					
FPT_STM.1						X			X	
FPT_TST.1		X					X			
FPT_PHP.1							X			
FTP_ITC.1/WAN	X									
FTP_ITC.1/MTR				X						
FTP_ITC.1/USR									X	

table 20: Fulfilment of Security Objectives

The following paragraphs contain more details on this mapping.

6.12.1.1.1 O.Firewall

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

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

6.12.1.1.2 O.SeparateIF

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

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

6.12.1.1.3 O.Conceal

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

6.12.1.1.4 O.Meter

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

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

6.12.1.1.5 O.Crypt

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

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

6.12.1.1.6 O.Time

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

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

6.12.1.1.7 O.Protect

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

- **FCS_COP.1/MEM** defines that the TOE shall encrypt its TSF and user data as long as it is not in use.
- **FDP_RIP.2** defines that the TOE shall make information unavailable as soon as it is not 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 interface 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 authorized Gateway Administrators via the IF_GW_WAN interface and to authorizes 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 authorized 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 authorized Gateway Administrator via the IF_GW_WAN interface.

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

6.12.1.1.10 O.Access

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

6.12.1.2 Fulfilment of the dependencies

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

		FAU_GEN.1/CON FAU_GEN.1/CAL
FCO_NRO.2	FIA_UID.1 Timing of identification	FIA_UID.2
FCS_CKM.1/TLS	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/TLS FCS_CKM.4
FCS_COP.1/TLS	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1Cryptographic 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/TLS 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.1Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/CMS FCS_CKM.4
FCS_CKM.1/MTR	FCS_CKM.2Cryptographic key distribution, or FCS_COP.1Cryptographic operation] FCS_CKM.4Cryptographic 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.1Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/MTR FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1Cryptographic 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.1Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 Please refer to chapter 6.12.1.3 for missing dependency
FCS_COP.1/MEM	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security	FCS_CKM.1/CMS FCS_CKM.4

	attributes, or FCS_CKM.1Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	
FDP_ACC.2	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.2 FMT_MSA.3/AC
FDP_IFC.2/FW	FDP_IFF.1 Simple security attributes	FDP_IFF.1/FW
FDP_IFF.1/FW	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.2/FW FMT_MSA.3/FW
FDP_IFC.2/MTR	FDP_IFF.1 Simple security attributes	FDP_IFF.1/MTR
FDP_IFF.1/MTR	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.2/MTR FMT_MSA.3/MTR
FDP_RIP.2	-	-
FDP_SDI.2	-	-
FIA_ATD.1	-	-
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.2
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UAU.5	-	-
FIA_UAU.6	-	-
FIA_UID.2	-	-
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR1 FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FMT_MSA.1/AC	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.2 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3/AC	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/AC FMT_SMR.1
FMT_MSA.1/FW	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_IFC.2/FW FMT_SMR.1 FMT_SMF.1
FMT_MSA.3/FW	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/FW FMT_SMR.1
FMT_MSA.1/MTR	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management	FDP_IFC.2/MTR FMT_SMR.1 FMT_SMF.1

	Functions	
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 21: SFR Dependencies

6.12.1.3 Justification for missing dependencies

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

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 (TSS)

The following section explains how the security functions are implemented that cover the security requirements.

- This TOE fulfils all the requirements defined in [BSI-CC-PP-0073-2014]

In order to realize the features described in chapter 1.3 the TOE implements networking and metering functionalities. The primary security features of the TOE are:

- Cryptographic functionality and TLS handling
- Identification, authentication and authorization
- Self-protection and security management

7.1 CRYPTOGRAPHIC FUNCTIONALITY AND TLS HANDLING

7.1.1 CRYPTOGRAPHIC PRIMITIVES AND CERTIFICATE GENERATION

All key material (including the PACE key) stored in the TOE will be deleted using the key overwriting and NV memory zeroization standard (FCS_CKM.4.1).

The TOE implements the TLSv1.2 protocols as specified in the respective RFC. All cryptographic primitives (demanded in [BSI-TR 03116-3]) required by the protocols as well as other services in the TOE are fully implemented in the TOE, including:

cryptographic primitive	
digital signature	ECDSA (Elliptic Curve Digital Signature Algorithm)
key exchange	ECKA-DH (Elliptic Curve Key Agreement , Diffie-Hellman)
key transportation	ECKA-EG (Elliptic Curve Key Agreement, ElGamal)
block chiffre	AES • CBC-Mode • CMAC-Mode • GCM-Mode • XTS-Mode
hash functions	SHA-2 family

(FCS_COP.1/HASH, FCS_CKM.1/TLS, FCS_COP.1/TLS, FCS_CKM.1/CMS, FCS_COP.1/CMS, FCS_CKM.1/MTR, FCS_COP.1/MTR, FCS_COP.1/MEM).

A security module according to [BSI-TR-03109-2] and [BSI-CC-PP-0077-2015] is used to generate certificates.

The following keys and certificates are stored securely within the Security Module:

- ROOT_WAN_SIG_CRT (SM-PKI-ROOT-Certificate)
- Pace PIN

- Key for memory encryption
- Gateway Admin certificates for TLS communication, encryption, signature generation and authentication
- Gateway key pairs for TLS communication, encryption, signature generation and authentication

7.1.2 TLS HANDLING

The first phase within the TLS protocol is the handshake protocol, in which a cryptographic cipher suite (consisting of an asymmetric algorithm, a bulk data encryption algorithm, the key size for the bulk data encryption algorithm, a hash algorithm) and cryptographic keys (encryption/decryption keys, MAC secrets) are negotiated. Following cipher suites are supported by the TOE:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Separate bulk data encryption keys and MAC secrets are generated for each communication direction. The handshake protocol uses SHA-2 family (TLSv1.2) to create these session keys and MAC secrets. The MAC secrets are used for protecting integrity of the information exchanged.

After the handshake protocol has been successfully completed, user data can be securely transferred according to the agreed cipher suite. The TLS protocol ensures the confidentiality and integrity of transmitted user data.

Integrity is achieved specifically by the HMAC mechanism for message authentication using cryptographic hash functions in combination with the secret shared keys (MAC secrets). Concealment of asymmetric encrypted secrets is achieved by adding padding bytes according to the [RFC-5652] standard. A proper implementation of the TLS protocol allows detection of modification of data, substitution of data, re-ordering of data, deletion of data, insertion of data and replay of data as well as it prevents disclosure of data.

7.2 IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION

The TOE contains a firewall and an access control management.
The firewall enforces an information flow control policy based on [BSI-CC-PP-0073-2014] FDP_IFF.1.2/FW.
Communication that passes the firewall is handled by the access control management which restricts data access for each user to data which is explicitly assigned to this user.
(FDP_ACC.2, FDP_ACF.1, FDP_IFC.2/FW, FDP_IFF.1/FW, FDP_IFC.2/MTR, FDP_IFF.1.1/MTR, FMT_MOF.1)
These functionalities also handle connection establishment for the different interfaces:

- Communication via IF_GW_WAN is initiated by the TSF
- Communication via IF_GW_MTR is initiated by the meter
- Communication via IF_GW_CON is initiated by the consumer

(FTP_ITC.1/USR, FTP_ITC.1/WAN)

User authentication is performed for communication via all interfaces according to TR-03109. A virtual file system is used, which allows only authenticated users via defined interfaces access to their data. For this functionality user attributes are maintained for each user. The system log is assigned to the Gateway Admin and the Service Technician, the calibration log only to the Gateway Administrator. For each end consumer a separate consumer log is provided. No user is allowed to alter or delete any log entries.
(FAU_SAR.1, FAU_STG.2, FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FIA_USB.1)

The only user which is allowed to alter parameters is the SMGW Gateway Administrator. The changes are restricted to those defined in BSI-TR-03109, limited or expanded by FMT_MSA.1.

All data (including meter data) are handled according to [BSI-CC-PP-0073-2014]. This includes pseudonymisation of user data to guarantee data privacy as well as user data encryption.
Meter data are provided with a time stamp and an Identifier for allocation to the meter and validated regarding authenticity, integrity and confidentiality. The handling of meter data is further defined in Processing Profiles.
(FCO_NRO.2, FDP_IFF.1/MTR, FDP_IFC.2/MTR, FMT_MSA.1/MTR, FPR_PSE.1, FPT_STM.1, FTP_ITC.1/MTR)
The system time is synchronized with a legal time provided by the PTB to guarantee reliable time stamps (FPT_STM.1).

7.3 SELF PROTECTION AND SECURITY MANAGEMENT

7.3.1 SELF PROTECTION

The TOE periodically performs a self-test to detect malfunction or manipulation. This includes a data integrity check (including the TSF itself) using checksums and the evaluation of logging entries. This test can also be started by a user request. If a potential security violation is detected, the Gateway Administrator is informed.
(FAU_ARP.1/SYS, FAU_SAA.1, FDP_SDI.2.2, FPT_TST.1)

If the time deviation is too high or a hardware error is detected, the TOE will always stay in a defined state. This secure state will be differentiated by the event causing unexpected behavior:

- In case of an illegitimate time basis, the TOE falls into the secure state. A recovery from the secure state is possible if valid system time can be retrieved from a trusted external time source.
- In case of a hardware error the TOE will switch into the secure state.

(FPT_FLS.1)

Besides a self-test on a regular basis, the TOE also actively monitors all data communication including the time of reception. In case of reaching a configurable threshold delay, these data packets will be dropped in order to avoid replay attacks with captured data packets (FPT_RPL.1).

The TOE only accepts authenticated communication channels. If the TOE refuses the connection to a specific communication partner several times (configurable number of attempts), the TOE will block this specific communication partner for a defined time span (FIA_AFL.1).

In order to prevent reading deallocated data, these resources will be overwritten after the deallocation of this data by a process or access protected using a transparent overlay file system (FDP_RIP.2).

The TOE performs a re-authentication process after a defined time or amount of transmitted data or inactivity of the connected user. (FIA_UAU.6)

Connections to the external entities are established periodically in order to conceal the communication. This is handled by the firewall functionality. (FPR_CON.1)

The TOE contains a consumer log for all end consumers as well as a system log and a calibration log. All logs are implemented and provided according to BSI-TR-03109. The calibration log is never deleted. Before the storage capacity is exceeded, the Gateway Administrator is informed. If the storage capacity is exceeded, the TOE will fall into the secure state (FPT_FLS.1). Consumer and system log are designed as circular buffers. The oldest entries are overwritten if the storage capacity is exceeded. Before deletion the Gateway Administrator (system log) is informed (FAU_GEN.1, FAU_SAR.1, FAU_STG.4.1, FAU_GEN.2).

For each log all entries will always be maintained even in case of an audit storage exhaustion or failure by a log file backup system (FAU_STG.2).

7.3.2 SECURITY MANAGEMENT

A security management system is implemented in the TOE in order to preserve the security functionality in any case. Nobody should be able to circumvent a single security function provided by the TOE (FMT_SMF.1).

The security functionalities of the TOE are protected against intentional and unintentional manipulation by a user. Therefore, all users are assigned to security roles and provided with security attributes. Following roles are available in the TOE:

- Authorized consumer
- Authorized gateway administrator
- Authorized service technician
- Authorized External Entity (FMT_SMR.1).

The default values of the security attributes, which are handled in the processing profiles, are restrictive and cannot be changed by any user. In case of an error or failing of plausibility checks, these default security parameters will be used in order to prevent unauthorized actions on the TOE (FMT_MSA.3).

8 APPENDIX

8.1 GLOSSARY SUPPLEMENT

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])
Confidentiality	the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (according to [SD-6])
Consumer	End user of electricity, gas, water or heat. (according to [CEN]), See chapter 3.1
DTBS	Data To Be Signed
Energy Service Provider	Organisation offering energy related services to the consumer (according to [CEN])
Home Area Network (HAN)	In-house LAN which interconnects domestic equipment and can be used for energy management purposes. (according to [CEN])
Independent Service Provider	Company independent of grid operators, supply companies and metering companies that uses an infrastructure which supports smart metering (according to [CEN])
Integrity	property that sensitive data has not been modified or deleted in an unauthorized and undetected manner (according to [SD-6])
IT-System	Computer system
Aggregator (MDA)	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	In-house LAN which interconnects metrological equipment (i.e.Meters) and can be used for energy management purposes. (according to [CEN])

Network	
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
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])

8.2 REFERENCES SUPPLEMENT

9 BIBLIOGRAPHY

[BSI-CC-PP-0073-2014]	BSI-CC-PP-0073-2014, Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP) - Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, Version 1.3
[BSI-CC-PP-0077-2015]	Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), Version 1.03, BSI-CC-PP-0077-V2-2015
[BSI-DSZ-CC-1003-2018]	BSI-DSZ-CC-1003-2018 Smart Meter Gateway Security Module Application on MultiApp V4 Revision A, 2018
[BSI-TR-03109]	BSI TR-03109: Dachdokument, Version 1.1
[BSI-TR-03109-1]	BSI TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messystems, Version 1.1.
[BSI-TR-03109-1-I]	BSI TR-03109-1 Anlage I, BSI, CMS Datenformat für die Inhaltsdatenverschlüsselung und -signatur, Version1.09
[BSI-TR-03109-1-VI]	BSI TR-03109-1 Anlage VI: Betriebsprozesse, Version 1.0
[BSI-TR-03109-3]	BSI TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, Version 1.1.
[BSI-TR-03111]	BSI TR-03111 Elliptic Curve Cryptography, Version 2.10
[BSI-TR-03116-3]	BSI TR-03116-3 Kryptographische Vorgaben für Projekte der Bundesregierung Teil3, Stand: 2023
[CC]	Common Criteria, Common Criteria for Information Technology Security Evaluation, Version 3.14 Revision 4.
[CEN]	SMART METERS CO-ORDINATION GROUP (SM-CG) Item 5. M/441 first phase deliverable – Communication – Annex: Glossary (SMCG/Sec0022/DC).
[FIPS-180-4]	FIPS 180-4 Secure Hash Standard (SHS), 2015
[FIPS-197]	FIPS 197 Advanced Encryption Standard (AES), 2001
[IEEE-1619]	IEEE 1619-2018, IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices, 2018
[ISO/IEC-18033-2:2006]	Information technology — Security techniques — Encryption algorithms — Part 2:Asymmetric ciphers, 2006

[NIST-SP800-38A]	NIST SP 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001
[NIST-SP800-38D]	NIST SP 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007
[PTB-A50.7]	Anforderungen an elektronische und software-gesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme, PTB-A 50.7, April 2002.
[PTB-A50.8]	PTB Anforderungen Smart Meter Gateway, Dezember 2014.
[RFC-2104]	IETF RFC 2104, H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing for Message Authentication, 1997
[RFC-3394]	IETF RFC 3394, J. Schaad: Advanced Encryption Standard (AES) Key Wrape Algorithm, 2002
[RFC-4493]	ETF RFC 4493, JH. Song, R. Poovendran, The AES-CMAC Algorithm, 2006
[RFC-5084]	IETF RFC 5084. R. Housley: Using AES-CCM and AES-CGM Authenticated Encryption in the Crypto-graphic Message Syntax (CMS)
[RFC-5246]	IETF RFC 5246, T. Dierks: The Transport Layer Security (TLS) Protocol Version 1.2, 2008
[RFC-5289]	IETF RFC 5289, M. Rescorla: TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (CGM), 2008
[RFC-5652]	IETF RFC 5652, R. Housley, Cryptographic Message Syntax (CMS), 2009
[SD-6]	ISO/IEC JTC 1/SC 27 N7446 Standing Document 6 (SD6): Glossary of IT Security Terminology 2009-04-29 http://www.jtc1sc27.din.de/sce/sd6