Federal Office
for Information Security

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

SMGW-PP

Version 1.3 - 31 March 2014

(Final Release)

Certification-ID: BSI-CC-PP-0073

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-0
E-Mail: SmartMeter@bsi.bund.de
Internet: http://www.bsi.bund.de

Table of content

112

List of Tables

List of Figures

1 PP introduction

1.1 Introduction

The increasing use of *green energy* and upcoming technologies around e-mobility lead to an increasing demand for functions of a so called smart grid. A smart grid hereby refers to a commodity[1] network that intelligently integrates the behaviour and actions of all entities connected to it – suppliers of natural resources and energy, its consumers and those that are both – in order to efficiently ensure a more sustainable, economic and secure supply of a certain commodity (definition adopted from [CEN]).

In its vision such a smart grid would allow to invoke consumer devices to regulate the load and availability of resources or energy in the grid, e.g. by using consumer devices to store energy or by triggering the use of energy based upon the current load of the grid[2]. Basic features of such a smart use of energy or resources are already reality. Providers of electricity in Germany, for example, have to offer at least one tariff that has the purpose to motivate the consumer to save energy.

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

An essential aspect for all considerations of a smart grid is the so called Smart Metering System that meters the consumption or production of certain commodities at the consumer's side and allows sending the information about the consumption or production to external entities, which is then the basis for e.g. billing the consumption or production.

This Protection Profile defines the security objectives and corresponding requirements for a Gateway which is the central communication component of such a Smart Metering System (please refer to chapter 1.4.2 for a more detailed overview). The PP is directed to developers of Smart Meter Gateways and informs them about the requirements that have to be implemented. It is further directed to stakeholders being responsible for purchasing Smart Meter Gateways.

The Target of Evaluation (TOE) that is described in this document is an electronic unit comprising hardware and software/firmware[3] used for collection, storage and provision of Meter Data[4] from one or more Meters of one or multiple commodities.

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

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

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

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

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

[3] For the rest of this document the term "firmware" will be used.

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

176 ## 1.2 PP Reference

Title:	Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)
Version	1.3 (Final Release)
Date	31.03.2014
Authors	Dr. Helge Kreutzmann, M.Sc. Stefan Vollmer (BSI)
Registration	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security, Germany
Certification-ID	BSI-CC-PP-0073
Evaluation Assurance Level:	The assurance level for this PP is EAL 4 augmented by AVA_VAN.5 and ALC_FLR.2.
CC-Version	3.1 Revision 4
Keywords	Smart Metering, Protection Profile, Meter, Gateway, PP

177 ## 1.3 Specific terms

178 Various different vocabularies exist in the area of Smart Grid, Smart Metering, and Home Automation.
179 Further, the Common Criteria maintain their own vocabulary. The following table provides an
180 overview over the most prominent terms that are used in this Protection Profile and should serve to
181 avoid any bias. A complete glossary and list of acronyms can be found in chapter 7.2.

Term	Definition	Source (if any)
CLS, Controllable Local Systems	CLS are systems containing IT-components in the Home Area Network (HAN) of the consumer that do not belong to the Smart Metering System but may use the Gateway for dedicated communication purposes. CLS may range from local power generation plants, controllable loads such as air condition and intelligent household appliances (“white goods”) to applications in home automation.	
Commodity	Electricity, gas, water or heat[5]	
Consumer	End user of electricity, gas, water or heat. The consumer can also generate energy using a Distributed Energy Resource.	[CEN]

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

Term	Definition	Source (if any)
Gateway Smart Meter Gateway (SMGW)[6]	Device or unit responsible for collecting Meter Data, processing Meter Data, providing communication capabilities for devices in the LMN, protecting devices in the LAN (such as Controllable Local Systems) against attacks from the WAN and providing cryptographic primitives (in cooperation with a Security Module). The Gateway is specified in this document and combines aspects of the following devices according to [CEN]: • Meter Data Collector • Meter Data Management System • Meter Data Aggregator The Gateway does not aim to be a complete implementation of those devices but focusses on the required security functionality.	
Gateway Administrator	Authority that installs, configures, monitors, and controls the Smart Meter Gateway.	
HAN, Home Area Network	In-house data communication network which interconnects domestic equipment and can be used for energy management purposes.	[CEN], adopted
LAN, Local Area Network	Data communication network, connecting a limited number of communication devices (Meters and other devices) and covering a moderately sized geographical area within the premises of the consumer. In the context of this PP the term LAN is used as a hypernym for HAN and LMN.	[CEN], adopted
LMN, Local Metrological Network	In-house data communication network which interconnects metrological equipment.	
Meter	The term Meter refers to a unit for measuring the consumption or production of a certain commodity with additional functionality. It collects consumption or production data and transmits this data to the Gateway. As not all aspects of a Smart Meter according to [CEN] are implemented in the descriptions within this document the term Meter is used. The Meter has to be able to encrypt and sign the data it sends and will typically deploy a Security Module for this. Please note that the term Meter refers to metering devices for all kinds of commodities.	[CEN], adopted

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

Term	Definition	Source (if any)
Meter Data	Meter readings that allow calculation of the quantity of a commodity, for example electricity, gas, water or heat consumed or produced over a period. Other readings and data may also be included[7] (such as quality data, events and alarms).	[CEN]
Security Module	A Security device utilised by the Gateway for cryptographic support – typically realised in form of a smart card. The complete description of the Security Module can be found in [SecMod-PP].	
Service Technician	Human entity that is responsible for diagnostic purposes.	
Smart Metering System	The Smart Metering System consists of a Smart Meter Gateway and connected to one or more meters. In addition, CLS (i.e. generation plants) may be connected with the gateway for dedicated communication purposes.	
User, external entity	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary.	[CC]
WAN, Wide Area Network	Extended data communication network connecting a large number of communication devices over a large geographical area.	[CEN]

182 **Table 1: Specific Terms**

183 1.4 TOE Overview

184 1.4.1 Introduction

185 The TOE as defined in this Protection Profile is the Gateway in a Smart Metering System. In the
186 following subsections the overall Smart Metering System will be described first and afterwards the
187 Gateway itself.

188 1.4.2 Overview of the Gateway in a Smart Metering System

189 The following figure provides an overview of the TOE as part of a complete Smart Metering System
190 from a purely functional perspective as used in this PP.[8]

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

[8] 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 PP. It does not aim to provide a universal description of a Smart Metering System for all application cases.

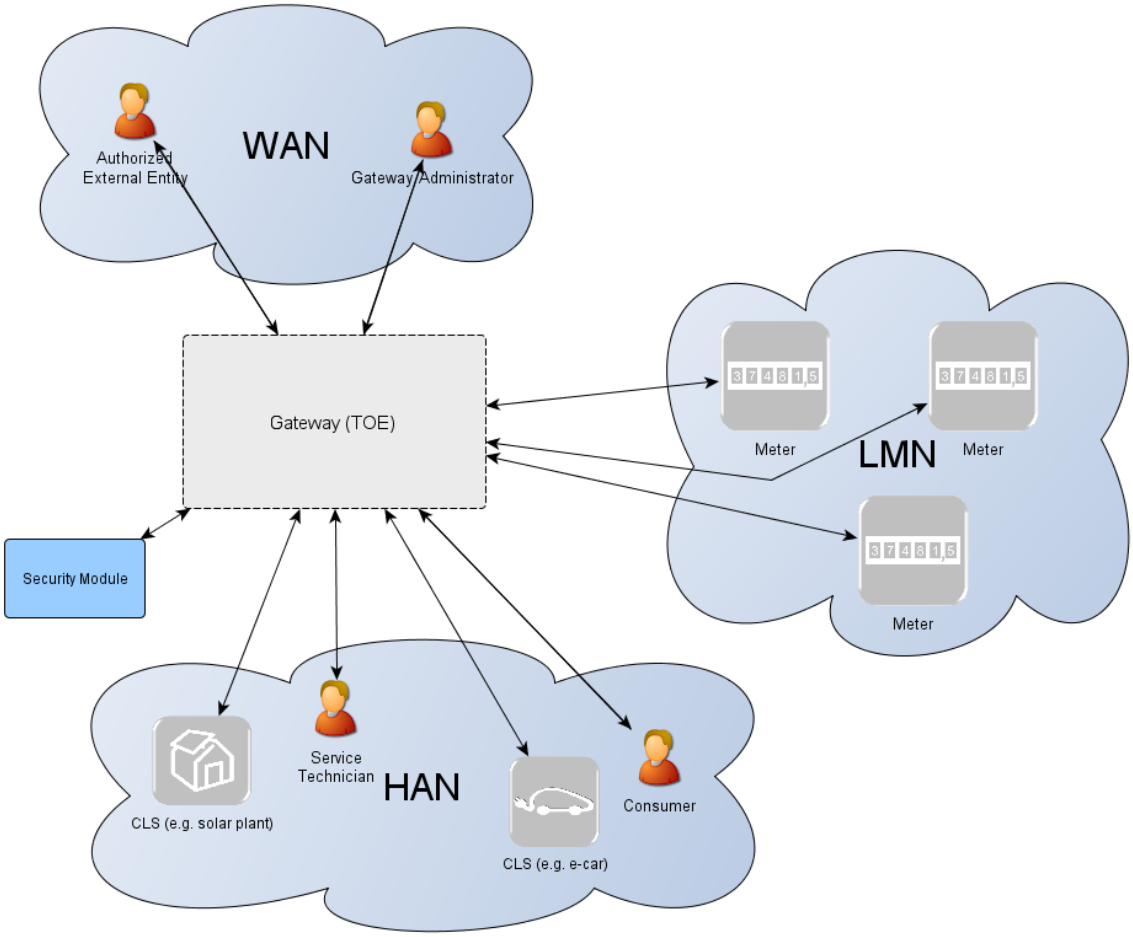


Figure 1: The TOE and its direct environment

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

- The **Gateway** (as defined in this PP) serves as the communication component between the components in the LAN of the consumer (such as meters and added generation plants) and the outside world. It can be seen as a special kind of firewall dedicated to the smart metering functionality. It also collects, processes, and stores the records from Meter(s) and ensures that only authorised parties have access to them or derivatives thereof. Before sending Meter Data[9] the information will be encrypted and signed using the services of a Security Module. The Gateway features a mandatory user interface, enabling authorised consumers to access the data relevant to them.
- The **Meter** itself records the consumption or production of one or more commodities (e.g. electricity, gas, water, heat) and submits those records in defined intervals to the Gateway. The Meter Data has to be signed and encrypted before transfer in order to ensure its confidentiality, authenticity, and integrity. The Meter is comparable to a classical meter[10] and has comparable security requirements; it will be sealed as classical meters according to the regulations of the

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

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

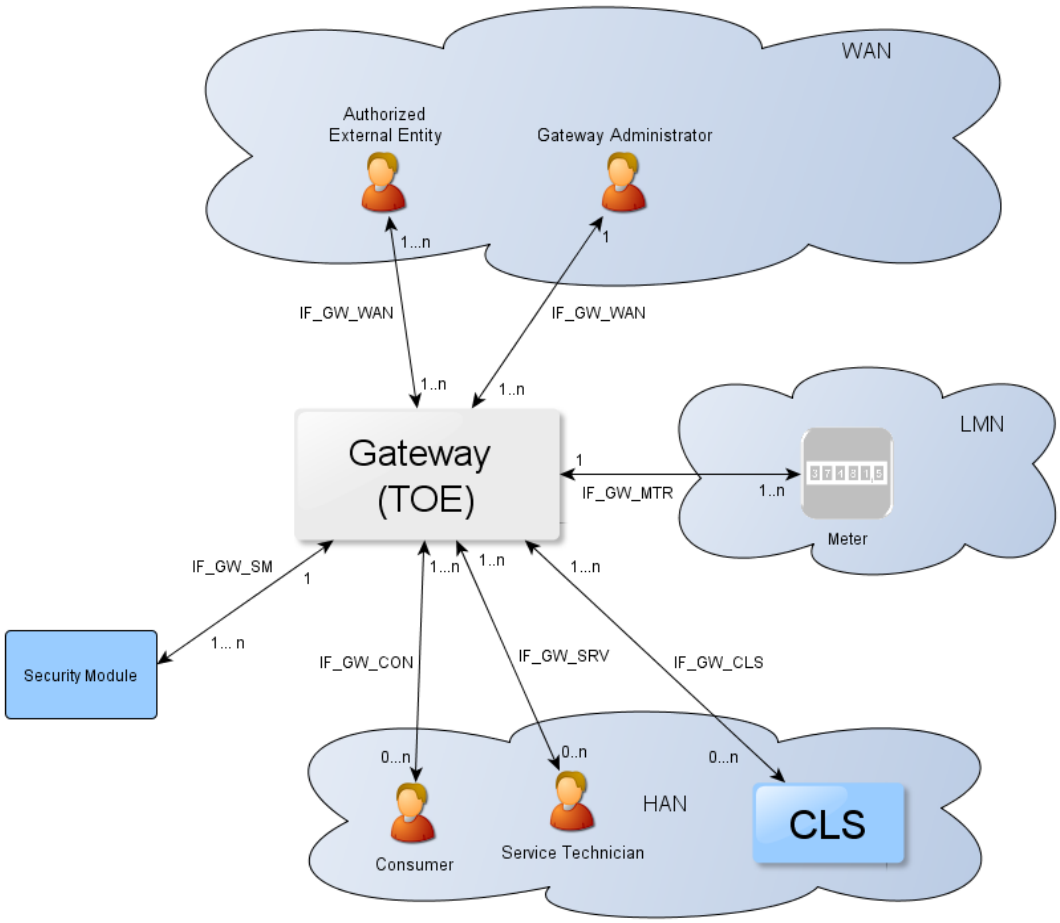
208 calibration authority. The Meter further supports the encryption and integrity protection of its
209 connection to the Gateway[11].

210 • The Gateway utilises the services of a **Security Module** (e.g. a smart card) as a cryptographic
211 service provider and as a secure storage for confidential assets. The Security Module will be
212 evaluated separately according to the requirements in the corresponding Protection Profile
213 (c.f. [SecMod-PP]).

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

218 The following figure introduces the external interfaces of the TOE and shows the cardinality of the
219 involved entities.

220 Please note that the arrows of the interfaces within the Smart Metering System as shown in Figure 2
221 indicate the flow of information. However, it does not indicate that a communication flow can be
222 initiated bi-directionally. Indeed, the following chapters of this PP will place dedicated requirements
223 on the way an information flow can be initiated[12].



224
225 **Figure 2: The logical interfaces of the TOE**

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

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

The overview of the Smart Metering System as described before is based on a 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 shall be the only unit directly connected to the WAN, to be the first line of defence an attacker located in the WAN would have to conquer.
- The Gateway is the central component that 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 CLS with the WAN there might be more Meters and CLS in a Smart Metering System than there are Gateways.

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

It should be noted that this Protection Profile does not aim to imply any concrete system architecture or product design as long as the security requirements from this Protection Profile are fulfilled. Only in cases where the implementation of the Security Functional Requirements will definitely requires a certain architecture, this architecture is described in this PP 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 PP 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. Possible forms of implementing the units of a Smart Metering System in components are described in chapter 1.4.5.

1.4.3 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[13] 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[14].

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

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

1.4.4 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.

1.4.5 TOE physical boundary

1.4.5.1 Introduction

The TOE comprises the hardware and firmware that is relevant for the security functionality of the Gateway as defined in this PP. The Security Module that is utilised by the TOE is considered being not part of the TOE[15].

As mentioned in chapter 1.4.2 this Protection Profile does not want to imply any concrete physical architecture for the components that make up the Smart Metering System. The following sections introduce some examples of physical representations for the different components of the Smart Metering System – focussing on the Gateway.

It should be noted that this overview of possible physical implementations does not claim being a complete overview of all possibilities. The Common Criteria allow to combine multiple TOE into one device and have the flexibility to identify functionality that is not relevant for the security functionality of the TOE or the environment. However, when focussing on a system of multiple TOEs, it is not possible to move security features from the scope of one TOE to another.

[15] Please note that the security module is physically integrated into the Gateway even though it is not part of the TOE.

1.4.5.2 Possible TOE design: A Gateway and multiple Meters

The following figure provides an example for an implementation of a Gateway as defined in this PP from a physical perspective.

It is possible that 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 TOE (e.g. the unit for communication[16]), 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.

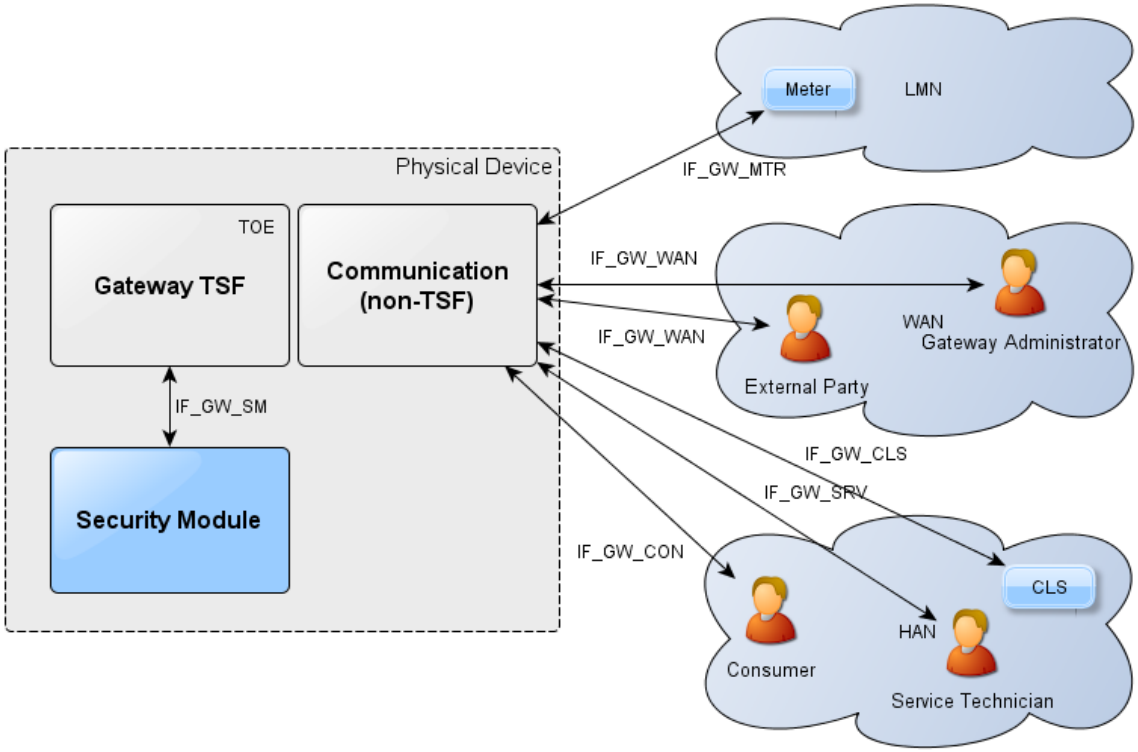


Figure 3: TOE design: A Gateway and multiple Meters

[16] Please note that this refers to the pure communication services excluding encryption functionality.

1.4.5.3 Possible TOE Design: One Box Solution

The components Gateway and Meter may also be realised by a single physical device providing functionality of both. Such a One Box Solution is shown in the following figure. This One Box Solution may be the preferred implementation for one family houses or large houses with several flats where all electricity meters are installed in one single cabinet.

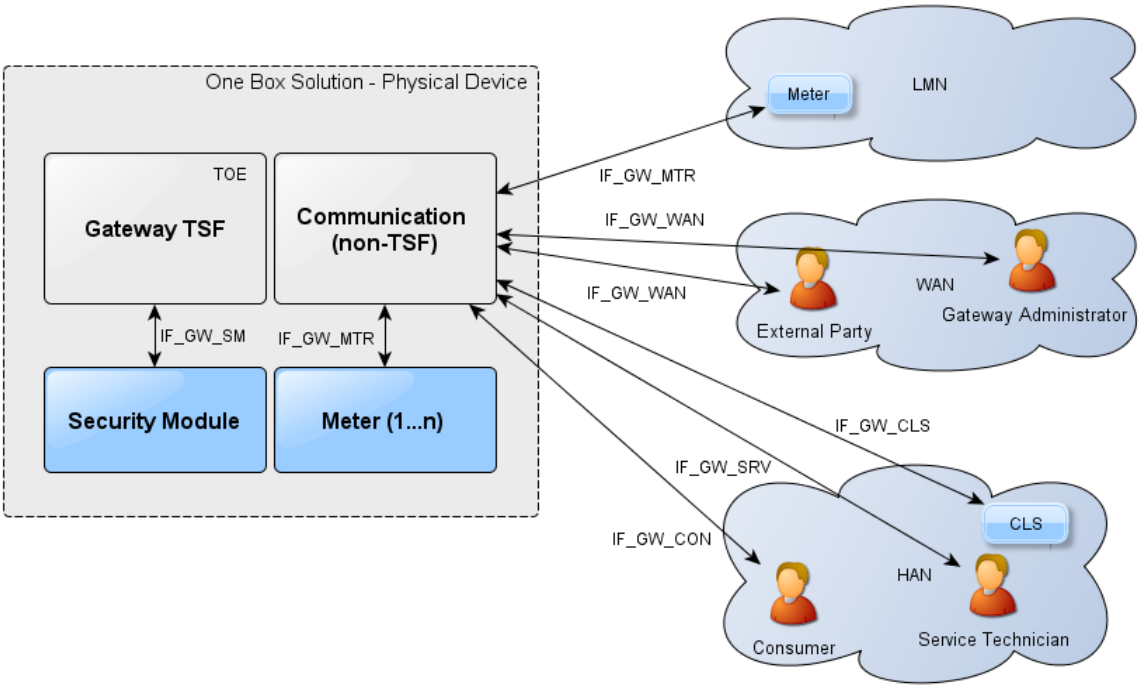


Figure 4: TOE design: One Box Solution

However, also in this case this PP requires the implementation of an external interface for additional meters outside the box that is protected by cryptographic functionality.

1.4.5.4 Possible TOE Design: Gateway with external communication components

The following figure acknowledges that there may be functional aspects in the context of a Gateway that are essential for the overall operation of the Gateway but not required to enforce the security functionality of the Gateway. Those functionalities may also be implemented in form of external components that do not belong to the TOE.

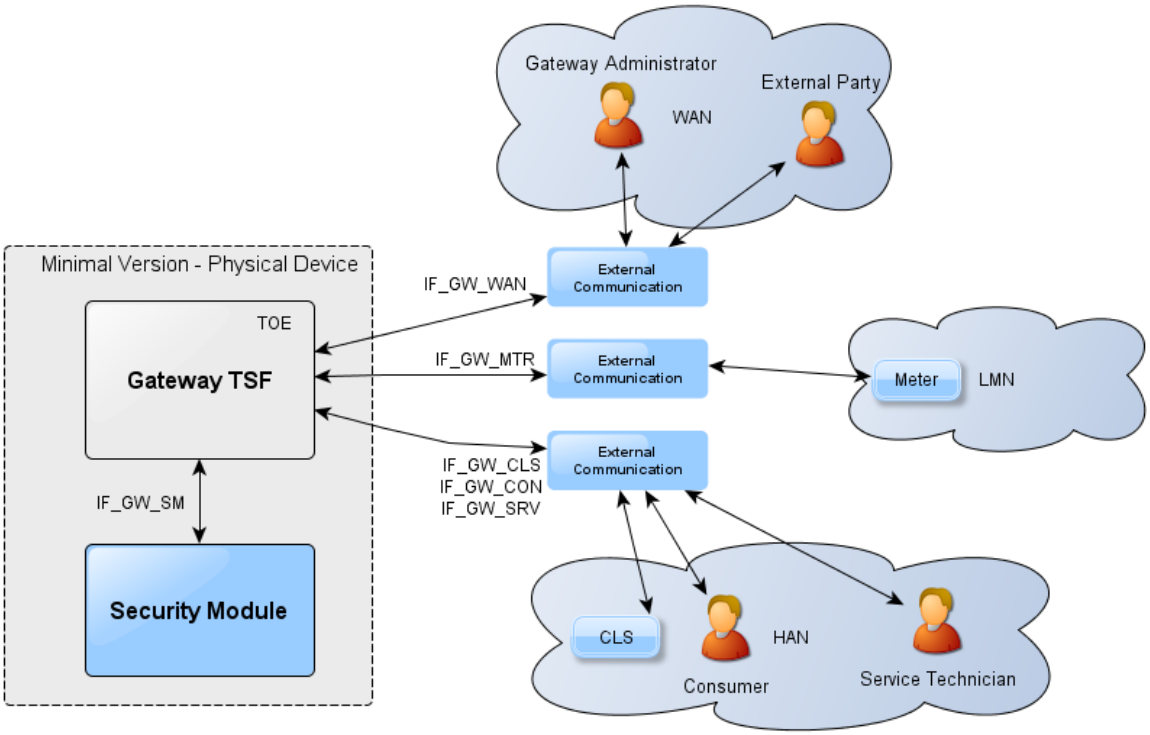


Figure 5: TOE design: Minimal implementation

Classic examples of such functionality are the communication capabilities to the WAN, LMN or HAN. As long as the requirements for separate networks, encryption and so forth are implemented within the Gateway TSF it may be possible to utilise an external communication component. A failure of such a component would of course lead to an inoperative Gateway. However – as the availability of the Gateway is not within the focus of the requirements in this PP – this would not violate any security requirement.

Please note that the requirements around physically separated interfaces for different networks (see also O.SeparateIF) also apply to this configuration as indicated by the multiple arrows between the TOE and its external communication components.

1.4.6 TOE logical boundary

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

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

- **Management** of Security Functionality
- **Identification and Authentication** of TOE users

Please note that it is possible that a Gateway provides more functionality than required by this PP. In those cases however, it is essential that the additional functionality is separated from the evaluated functionality in a way that it cannot impact the security functionality.

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

1.4.6.1 Handling of Meter Data[17]

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

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

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

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

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

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

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

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

These functionalities shall

- prevent that the Gateway accepts data from or sends data to unauthorised entities,
- ensure that only the minimum amount of data leaves the scope of control of the consumer[18],
- preserve the integrity of billing processes and as such serve in the interests of the consumer as well as in the interests of the supplier. Both parties are interested in an billing process that ensures that the value of the consumed amount of a certain commodity (and only the used amount) is transmitted[19],
- preserve the integrity of the system components and their configurations.

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

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

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

The TOE offers a local interface to the consumer (see also IF_GW_CON in Figure 2) and allows the consumer to obtain information via this interface. This information comprises the billing-relevant data (to allow the consumer to verify an invoice) and information about which Meter Data has been and will be sent to which external entity. The TOE ensures that the communication to the consumer is protected (e.g. by using SSL/TLS) and ensures that consumers only get access to their own data. Please note that accessing of this interface by the consumer may happen via different technologies as long as the security requirements are fulfilled. The interface IF_GW_CON may be used by a remote display dedicated to this purpose or may be accessed by standard technologies (e.g. via a PC-based web browser)[20].

1.4.6.2 Confidentiality protection

The TOE protects data from unauthorised disclosure

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

Furthermore, all data, which no longer have to be stored in the Gateway, are securely erased to prevent any form of access to residual data via external interfaces of the TOE.

These functionalities shall protect the privacy of the consumer and shall prevent that an unauthorised party is able to disclose any of the data transferred in and from the Smart Metering System (e.g. Meter Data, configuration settings).

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

1.4.6.3 Integrity and Authenticity protection

The Gateway shall provide the following authenticity and integrity protection:

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

These functionalities shall:

- prevent within the Smart Metering System that data may be sent by a non-authentic component without the possibility that the data recipient can detect this,
- facilitate the integrity of billing processes and serve for the interests of the consumer as well as for the interest of the supplier. Both parties are interested in the transmission of correct processed Meter Data to be used for billing,
- protect the Smart Metering System and a corresponding large scale Smart Grid infrastructure by preventing that data (e.g. Meter Data, configuration settings, or firmware updates) from forged components (with the aim to cause damage to the Smart Grid) will be accepted in the system.

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

1.4.6.4 Information flow control and firewall

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

- only the Gateway may establish a connection to an external entity in the WAN[21]; specifically connection establishment by an external entity in the WAN or a Meter in the LMN to the WAN is not possible,
- the Gateway can establish connections to devices in the LMN or in the HAN,
- Meters in the LMN are only allowed to establish a connection to the Gateway,
- the Gateway shall offer a wake-up service that allows external entities in the WAN to trigger a connection establishment by the Gateway,
- connections are allowed to pre-configured addresses only,
- only cryptographically-protected (i.e. encrypted, integrity protected and mutually authenticated) connections are possible.[22]

These functionalities shall:

- prevent that the Gateway itself or the components behind the Gateway (i.e. Meters or Controllable Local Systems) can be conquered by a WAN attacker (as defined in section 3.4), that processed data are transmitted to the wrong external entity, and that processed data are transmitted without being confidentiality/authenticity/integrity-protected,
- protect the Smart Metering System and a corresponding large scale infrastructure in two ways: by preventing that conquered components will send forged Meter Data (with the aim to cause damage to the Smart Grid), and by preventing that widely distributed Smart Metering Systems can be abused as a platform for malicious software to attack other systems in the WAN (e.g. a WAN attacker who would be able to install a botnet on components of the Smart Metering System).

The communication flows that are enforced by the Gateway between parties in the HAN, LMN and WAN are summarized in the following table[23]:

Source(1st column) Destination (1st row)	**WAN**	**LMN**	**HAN**
WAN	- (see following list)	No connection establishment allowed	No connection establishment allowed
LMN	No connection establishment allowed	- (see following list)	No connection establishment allowed
HAN	Connection establishment is allowed to trustworthy, pre-configured endpoints and via an encrypted channel only[24]	No connection establishment allowed	- (see following list)

Table 2: Communication flows between devices in different networks

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

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

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

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

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

1. Communications within the **WAN** are not restricted. However, the Gateway is not involved in this communication,
2. No communications between devices in the **LMN** are assumed. Devices in the LMN may only communicate to the Gateway and shall not be connected to any other network,
3. Devices in the **HAN** may communicate with each other. However, the Gateway is not involved in this communication. If devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is assumed to be appropriately protected. It should be noted that for the case that a TOE connects to more than one HAN communications between devices within different HAN via the TOE are only allowed if explicitly configured by a Gateway Administrator.

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

1. The Gateway shall accept the submission of Meter Data from the LMN,
2. the Gateway shall offer a wake-up service at the WAN side as described in chapter 1.4.6.5,
3. the Gateway shall offer a user interface to the HAN that allows CLS or consumers[25] to connect to the Gateway in order to read relevant information.

It shall be noted that this concept deliberately accepts that devices in the LMN or HAN of the consumer cannot directly be contacted from the WAN side. However, the Gateway may implement additional functionality (as long as it does not contradict a SFP from this PP) that sets the Gateway as a broker into the communication between an external authorised entity in the WAN and the CLS. As long as a Gateway has a TLS connection to an external entity (please refer to chapter 1.4.6.5 for details how to reach the Gateway from the WAN) it may be technically possible to negotiate a connection between an external entity and a CLS upon the request of the external entity without violating the information flow policies from this PP.

1.4.6.5 Wake-Up-Service

In order to protect the Gateway and the devices in the LAN against threats from the WAN side the Gateway implements a strict firewall policy and enforces that connections with external entities in the WAN shall only be established by the Gateway itself (e.g. when the Gateway delivers Meter Data or contacts the Gateway Administrator to check for updates)[26].

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 PP allows the Gateway to keep existing connections to external entities open (please refer to [BSI-TR-03109-3] for more details) and to offer a so called wake-up service.

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

1. The Gateway verifies the wake-up packet. This comprises
   a) a check if the header identification is correct,
   b) the recipient is the Gateway,
   c) the wake-up packet has been sent/received within an acceptable period of time in order to prevent replayed messages,
   d) the wake-up message has not been received before,
2. If the wake-up message could <u>not</u> be verified as described in step #1 the message will be dropped/ignored. No further operations will be initiated and no feedback is provided.

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

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

3. If the message could be verified as described in step #1 the signature of the wake-up message will be verified. The Gateway shall use the services of its Security Module for signature verification.
4. If the signature of the wake-up message cannot be verified as described in step #3 the message will be dropped/ignored. No feedback is given to the sending external entity and the wake-up sequence terminates.
5. If the signature of the wake-up message could be verified successfully, the Gateway initiates a connection to a pre-configured external entity; however no feedback is given to the sending external entity.

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

1.4.6.6 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 PP.

This contains two aspects:

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

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

Monitoring of Data Transfers

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

Configuration Reporting

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

Audit Log and Monitoring

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

1.4.6.7 Management of Security Functions

The Gateway provides authorised Gateway Administrators with functionality to manage the behaviour of the security functions and to update the TOE. This Protection Profile defines a minimum set of management functions that must be implemented by each Gateway seeking conformance to this PP.

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

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

546 #### 1.4.6.8 Identification and Authentication

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

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

556 ### 1.4.7 The logical interfaces of the TOE

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

Interface Name	Description
IF_GW_CON	Via this interface the Gateway provides the consumer[27] 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.[28]
IF_GW_SM	The Gateway invokes the services of its Security Module via this interface.
IF_GW_CLS	CLS may use the communication services of the Gateway via this interface. The implementation of at least one interface for CLS is mandatory.
IF_GW_WAN	The Gateway submits information to authorised external entities via this interface.
IF_GW_SRV	Local interface via which the service technician has the possibility to review information that are relevant to maintain the Gateway. Specifically he has read access to the system log only via this interface. He has also the possibility to view non-TSF data via this interface.

560 **Table 3: Mandatory TOE external interfaces**

561 ### 1.4.8 The cryptography of the TOE and its Security Module

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

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

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

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

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

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

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

1.4.8.1 Content data encryption vs. an encrypted channel

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

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

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

This concept of encryption on two layers facilitates use cases in which the external entity that the TOE communicates with is not the final recipient of the Meter Data. In this way it is for example possible that the Gateway Administrator receives Meter Data that they forward to other parties. In such a case the Gateway Administrator is the endpoint of the trusted channel but cannot read the Meter Data.

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

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

The basic information flow for Meter Data is as follows and shown in Figure 6:

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

    Or

    c) If a unidirectional communication is performed between the Meter and the Gateway the Meter Data is encrypted using a symmetric algorithm (according to [BSI-TR-03109-3]) and facilitating a defined data structure to ensure the authenticity and confidentiality.
3. The authenticity and integrity of the Meter Data is verified by the Gateway
4. If (and only if) authenticity and integrity have been verified successfully the Meter Data is further processed by the Gateway according to the rules in the Processing Profile else the cryptographic information flow will be cancelled.
5. The processed Meter Data is encrypted and integrity protected using CMS (according to [BSI-TR-03109-1-I]) for the final recipient of the data[29].
6. The processed Meter Data is signed using the services of the Security Module.
7. The processed and signed Meter Data may be stored for a certain amount of time.
8. The processed Meter Data is finally submitted to an authorised external entity in the WAN via an encrypted and mutually authenticated channel.

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

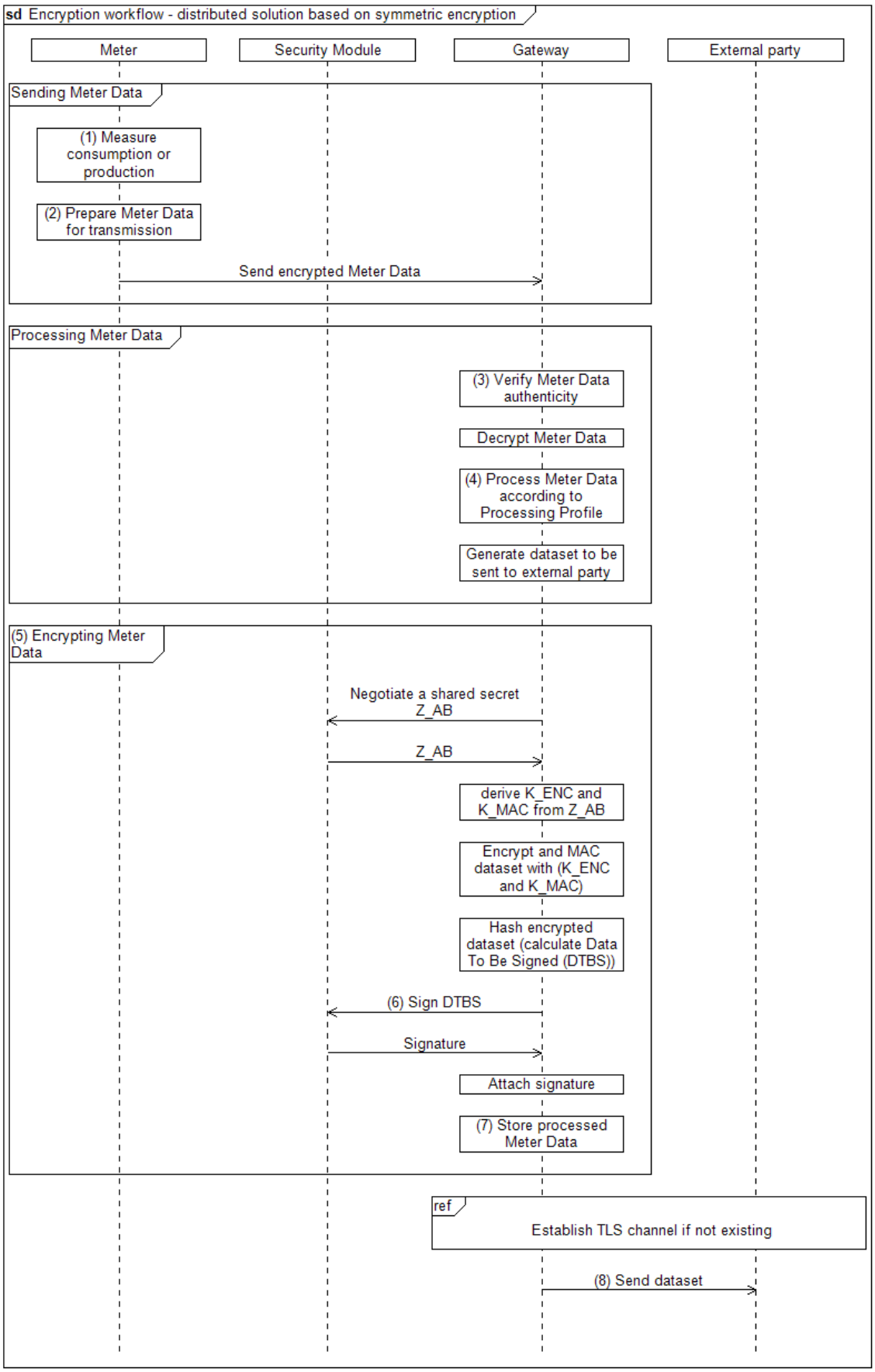


Figure 6: Cryptographic workflow for Meter, Gateway and the Security Module

1.4.9 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 premises (without Security Module)
4. Pre-personalization and integration of Security Module
5. Installation and start of operation
6. Personalization
7. Normal operation

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

For the Protection Profile it is important to know that the certified configuration of the TOE will be established after phase “Personalization”. It has to be ensured that previous phases are performed by trusted personal in secure environments. Since the realization of the phases depend on the concrete TOE it is important that the TOE developer considers and enforces appropriate security measures during the life-cycle phases. The TOE life-cycle will be examined during evaluation of assurance aspect ALC.

2 Conformance Claims

2.1 Conformance statement

This PP requires strict conformance of any PP/ST to this PP.

2.2 CC Conformance Claims

This PP has been developed using Version 3.1 Revision 4 of Common Criteria [CC].

This PP is [CC] part 2 extended due to the use of FPR_CON.1.

This PP claims conformance to [CC] part 3; no extended assurance components have been defined.

2.3 PP Claim

This PP does not claim conformance to any other PP.

2.4 Conformance claim rationale

Since this PP does not claim conformance to any Protection Profile, this section is not applicable.

2.5 Package Claim

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

3 Security Problem Definition

3.1 External entities

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

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

Table 5: Roles used in the Protection profile

3.2 Assets

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

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

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

Asset	Description	Need for Protection
Consumer log data	Log data from the • consumer log.	• Integrity • Confidentiality (only authorised Consumers may read the log data)
Calibration log data	Log data from the • calibration log.	• Integrity • Confidentiality (only authorised SMGW administrators may read the log data)
Consumption Data	Billing-relevant part of Meter Data. Please note that the term Consumption Data implicitly includes Production Data.	• Integrity and authenticity (comparable to the classical meter and its security requirements) • Confidentiality (due to privacy concerns)
Status Data	Grid status data, subset of Meter Data that is not billing-relevant[30].	• Integrity and authenticity (comparable to the classical meter and its security requirements) • Confidentiality (due to privacy concerns)
Supplementary Data	The Gateway may be used for communication purposes by devices in the LMN or HAN. It may be that the functionality of the Gateway that is used by such a device is limited to pure (but secure) communication services. Data that is transmitted via the Gateway but that does not belong to one of the aforementioned data types is named Supplementary Data.	• According to their specific need
Data	The term Data is used as a hypernym for Meter Data and Supplementary Data.	• According to their specific need
Gateway time	Date and time of the real-time clock of the Gateway. Gateway Time is used in Meter Data records sent to external entities.	• Integrity • Authenticity (when time is adjusted to an external reference time)
Personally Identifiable Information (PII)	Personally Identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.	• Confidentiality

661 **Table 6: Assets (User data)**

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

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

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

663 **Table 7: Assets (TSF data)**

664 3.3 Assumptions

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

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

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

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

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

A.Update It is assumed that firmware updates for the Gateway that can be provided by an authorised external entity have undergone a certification process according to this Protection Profile before they are issued and can therefore be assumed to be correctly implemented. It is further assumed that the external entity that is authorised to provide the update is trustworthy and will not introduce any malware into a firmware update.

A.Network It is assumed that

- a WAN network connection with a sufficient reliability and bandwidth for the individual situation is available,
- one or more trustworthy sources for an update of the system time are available in the WAN,
- the Gateway is the only communication gateway for Meters in the LMN[31],
- 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 PP acknowledges that the Gateway cannot be completely protected against unauthorised physical access by its environment. However, it is important for the overall security of the TOE that it is not installed within a public environment.

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

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

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

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

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

Application Note 3: When the ECC key pair generation is done by the SMGW, the ST author has to model this with an appropriate SFR.

3.4 Threats

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

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

- Attackers having physical access to Meter, Gateway, a connection between these components, or local logical access to any of the interfaces (local attacker), trying to disclose or alter assets while stored in the Gateway or while transmitted between meters in the LMN and the Gateway. Please note that the following threat model assumes that the local attacker has less motivation than the WAN attacker as a successful attack of a local attacker will always only impact one Gateway. Please further note that the local attacker includes the authorised individuals like consumers.
- An attacker located in the WAN (WAN attacker) trying to compromise the confidentiality and/or integrity of the processed Meter Data and or configuration data transmitted via the WAN, or attacker trying to conquer a component of the infrastructure (i.e. Meter, Gateway or Controllable Local System) via the WAN to cause damage to a component itself or to the corresponding grid (e.g. by sending forged Meter Data to an external entity).

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

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

In order to achieve the modification, the attacker may also try to modify secondary assets like the firmware or configuration parameters of the Gateway.

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

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

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

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

T.DisclosureWAN	A WAN attacker may try to violate the privacy of the consumer by disclosing Meter Data or configuration data (Meter config, Gateway config or CLS config) or parts of it when transmitted between Gateway and external entities in the WAN.
T.DisclosureLocal	A Local Attacker may try to violate the privacy of the consumer by disclosing Meter Data transmitted between the TOE and the Meter. This threat is of specific importance if Meters of more than one consumer are served by one Gateway.
T.Infrastructure	A WAN attacker may try to obtain control over Gateways, Meters or CLS via the TOE, which enables the WAN Attacker to cause damage to consumers or external entities or the grids used for commodity distribution (e.g. by sending wrong data to an external entity). A WAN attacker may also try to conquer a CLS in the HAN first in order to logically attack the TOE from the HAN side.
T.ResidualData	By physical and/or logical means a local attacker or a WAN attacker may try to read out data from the Gateway, which travelled through the Gateway before and which are no longer needed by the Gateway (i.e. Meter Data, Meter config, or CLS config).
T.ResidentData	A WAN or local attacker may try to access (i.e. read, alter, delete) information to which they don't have permission to while the information is stored in the TOE. While the WAN attacker only uses the logical interface of the TOE that is provided into the WAN the local attacker may also physically access the TOE.
T.Privacy	A WAN attacker may try to obtain more detailed information from the Gateway than actually required to fulfil the tasks defined by its role or the contract with the consumer. This includes scenarios in which an external entity that is primarily authorised to obtain information from the TOE tries to obtain more information than the information that has been authorised as well as scenarios in which an attacker who is not authorised at all tries to obtain information.

690 3.5 Organizational Security Policies (OSPs)

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

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

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

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

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

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

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

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

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

Application Note 4: When the RNG functionality is provided by the Gateway itself, it has to be appropriately modelled by the ST author using SFR FCS_RNG according to [AIS20] or [AIS31] and considering [BSI-TR-03109-3].

692 # 4 Security Objectives

693 ## 4.1 Security Objectives for the TOE

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

The firewall:

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

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

Application Note 5: 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.[32]

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

This includes that:

- the TOE shall ensure that the communication to the Meter(s) is established in an Gateway Administrator-definable interval or an interval as defined by the Meter,
- the TOE shall enforce encryption and integrity protection for the communication with the Meter[33],
- the TOE shall verify the integrity and authenticity of the data received from a Meter before handling it further,

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

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

- the TOE shall process the data according to the definition in the corresponding Processing Profile,
- the TOE shall encrypt the processed Meter Data for the final recipient, sign the data and
- deliver the encrypted data to authorised external entities as defined in the corresponding Processing Profiles facilitating an encrypted channel,
- the TOE shall store processed Meter Data if an external entity cannot be reached and re-try to send the data until a configurable number of unsuccessful retries has been reached,
- the TOE shall pseudonymise the data for parties that do not need the relation between the processed Meter Data and the identity of the consumer.

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[34].

In addition the TOE shall generate the required keys utilising the services of its Security Module[35], ensure that the keys are only used for an acceptable amount of time and destroy ephemeral[36] keys if not longer needed.

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

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

[35] Please refer to chapter 1.4.8 for an overview on how the cryptographic functions are distributed between the TOE and its Security Module.

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

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

Specifically, the TOE shall

- encrypt its TSF and user data as long as it is not in use,
- overwrite any information that is no longer needed to ensure that it is no longer available via the external interfaces of the TOE[36],
- monitor user data and the TOE firmware for integrity errors,
- contain a test that detects whether the interfaces for WAN and LAN are separate,
- have a fail-safe design that specifically ensures that no malfunction can impact the delivery of a commodity (e.g. energy, gas, heat or water)[37],
- make any physical manipulation within the scope of the intended environment detectable for the consumer and Gateway Administrator.

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

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

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

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

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

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

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

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

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

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

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

For the consumer log the TOE shall ensure that a sufficient amount of events is available (in order to allow a consumer to verify an 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[38]. Access control shall depend on the destination interface that is used to send that information.

694 4.2 Security objectives for the operational environment

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

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

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

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

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

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

The Security Module used shall be certified according to [SecMod-PP]

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

and shall be used in accordance with its relevant guidance documentation.

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

OE.Network It shall be ensured that

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

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

695 ## 4.3 Security Objectives rationale

696 ### 4.3.1 Overview

697 The following table gives an overview how the assumptions, threats, and organisational security
698 policies are addressed by the security objectives. The text of the following sections justifies this more
699 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

700 **Table 8: Rationale for Security Objectives**

701 ### 4.3.2 Countering the threats

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

4.3.2.1 General objectives

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

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

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

4.3.2.2 T.DataModificationLocal

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

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

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

4.3.2.3 T.DataModificationWAN

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

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

4.3.2.4 T.TimeModification

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

O.Time defines that the TOE needs a reliable time stamp mechanism that is also updated from reliable sources regularly in the WAN. **O.Crypt** defines the required cryptographic functionality for the communication to external entities in the WAN. Therewith, **O.Time** and **O.Crypt** are the core objective to counter the threat **T.TimeModification**.

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

4.3.2.5 T.DisclosureWAN

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

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

O.Conceal ensures that no information can be disclosed based on additional characteristics of the communication like frequency, load or the absence of a communication.

4.3.2.6 T.DisclosureLocal

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

O.Meter defines that the TOE will enforce the encryption and integrity protection of communication when polling or receiving Meter Data from the Meter. **O.Crypt** defines the required cryptographic

functionality. Both objectives together ensure that the communication between the Meter and the TOE cannot be disclosed.

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

4.3.2.7 T.Infrastructure

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

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

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

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

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

4.3.2.8 T.ResidualData

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

4.3.2.9 T.ResidentData

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

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

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

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

4.3.2.10 T.Privacy

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

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

4.3.3 Coverage of organisational security policies

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

4.3.3.1 OSP.SM

The Organizational Security Policy **OSP.SM** that mandates that the TOE utilises the services of a certified Security Module is directly addressed by the security objectives **OE.SM** and **O.Crypt**. The

objective **OE.SM** addresses the functions that the Security Module shall be utilised for as defined in **OSP.SM** and also requires a certified Security Module. **O.Crypt** defines the cryptographic functionalities for the TOE itself. In this context it has to be ensured that the Security Module is operated in accordance with its guidance documentation.

4.3.3.2 OSP.Log

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

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

4.3.4 Coverage of assumptions

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

4.3.4.1 A.ExternalPrivacy

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

4.3.4.2 A.TrustedAdmins

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

4.3.4.3 A.PhysicalProtection

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

4.3.4.4 A.ProcessProfile

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

4.3.4.5 A.Update

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

4.3.4.6 A.Network

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

4.3.4.7 A.Keygen

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

841 5 Extended Component definition

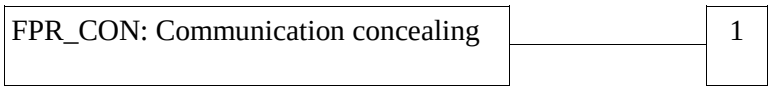
842 5.1 Communication concealing (FPR_CON)

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

847 5.2 Family behaviour

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

852 5.3 Component levelling



853 5.4 Management

854 The following actions could be considered for the management functions in FMT:

855 a) Definition of the interval in FPR_CON.1.2 if definable within the operational phase of the
856 TOE.

857 5.5 Audit

858 There are no auditable events foreseen.

859 5.6 Communication concealing (FPR_CON.1)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPR_CON.1.1	**The TSF shall enforce the [assignment: *information flow policy*] in order to ensure that no personally identifiable information (PII) can be obtained by an analysis of [assignment: *characteristics of the information flow that need to be concealed*].**
FPR_CON.1.2	**The TSF shall connect to [assignment: *list of external entities*] in intervals as follows [selection: *weekly, daily, hourly, [assignment: other interval]*] to conceal the data flow.**

6 Security Requirements

6.1 Overview

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

The following notations are used:

- **Refinement** operation (denoted by **bold text**): is used to add details to a requirement, and thus further restricts a requirement. In case that a word has been deleted from the original text this refinement is indicated by ~~**crossed out bold**~~ text
- **Selection** operation (denoted by underlined text): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicised text)*: is used to assign a specific value to an unspecified parameter, such as the length of a password.
- **Iteration** operation: are identified with a suffix in the name of the SFR (e.g. FDP_IFC.2/FW).

It should be noted that the requirements in the following chapters are not necessarily be ordered alphabetically. Where useful the requirements have been grouped.

The following table summarises all TOE security functional requirements of this PP:

Class FAU: Security Audit	
FAU_ARP.1/SYS	Security alarms for system log
FAU_GEN.1/SYS	Audit data generation for system log
FAU_SAA.1/SYS	Potential violation analysis for system log
FAU_SAR.1/SYS	Audit review for system log
FAU_STG.4/SYS	Prevention of audit data loss for the system log
FAU_GEN.1/CON	Audit data generation for consumer log
FAU_SAR.1/CON	Audit review for consumer log
FAU_STG.4/CON	Prevention of audit data loss for the consumer log
FAU_GEN.1/CAL	Audit data generation for calibration log
FAU_SAR.1/CAL	Audit review for calibration log
FAU_STG.4/CAL	Prevention of audit data loss for the calibration log
FAU_GEN.2	User identity association
FAU_STG.2	Guarantees of audit data availability
Class FCO: Communication	
FCO_NRO.2	Enforced proof of origin
Class FCS: Cryptographic Support	
FCS_CKM.1/TLS	Cryptographic key generation for TLS
FCS_COP.1/TLS	Cryptographic operation for TLS

FCS_CKM.1/CMS	Cryptographic key generation for CMS
FCS_COP.1/CMS	Cryptographic operation for CMS
FCS_CKM.1/MTR	Cryptographic key generation for Meter communication encryption
FCS_COP.1/MTR	Cryptographic operation for Meter communication encryption
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/HASH	Cryptographic operation for Signatures
FCS_COP.1/MEM	Cryptographic operation for TSF and user data encryption
Class FDP: User Data Protection	
FDP_ACC.2	Complete Access Control
FDP_ACF.1	Security attribute based access control
FDP_IFC.2/FW	Complete information flow control for firewall
FDP_IFF.1/FW	Simple security attributes for Firewall
FDP_IFC.2/MTR	Complete information flow control for Meter information flow
FDP_IFF.1/MTR	Simple security attributes for Meter information
FDP_RIP.2	Full residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
Class FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_AFL.1	Authentication failure handling
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.6	Re-Authenticating
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behaviour
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_MSA.1/AC	Management of security attributes for Gateway access policy
FMT_MSA.3/AC	Static attribute initialisation for Gateway access policy
FMT_MSA.1/FW	Management of security attributes for firewall policy
FMT_MSA.3/FW	Static attribute initialisation for Firewall policy

FMT_MSA.1/MTR	Management of security attributes for Meter policy
FMT_MSA.3/MTR	Static attribute initialisation for Meter policy
Class FPR: Privacy	
FPR_CON.1	Communication Concealing
FPR_PSE.1	Pseudonymity
Class FPT: Protection of the TSF	
FPT_FLS.1	Failure with preservation of secure state
FPT_RPL.1	Replay Detection
FPT_STM.1	Reliable time stamps
FPT_TST.1	TSF testing
FPT_PHP.1	Passive detection of physical attack
Class FTP: Trusted path/channels	
FTP_ITC.1/WAN	Inter-TSF trusted channel for WAN
FTP_ITC.1/MTR	Inter-TSF trusted channel for Meter
FTP_ITC.1/USR	Inter-TSF trusted channel for User

877 **Table 9: List of Security Functional Requirements**

878 ## 6.2 Class FAU: Security Audit

879 ### 6.2.1 Introduction

880 A TOE compliant to this Protection Profile shall implement three different audit logs as defined in
881 OSP.Log and O.Log. The following table provides an overview over the three audit logs before the
882 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 functionaltity • 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

	System-Log	Consumer-Log	Calibration-Log
Data	• As defined by CC part 2 • Augmented by specific events for the security functions	• Information about all information flows to the WAN • Information about the current and the previous Processing Profiles • Non-billing-relevant Meter Data • Information about the system status (including relevant errors) • Billing-relevant data needed to verify an invoice	• Calibration relevant data only
Access	• Access by authorised Gateway Administrator and via IF_GW_WAN only • Events may only be deleted by an authorised Gateway Administrator via IF_GW_WAN • Read access by authorised service technician via IF_GW_SRV only	• Read access by authorised consumer and via IF_GW_CON only to the data related to the current consumer	• Read access by authorised Gateway Administrator and via IF_GW_WAN only
Deletion	• Ring buffer. • The availability of data has to be ensured for a sufficient amount of time • Overwriting old events is possible if the memory is full	• Ring buffer. • The availability of data has to be ensured for a sufficient amount of time • Overwriting old events is possible if the memory is full • Retention period is set by authorised Gateway Administrator on request by consumer, data older than this are deleted.	• The availability of data has to be ensured over the lifetime of the TOE.

883 **Table 10: Overview over audit processes**

884 ## 6.2.2 Security Requirements for the System Log

885 ### 6.2.2.1 Security audit automatic response (FAU_ARP)

886 #### 6.2.2.1.1 FAU_ARP.1/SYS: Security Alarms for system log

FAU_ARP.1.1/SYS	The TSF shall ~~**take**~~ *[inform an authorised Gateway Administrator and [assignment: list of actions]*] upon detection of a potential security violation.
Hierarchical to:	No other components
Dependencies:	FAU_SAA.1 Potential violation analysis

887 ### 6.2.2.2 Security audit data generation (FAU_GEN)

888 #### 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) [assignment*: **other non-privacy relevant auditable events***].
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, [assignment*: other audit relevant information*].
Hierarchical to:	No other components
Dependencies:	FPT_STM.1

889 ### 6.2.2.3 Security audit analysis (FAU_SAA)

890 #### 6.2.2.3.1 FAU_SAA.1/SYS: Potential violation analysis for system log

FAU_SAA.1.1/SYS	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2/SYS	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [assignment: *subset of defined auditable events]* known to indicate a potential security violation; b) [assignment*: any other rules*].
Hierarchical to:	No other components
Dependencies:	FAU_GEN.1

Application Note 6: The specific events that shall be analysed in the system audit log in order to ensure a correct operation of the TOE highly depend on the specific implementation and application of the TOE; as such the authors of the ST will have to complete the operations in FAU_SAA.1/SYS.

At least all types of failures in the TSF as listed in FPT_FLS.1 should be recognised as potential violation by the TOE.

891 **6.2.2.4 Security audit review (FAU_SAR)**

892 **6.2.2.4.1 FAU_SAR.1/SYS: Audit Review for system log**

FAU_SAR.1.1/SYS	The TSF shall provide [*only authorised Gateway Administrators via the IF_GW_WAN interface and authorised Service Technicians via the IF_GW_SRV interface*] with the capability to read [*all information*] from the **system** audit records.
FAU_SAR.1.2/SYS	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Hierarchical to:	No other components
Dependencies:	FAU_GEN.1

893 **6.2.2.5 Security audit event storage (FAU_STG)**

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

895 **6.2.3 Security Requirements for the Consumer Log**

896 **6.2.3.1 Security audit data generation (FAU_GEN)**

897 **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 11 and [assignment: additional events or none]*].
FAU_GEN.1.2/CON	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*additional information as*

listed in Table 11 and [assignment: additional events or 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 shall 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.

Further, the ST author shall consider the descriptions in chapter 1.4.6.6 to decide whether additional information needs to be audited for a specific TOE.

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

Table 11: Events for consumer log

6.2.3.2 Security audit review (FAU_SAR)

6.2.3.2.1 FAU_SAR.1/CON Audit Review for consumer log

FAU_SAR.1.1/CON The TSF shall provide [*only authorised consumer via the IF_GW_CON interface*] 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 shall ensure that the consumer is able to interpret the information that is provided to him in a way that allows him to verify the invoice.

901 **6.2.3.3 Security audit event storage (FAU_STG)**

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

903 **6.2.4 Security Requirements for the Calibration Log**

904 **6.2.4.1 Security audit data generation (FAU_GEN)**

905 **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) [assignment: *all calibration-relevant information*].
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, [assignment: *other audit relevant information*].
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 are left open to the ST author. The ST author shall seek the guidance of the relevant national authority before deciding about those requirements.

906 **6.2.4.2 Security audit review (FAU_SAR)**

907 **6.2.4.2.1 FAU_SAR.1/CAL: Audit Review for the calibration log**

FAU_SAR.1.1/CAL	The TSF shall provide [*only authorised Gateway Administrators via the IF_GW_WAN interface*] with the capability to read [*all information*] from the **calibration** audit records.
FAU_SAR.1.2/CAL	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Hierarchical to:	No other components

Dependencies:	FAU_GEN.1

908 **6.2.4.3 Security audit event storage (FAU_STG)**

909 **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 Administrato*r] 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. The developer shall consider choosing a sufficient size so that the calibration log cannot become full.

910 **6.2.5 Security Requirements that apply to all logs**

911 **6.2.5.1 Security audit data generation (FAU_GEN)**

912 **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.

913 **6.2.5.2 Security audit event storage (FAU_STG)**

914 **6.2.5.2.1 FAU_STG.2: Guarantees of audit data availability**

FAU_STG.2.1	The TSF shall protect the stored audit records in ~~**the**~~ **all** audit trail**s** from unauthorised deletion.
FAU_STG.2.2	The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in ~~**the**~~ **all** audit trail**s**.
FAU_STG.2.3	The TSF shall ensure that [*assignment: metric for saving audit records*] stored audit records will be maintained when the following conditions occur: [audit storage exhaustion or failure].
Hierarchical to:	FAU_STG.1 Protected audit trail storage
Dependencies:	FAU_GEN.1 Audit data generation
Application Note 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 shall consider 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*[39]] of the originator of the information, and the [*signature*] of the information to which the evidence applies.
FCO_NRO.2.3	The TSF shall provide a capability to verify the evidence of origin of information to [recipient, *[consumer]*] given [*limitations of the digital signature according to BSI TR-03109-1*].
Hierarchical to:	FCO_NRO.1 Selective proof of origin
Dependencies:	FIA_UID.1 Timing of identification

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

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

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 [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], fulfilled by FCS_COP.1/TLS FCS_CKM.4 Cryptographic key destruction

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

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

Application Note 18: The TOE *shall only* use cryptographic specifications and algorithms as described in [BSI-TR-03109-3].

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

6.4.1.2 Cryptographic operation (FCS_COP)

6.4.1.2.1 FCS_COP.1/TLS: Cryptographic operation for TLS

FCS_COP.1.1/TLS	The TSF shall perform [*TLS encryption, decryption, and integrity protection*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], fulfilled by FCS_CKM.1/TLS FCS_CKM.4 Cryptographic key destruction

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

Application Note 21: Based on [BSI-TR-03109-3] the ST author shall exactly reference 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 [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], fulfilled by FCS_COP.1/CMS FCS_CKM.4 Cryptographic key destruction

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

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

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

927 #### 6.4.2.2 Cryptographic operation (FCS_COP)

928 ##### 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 [assignment*: cryptographic algorithm*] and cryptographic key sizes [assignment*: cryptographic key sizes*] that meet the following: [assignment: *list of standards*].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], fulfilled by FCS_CKM.1/CMS FCS_CKM.4 Cryptographic key destruction

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

Application Note 26: Based on [BSI-TR-03109-3] and [BSI-TR-03109-1-I] the ST author shall exactly reference the applied cryptographic algorithm for CMS.

929 ### 6.4.3 Cryptographic support for Meter communication encryption

930 #### 6.4.3.1 Cryptographic key management (FCS_CKM)

931 ##### 6.4.3.1.1 FCS_CKM.1/MTR: Cryptographic key generation for Meter communication
932 (symmetric encryption)

FCS_CKM.1.1/MTR	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], fulfilled by FCS_COP.1/MTR FCS_CKM.4 Cryptographic key destruction

Application Note 27: Based on [BSI-TR-03109-3] the ST author shall exactly reference the applied cryptographic key generation algorithm for Meter communication encryption.

Application Note 28: The TOE *shall only* use cryptographic specifications and algorithms as described in [BSI-TR-03109-3].

933 **6.4.3.2 Cryptographic operation (FCS_COP)**

934 **6.4.3.2.1 FCS_COP.1/MTR: Cryptographic operation for Meter communication encryption**

FCS_COP.1.1/MTR	The TSF shall perform [*symmetric encryption, decryption, integrity protection*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], fulfilled by FCS_CKM.1/MTR FCS_CKM.4 Cryptographic key destruction

Application Note 29: The PP allows different scenarios of key generation for Meter communication encryption. Those are**:**

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

Application Note 30: If the connection between the Meter and TOE is unidirectional, the communication between the Meter and the TOE shall be secured by the use of a symmetric AES encryption. If a bidirectional connection between the Meter and the TOE is established, the communication shall be secured by a TLS channel as described in chapter 6.4.1. As the TOE shall be interoperable with all kind of Meters it requires the implementation of both kinds of encryption.

Application Note 31: Based on [BSI-TR-03109-3] the ST author shall exactly reference the applied cryptographic algorithm.

Application Note 32: The TOE *shall only* use cryptographic specifications and algorithms as described in [BSI-TR-03109-3].

935 ### 6.4.4 General Cryptographic support

936 #### 6.4.4.1 Cryptographic key management (FCS_CKM)

937 ##### 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 [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], fulfilled by FCS_CKM.1/TLS and FCS_CKM.1/CMS and FCS_CKM.1/MTR

Application Note 33: Please note that as against the requirement FDP_RIP.2 the mechanisms implementing the requirement from FCS_CKM.4 shall be suitable to avoid attackers with physical access to the TOE from accessing the keys after they are no longer used.

938 #### 6.4.4.2 Cryptographic operation (FCS_COP)

939 ##### 6.4.4.2.1 FCS_COP.1/HASH: Cryptographic operation, hashing for signatures

FCS_COP.1.1/HASH	The TSF shall perform [*hashing for signature creation and verification*] in accordance with a specified cryptographic algorithm [assignment*: cryptographic algorithm*] and cryptographic key sizes [*none*] that meet the following: [assignment: *list of standards*]
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[40]] FCS_CKM.4 Cryptographic key destruction

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

Application Note 35: The TOE *shall only* use cryptographic specifications and algorithms as described in [BSI-TR-03109-3].

Application Note 36: Based on [BSI-TR-03109-3] the ST author shall exactly reference the applied cryptographic algorithm.

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

940 **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 [assignment*: cryptographic algorithm*] and cryptographic key sizes [assignment*: cryptographic key sizes*] that meet the following: [assignment: *list of standards*]
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], fulfilled by FCS_CKM.1/CMS FCS_CKM.4 Cryptographic key destruction
Application Note 37:	Please note that the key generation functionality as defined by FCS_CKM.1/CMS can be used for this functionality as well.
Application Note 38:	The TOE shall encrypt its local TSF and user data while it is not in use (i.e. while stored in a persistent memory). The exact approach to handle the key that is used for this functionality is left to the ST author. However, the ST author is motivated to consider the use of the build in Security Module to store the symmetric key that is used for the encryption of TSF and user data. It shall be noted that this kind of encryption cannot provide an absolute protection against physical manipulation and does not aim to. It however contributes to the security concept that considers the protection that is provided by the environment.
Application Note 39:	[BSI-TR-02102] should be considered when a cryptographic algorithm is chosen.

941 # 6.5 Class FDP: User Data Protection

942 ## 6.5.1 Introduction to the Security Functional Policies

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

946 • The Gateway access SFP is an access control policy to control the access to objects under the
947 control of the TOE. The details of this access control policy highly depend on the concrete
948 application of the TOE. The access control policy is described in more detail in [BSI-TR-
949 03109-1].

950 • The Firewall SFP implements an information flow policy to fulfil the objective O.Firewall. All
951 requirements around the communication control that the TOE poses on communications
952 between the different networks are defined in this policy.

953 • The Meter SFP implements an information flow policy to fulfil the objective O.Meter. It
954 defines all requirements concerning how the TOE shall handle Meter Data.

955 ## 6.5.2 Gateway Access SFP

956 ### 6.5.2.1 Access control policy (FDP_ACC)

957 **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

958 **6.5.2.1.2 FDP_ACF.1 Security attribute based access control**

FDP_ACF.1.1	The TSF shall enforce the [*Gateway access SFP*] to objects based on the following: [*subjects: external entities on the WAN, HAN or LMN side* *objects: any information that is sent to, from or via the TOE* *attributes: destination interface*].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [• *an authorised Consumer is only allowed to have read access to his own User Data via the interface IF_GW_CON,* • *an authorised Service Technician is only allowed to have read access to the system log via the interface IF_GW_SRV, the service technician must not be allowed to read, modify or delete any other TSF data,* • *an authorised Gateway Administrator is allowed to interact with the TOE only via IF_GW_WAN,* • *only authorised Gateway Administrators are allowed to establish a wake-up call,* • *[*assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects or none]*].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes that explicitly authorise access of subjects to objects*].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [• *the Gateway Administrator is not allowed to read consumption data or the Consumer Log,* • *nobody must be allowed to read the symmetric keys used for encryption*].
Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Application Note 40:	The ST author shall consider the regulations from [BSI-TR-03109-1] for additional rules regarding the Gateway access SFP.

959 ### 6.5.3 Firewall SFP

960 #### 6.5.3.1 Information flow control policy (FDP_IFC)

961 ##### 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

962 #### 6.5.3.2 Information flow control functions (FDP_IFF)

963 ##### 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: [s*ubjects: 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*].
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* *[assignment: other rules or none]* *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: [assignment: *rules, based on security attributes that explicitly deny information flows*].
Hierarchical to:	No other components

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

Application Note 41: 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 42: The assignment in FDP_IFF.1.2/FW may be 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 shall not accept any connections from the WAN side.

964 ### 6.5.4 Meter SFP

965 #### 6.5.4.1 Information flow control policy (FDP_IFC)

966 ##### 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

967 #### 6.5.4.2 Information flow control functions (FDP_IFF)

968 ##### 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: [s*ubjects: TOE, external entities in WAN, Meters located in LMN* *information: any information that is sent via the TOE* *attributes: destination interface, source interface (LMN or WAN), Processing Profile*].
FDP_IFF.1.2/MTR	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [• *an information flow shall only be initiated if allowed by a corresponding Processing Profile*].

FDP_IFF.1.3/MTR The TSF shall enforce the [*following rules:*

- *Data received from Meters shall be processed as defined in the corresponding Processing Profile,*
- *Results of processing of Meter Data shall be submitted to external entities as defined in the Processing Profiles,*
- *The internal system time shall be synchronised as follows:*
  - *The TOE shall compare the system time to a reliable external time source [assignment: synchronization interval between 1 minute and 24 hours]*.
  - *If the deviation between the local time and the remote time is acceptable*[41] *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*[42] *and*
    - *inform a Gateway Administrator*].

FDP_IFF.1.4/MTR The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes that explicitly authorise information flows*].

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

Reliability of external source

There are several ways to achieve the reliability of the external source. On the one hand there may be a source in the WAN that has an acceptable reliability on its own (e.g. because it is operated by a very trustworthy organisation (an official legal time issued by the calibration authority would be a good example for such a source[43])). On the other hand a developer may choose to maintain multiple external sources that all have a certain level of reliability but no absolute reliability. When using such sources the TOE shall contact more than one source and harmonize the results in order to ensure that no attack happened.

Acceptable deviation

For the question whether a deviation between the time source(s) in the WAN and the local system time is still acceptable, normative or legislative

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

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

[43] By the time that this PP is developed however, this time source is not yet available

regulations shall be considered. If no regulation exists, a maximum deviation of 3% of the measuring period is allowed to be in conformance with this Protection Profile. It should be noted that depending on the kind of application a more accurate system time is needed. But this aspect is not within the scope of this Protection Profile.

Please further note that – depending on the exactness of the local clock – it may be required to synchronize the time more often than every 24 hours.

Application Note 44: In FDP_IFF.1.5/MTR the TOE is required to verify the authenticity, integrity and confidentiality of the Meter Data received from the Meter. The TOE has two options to do so:

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

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

969 ## 6.5.5 General Requirements on user data protection

970 ### 6.5.5.1 Residual information protection (FDP_RIP)

971 #### 6.5.5.1.1 FDP_RIP.2: Full residual information protection

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

Application Note 45: Please refer to chapter F.9 of part 2 of [CC] for more detailed information about what kind of information this requirement applies to.

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

972 ### 6.5.5.2 Stored data integrity (FDP_SDI)

973 #### 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 [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [*assignment: action to be taken*].
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring

Dependencies:	No dependencies.
Application Note 46:	This Protection Profile defines that the TOE shall be capable of detecting integrity errors on all objects. However, the definition of real attributes (e.g. hash values) that are used to implement this functionality are left to the ST author. The developer should further consider the use of the built-in Security Module as an anchor of trust for this functionality.

974 # 6.6 Class FIA: Identification and Authentication

975 ## 6.6.1 User Attribute Definition (FIA_ATD)

976 ### 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*
- *[assignment: list of security attributes or none]*].

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

977 ## 6.6.2 Authentication Failure handling (FIA_AFL)

978 ### 6.6.2.1 FIA_AFL.1: User authentication before any action

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [assignment: *list of actions*].

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

979 ## 6.6.3 User Authentication (FIA_UAU)

980 ### 6.6.3.1 FIA_UAU.2: User authentication before any action

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

Hierarchical to:	FIA_UAU.1
Dependencies:	FIA_UID.1 Timing of identification
Application Note 47:	Please refer to [BSI-TR-03109-1] for a more detailed overview on the authentication of the TOE users.

981 **6.6.3.2 FIA_UAU.5: Multiple authentication mechanisms**

FIA_UAU.5.1 The TSF shall provide [

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

] to support user authentication.

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

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

].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 48: Please refer to [BSI-TR-03109-1] for a more detailed overview on the authentication of the TOE users.

982 **6.6.3.3 FIA_UAU.6: Re-authenticating**

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

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

].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 49: This requirement on re-authentication for external entities in the WAN and LMN is addressed by disconnecting the TLS channel even though a re-authentication is – strictly speaking - only achieved if the TLS channel is build up again.

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: [assignment: *rules for the initial association of attributes*].
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: [assignment: *rules for the changing of attributes*].
Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition

6.7 Class FMT: Security Management

6.7.1 Management of the TSF

6.7.1.1 Management of functions in TSF

6.7.1.1.1 FMT_MOF.1: Management of security functions behaviour

FMT_MOF.1.1	The TSF shall restrict the ability to [modify the behaviour of] the functions [*for management as defined in FMT_SMF.1*] to [*roles and criteria as defined in Table 12*].
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

Function	Limitation
Display the version number of the TOE Display the current time	The management functions must only be accessible for an authorised consumer and only via the interface IF_GW_CON.

All other management functions as defined in FMT_SMF.1	The management functions must only be accessible for an authorised Gateway Administrator and only via the interface IF_GW_WAN[44].
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.

991 **Table 12: Restrictions on Management Functions**

992 **6.7.1.2 Specification of Management Functions (FMT_SMF)**

993 **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 13 and Table 14 and [assignment: additional functionalities]*].

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	- [45]
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	- [46]
FAU_GEN.2	-

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

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

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

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 authorised units for communication (pairing). • Management of endpoint to be contacted after successful wake-up call. • Management of CLS systems.
FDP_IFC.2/MTR	-
FDP_IFF.1/MTR	• Managing the attributes (including Processing Profiles) used to make explicit access based decisions.
FDP_RIP.2	-
FDP_SDI.2	• The actions to be taken upon the detection of an integrity error shall be configurable.
FIA_ATD.1	• If so indicated in the assignment, the authorised Gateway Administrator might be able to define additional security attributes for users.
FIA_AFL.1	• Management of the threshold for unsuccessful authentication attempts; • Management of actions to be taken in the event of an authentication failure.
FIA_UAU.2	• Management of the authentication data by an Gateway

	Administrator;
FIA_UAU.5	- [47]
FIA_UAU.6	- [48]
FIA_UID.2	• The management of the user identities.
FIA_USB.1	• An authorised Gateway Administrator can define default subject security attributes, if so indicated in the assignment of FIA_ATD.1. • An authorised Gateway Administrator can change subject security attributes, if so indicated in the assignment of FIA_ATD.1.
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.[49]
FMT_MSA.3/AC	- [50]
FMT_MSA.1/FW	• Management of rules by which security attributes inherit specified values.[51]
FMT_MSA.3/FW	- [52]
FMT_MSA.1/MTR	• Management of rules by which security attributes inherit specified values.[53]
FMT_MSA.3/MTR	- [54]
FPR_CON.1	• Definition of the interval in FAU_CON.1.2 if definable within the operational phase of the TOE
FPR_PSE.1	-
FPT_FLS.1	-

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

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

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

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

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

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

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

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

FPT_RPL.1	-
FPT_STM.1	• Management of a time source.
FPT_TST.1	- [55]
FPT_PHP.1	• Management of the user or role that determines whether physical tampering has occurred.
FTP_ITC.1/WAN	- [56]
FTP_ITC.1/MTR	- [55]
FTP_ITC.1/USR	- [55]

994 **Table 13: 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[57]

995 **Table 14: Gateway specific Management Functionalities**

Application Note 50: When it is allowed to change the configuration of non-TSF data of the communication interface via IF_GW_SRV, this functionality shall be described within the management functional requirements in the ST.

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

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

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

996 ### 6.7.2 Security management roles (FMT_SMR)

997 #### 6.7.2.1 FMT_SMR.1: Security roles

FMT_SMR.1.1	The TSF shall maintain the roles [*authorised Consumer,* *authorised Gateway Administrator,* *authorised Service Technician,* *[assignment: the authorised identified roles]*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Hierarchical to:	No other components.
Dependencies:	No dependencies.

Application Note 51: The roles "authorised Gateway Administrator", "authorised Service Technician" and "authorised Consumer" are the minimum roles that are needed for the operation of the TOE. However, the assignment in FMT_SMR.1 deliberately allows the definition of additional roles.

The ST author is asked to complete the roles that are required for a specific TOE and introduce a more complex set of roles, if necessary.

998 ### 6.7.3 Management of security attributes for Gateway access SFP

999 #### 6.7.3.1 Management of security attributes (FMT_MSA)

1000 ##### 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, [assignment: *other operations]*] the security attributes [*all relevant security attributes*] to [*authorised Gateway Administrators*].
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], fulfilled by FDP_ACC.2 FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

1001 ##### 6.7.3.1.2 FMT_MSA.3/AC: Static attribute initialisation for Gateway access SFP

FMT_MSA.3.1/AC	The TSF shall enforce the [*Gateway access SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/AC	The TSF shall allow the [*no role*] to specify alternative initial values to override the default values when an object or information is created.
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

1002 ### 6.7.4 Management of security attributes for Firewall SFP

1003 #### 6.7.4.1 Management of security attributes (FMT_MSA)

1004 ##### 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, [assignment: *other operations]*] the security attributes [*all relevant security attributes*] to [*authorised Gateway Administrators*].
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], fulfilled by FDP_IFC.2/FW FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

1005 ##### 6.7.4.1.2 FMT_MSA.3/FW: Static attribute initialisation for Firewall policy

FMT_MSA.3.1/FW	The TSF shall enforce the [*Firewall SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/FW	The TSF shall allow the [*no role*] to specify alternative initial values to override the default values when an object or information is created.
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Application Note 52:	The definition of restrictive default rules for the firewall information flow policy refers to the rules as defined in FDP_IFF.1.2/FW and FDP_IFF.1.5/FW. Those rules apply to all information flows and must not be overwritable by anybody.

1006 ### 6.7.5 Management of security attributes for Meter SFP

1007 #### 6.7.5.1 Management of security attributes (FMT_MSA)

1008 ##### 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, [assignment: *other operations]*] the security attributes [*all relevant security attributes*] to [*authorised Gateway Administrators*].
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], fulfilled by FDP_IFC.2/FW FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

1009 ##### 6.7.5.1.2 FMT_MSA.3/MTR: Static attribute initialisation for Meter policy

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

override the default values when an object or information is created.

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

6.8 Class FPR: Privacy

6.8.1 Communication Concealing (FPR_CON)

6.8.1.1 FPR_CON.1: Communication Concealing

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 53: The interval and the list of external entities that shall be used in FPR_CON.1.2 highly depends on the actual application case. Therefore, the assignments in FPR_CON.1.2 are left to the ST author.

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 [assignment: *alias metric*].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 54: When the TOE submits information about the consumption or production of a certain commodity that is not relevant for the billing process nor for a secure operation of the Grid, there is no need that this information is sent with a direct link to the identity of the consumer. In those cases the TOE shall replace the identity of the consumer by a pseudonymous identifier. Please note that the identity of the consumer may not be their name but could also be a number (e.g. consumer ID) used for billing purposes.

A Gateway may use more than one pseudonymous identifier.

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

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

1015 ## 6.9 Class FPT: Protection of the TSF

1016 ### 6.9.1 Fail secure (FPT_FLS)

1017 #### 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,*
- *[assignment: other of types of failures in the TSF]*].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 55: 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 this Protection Profile.

1018 ### 6.9.2 Replay Detection (FPT_RPL)

1019 #### 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.

1020 ### 6.9.3 Time stamps (FPT_STM)

1021 #### 6.9.3.1 FPT_STM.1: Reliable time stamps

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

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 56: The 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 this Protection Profile.

1022 ### 6.9.4 TSF self test (FPT_TST)

1023 #### 6.9.4.1 FPT_TST.1: TSF testing

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

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 57: The self-test suite as defined in FPT_TST.1 shall contain 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 shall contain a test to verify the integrity of the TOE firmware.

1024 #### 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's elements has occurred.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application Note 58:	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].

1025 ## 6.10 Class FTP: Trusted path/channels

1026 ### 6.10.1 Inter-TSF trusted channel (FTP_ITC)

1027 #### 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.

1028 #### 6.10.1.2 FTP_ITC.1/MTR: Inter-TSF trusted channel for Meter

FTP_ITC.1.1/MTR	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/MTR	The TSF shall permit [selection: **the Meter, the TOE**] to initiate communication via the trusted channel.
FTP_ITC.1.3/MTR	The TSF shall initiate communication via the trusted channel for [*any communication between a Meter and the TOE*].
Hierarchical to:	No other components.
Dependencies:	No dependencies
Application Note 59:	The corresponding cryptographic primitives are defined by

FCS_COP.1/MTR.

1029 **6.10.1.3 FTP_ITC.1/USR: Inter-TSF trusted channel for User**

FTP_ITC.1.1/USR	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/USR	The TSF shall permit [**the consumer, the service technician**] to initiate communication via the trusted channel.
FTP_ITC.1.3/USR	The TSF shall initiate communication via the trusted channel for [*any communication between a consumer and the TOE and the service technician and the TOE*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application Note 60:	Please note that the requirement on a trusted channel for the consumer interface is implicitly fulfilled for the case that the user interface is implemented via a local display at the TOE.

1030 ## 6.11 Security Assurance Requirements for the TOE

1031 The minimum Evaluation Assurance Level for this Protection Profile is **EAL 4 augmented by**
1032 **AVA_VAN.5 and ALC_FLR.2**.

1033 The following table lists the assurance components which are therefore applicable to this PP.

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

Assurance Class	Assurance Component
	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

1034 **Table 15: Assurance Requirements**

1035 6.12 Security Requirements rationale

1036 6.12.1 Security Functional Requirements rationale

1037 6.12.1.1 Fulfilment of the Security Objectives

1038 This chapter proves that the set of security requirements (TOE) is suited to fulfil the security
1039 objectives described in chapter 4 and that each SFR can be traced back to the security objectives. At
1040 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	

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access
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		

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access
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 16: 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 no longer needed.
- **FDP_SDI.2** defines requirements around the integrity protection for stored data.

- **FPT_FLS.1** defines requirements that the TOE falls back to a safe state for specific error cases.
- **FPT_TST.1** defines the self-testing functionality to detect whether the interfaces for WAN and LAN are separate.
- **FPT_PHP.1** defines the exact requirements around the physical protection that the TOE has to provide.

6.12.1.1.8 O.Management

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

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

6.12.1.1.9 O.Log

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

System Log

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

Consumer Log

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

Calibration Log

The implementation of the calibration log itself is covered by the use of **FAU_GEN.1/CAL. FAU_STG.4/CAL** defines the requirements on what should happen if the audit log is full. **FAU_SAR.1/CAL** defines the requirements around the audit review functions for the calibration log

and that access to them shall be limited to authorised Gateway Administrator via the IF_GW_WAN interface.

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

6.12.1.1.10 O.Access

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

6.12.1.2 Fulfilment of the dependencies

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

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

SFR	Dependencies	Fulfilled by
	FCS_CKM.4 Cryptographic key destruction	
FCS_CKM.1/CMS	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/CMS FCS_CKM.4
FCS_COP.1/CMS	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/CMS FCS_CKM.4
FCS_CKM.1/MTR	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/MTR FCS_CKM.4
FCS_COP.1/MTR	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/MTR FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1/TLS FCS_CKM.1/CMS FCS_CKM.1/MTR
FCS_COP.1/HASH	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 Please refer to chapter 6.12.1.3 for missing dependency
FCS_COP.1/MEM	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/CMS FCS_CKM.4
FDP_ACC.2	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control	FDP_ACC.2

SFR	Dependencies	Fulfilled by
	FMT_MSA.3 Static attribute initialisation	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_MSA.1/FW FMT_SMR.1

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

Table 17: 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 Protection Profile it is assumed that – at least from the WAN side – a high attack potential is posed against the security functions of the TOE. This leads to the use of AVA_VAN.5 (Resistance against high attack potential).

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

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

6.12.2.1 Dependencies of assurance components

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

1175 7 Appendix

1176 7.1 Mapping from English to German terms

English term	German term
billing-relevant	abrechnungsrelevant
CLS, Controllable Local System	dezentral steuerbare Verbraucher- oder Erzeugersysteme
Consumer	Anschlussnutzer Letztverbraucher (im verbrauchenden Sinne) u.U. auch Einspeiser
Consumption Data	Verbrauchsdaten
Gateway	Kommunikationseinheit
Grid	Netz (für Strom/Gas/Wasser)
Grid Status Data	Zustandsdaten des Versorgungsnetzes
LAN, Local Area Network	Lokales Netz (für Kommunikation)
LMN, Local Metrological Network	Lokales Messeinrichtungsnetz
Meter	Messeinrichtung (Teil eines Messsystems)
Processing Profiles	Konfigurationsprofile
Security Module	Sicherheitsmodul (z.B. eine Smart Card)
Service Provider	Diensteanbieter
Smart Meter Smart Metering System[58]	Intelligente, in ein Kommunikationsnetz eingebundene, elektronische Messeinrichtung (Messsytem)
TOE	EVG (Evaluierungsgegenstand)
WAN, Wide Area Network	Weitverkehrsnetz (für Kommunikation)

1177 7.2 Glossary

Term	Description
Authenticity	property that an entity is what it claims to be (according to [SD_6])
Block Tariff	Tariff in which the charge is based on a series of different energy/volume rates applied to successive usage blocks of given size and supplied during a specified period. (according to [CEN])
CA	Certificate Authority or Certification Authority, an entity that issues digital certificates.
CLS config	See chapter 3.2

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

Term	Description
(secondary asset)	
CMS	Cryptographic Message Syntax
Confidentiality	the property that information is not made available or disclosed to unauthorised individuals, entities, or processes (according to [SD_6])
Consumer	End user of electricity, gas, water or heat. (according to [CEN]), See chapter 3.1
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level
Energy Service Provider	Organisation offering energy related services to the consumer (according to [CEN])
external entity	See chapter 3.1
firmware update	See chapter 3.2
Gateway Administrator	See chapter 3.1
Gateway config (secondary asset)	See chapter 3.2
Gateway time	See chapter 3.2
Home Area Network (HAN)	In-house LAN which interconnects domestic equipment and can be used for energy management purposes. (according to [CEN])
Integrity	property that sensitive data has not been modified or deleted in an unauthorised and undetected manner (according to [SD_6])
IT-System	Computersystem
LAN	Local Area Network
Local attacker	See chapter 3.4
Meter config (secondary asset)	See chapter 3.2
Meter Data	See chapter 3.2
Meter Data Aggregator (MDA)	Entity which offers services to aggregate metering data by grid supply point on a contractual basis. NOTE: The contract is with a supplier. The aggregate is of all that supplier's consumers connected to that particular grid supply point. The aggregate may include both metered data and data estimated by reference to standard load profiles (adopted from [CEN])
Meter Data Collector (MDC)	Entity which offers services on a contractual basis to collect metering data related to a supply and provide it in an agreed format to a data aggregator (that can also be the DNO). NOTE: The contract is with a supplier or a pool. The collection may be carried out by manual or automatic means. ([CEN])

Term	Description
Meter Data Management System (MDMS)	System for validating, storing, processing and analysing large quantities of Meter Data. ([CEN])
Metrological Area Network	In-house data communication network which interconnects metrological equipment (i.e. Meters).
Personally Identifiable Information (PII)	Personally Identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
Service Technician	See chapter 3.1
Tariff	Price structure (normally comprising a set of one or more rates of charge) applied to the consumption or production of a product or service provided to a consumer. (according to [CEN])
TLS	Transport Layer Security protocol according to RFC5246
TOE	Target of Evaluation - set of software, firmware and/or hardware possibly accompanied by guidance
TSF	TOE security functionality
WAN attacker	See chapter 3.4
WLAN	Wireless Local Area Network

7.3 References

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

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

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

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

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

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

[BSI-TR-03109-3]	BSI TR-03109-3, BSI, current version, Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen Respective: BSI TR-03116-3, BSI, current version, eCard-Projekte der Bundesregierung – Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen
[BSI-TR-03109-4]	BSI TR-03109-4, BSI, current version, Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways
[BSI-TR-03109-1-I]	BSI TR-03109-1 Anlage I, BSI, current version, CMS Datenformat für die Inhaltsdatenverschlüsselung und -signatur
[BSI-TR-03109-1-II]	BSI TR-03109-1 Anlage II, BSI, current version, COSEM/http Webservices
[BSI-TR-03109-1-IIIa]	BSI TR-03109-1 Anlage IIIa, BSI, current version, Feinspezifikation „Drahtlose LMN-Schnittstelle“ Teil 1
[BSI-TR-03109-1-IIIb]	BSI TR-03109-1 Anlage IIIb, BSI, current version, Feinspezifikation „Drahtlose LMN-Schnittstelle“ Teil 2
[BSI-TR-03109-1-IV]	BSI TR-03109-1 Anlage IV, BSI, current version, Feinspezifikation „Drahtgebundene LMN-Schnittstelle“
[BSI-TR-03109-1-V]	BSI TR-03109-1 Anlage V, BSI, current version, Anforderungen zum Betrieb beim Administrator
[BSI-TR-03109-1-VI]	BSI TR-03109-1 Anlage VI, BSI, current version, Betriebsprozesse
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4 • Part 2: Security functional requirements, dated September 2012, version 3.1, Revision 4 • Part 3: Security assurance requirements, dated September 2012, version 3.1, Revision 4
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1 Revision 4
[CEN]	SMART METERS CO-ORDINATION GROUP (SM-CG) Item 5. M/441 first phase deliverable – Communication – Annex: Glossary (SMCG/Sec0022/DC)
[RFC5114]	IETF RFC 5114, M. Lepinski, S. Kent: Additional Diffie-Hellman Groups for Use with IETF Standards, 2008
[RFC5639]	IETF RFC 5639, M. Lochter, J. Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010
[SD_6]	ISO/IEC JTC 1/SC 27 N7446 Standing Document 6 (SD6): Glossary of IT Security Terminology 2009-04-29, http://www.jtc1sc27.din.de/sce/sd6

[SecMod-PP] Common Criteria Protection Profile for a Security Module for Smart Metering Systems (BSI-CC-PP-0077-2013).

1179