Federal Office
for Information Security

Protection Profile for the Gateway of a Smart Metering System

Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen

Gateway PP

v01.01.01(final draft)

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

Table of content

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 consumers side and allows to send 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 Metering Systems (or their components) and informs them about the requirements that have to be implemented. It is further directed to stakeholders being responsible for purchasing Smart Metering Systems.

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 a functionality requires a 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”.

1.2 PP Reference

Title:	Protection Profile for the Gateway of a Smart Metering System (Gateway PP)
Version	01.01.01(final draft)
Date	25.08.11
Authors	Dr. Helge Kreutzmann, Stefan Vollmer (BSI), Nils Tekampe and Arnold Abromeit (TÜV Informationstechnik GmbH)
Registration	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Certification-ID	BSI-CC-PP-0073
CC-Version	3.1 Revision 3
Keywords	Smart Metering, Protection Profile, Meter, Gateway, PP

1.3 Specific terms

Various different vocabularies exist in the area of Smart Grid, Smart Metering, and Home Automation. Further, the Common Criteria maintain their own vocabulary. The following table provides an overview over the most prominent terms that are used in this Protection Profile and should serve to 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 or local producer of electricity, gas, water or heat (or other commodities).	[CEN]

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

Term	Definition	Source (if any)
Gateway Smart Metering Gateway[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 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.	
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 hyperonym for HAN and LMN.	[CEN], adopted
LMN, Local Metrological Network	In-house data communication network which interconnects metrological equipment and can be used for energy management purposes.	
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 transmit 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 (unless it is in the same device as the Gateway) and will typically deploy a Security Module for this. Please note that the term Meter refers to metering devices for all kinds of commodities.	[CEN], adopted
Meter Data	Meter readings that allow calculation of the quantity of a commodity, for example electricity, gas, water or heat consumed or produced over a period. Other readings and data may also be included[7] (such as quality data, events and alarms).	[CEN]

[6] Please note that the terms “Gateway” and “Smart Metering Gateway” are used synonymously within this document

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

Term	Definition	Source (if any)
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 [PP_SM].	
User, external entity	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary.	[CC]
WAN, Wide Area Network	Extended data communication network connecting a large number of communication devices over a large geographical area.	[CEN]

Table 1: Specific Terms

1.4 TOE Overview

1.4.1 Introduction

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

1.4.2 Description of the Smart Metering System

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

[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.

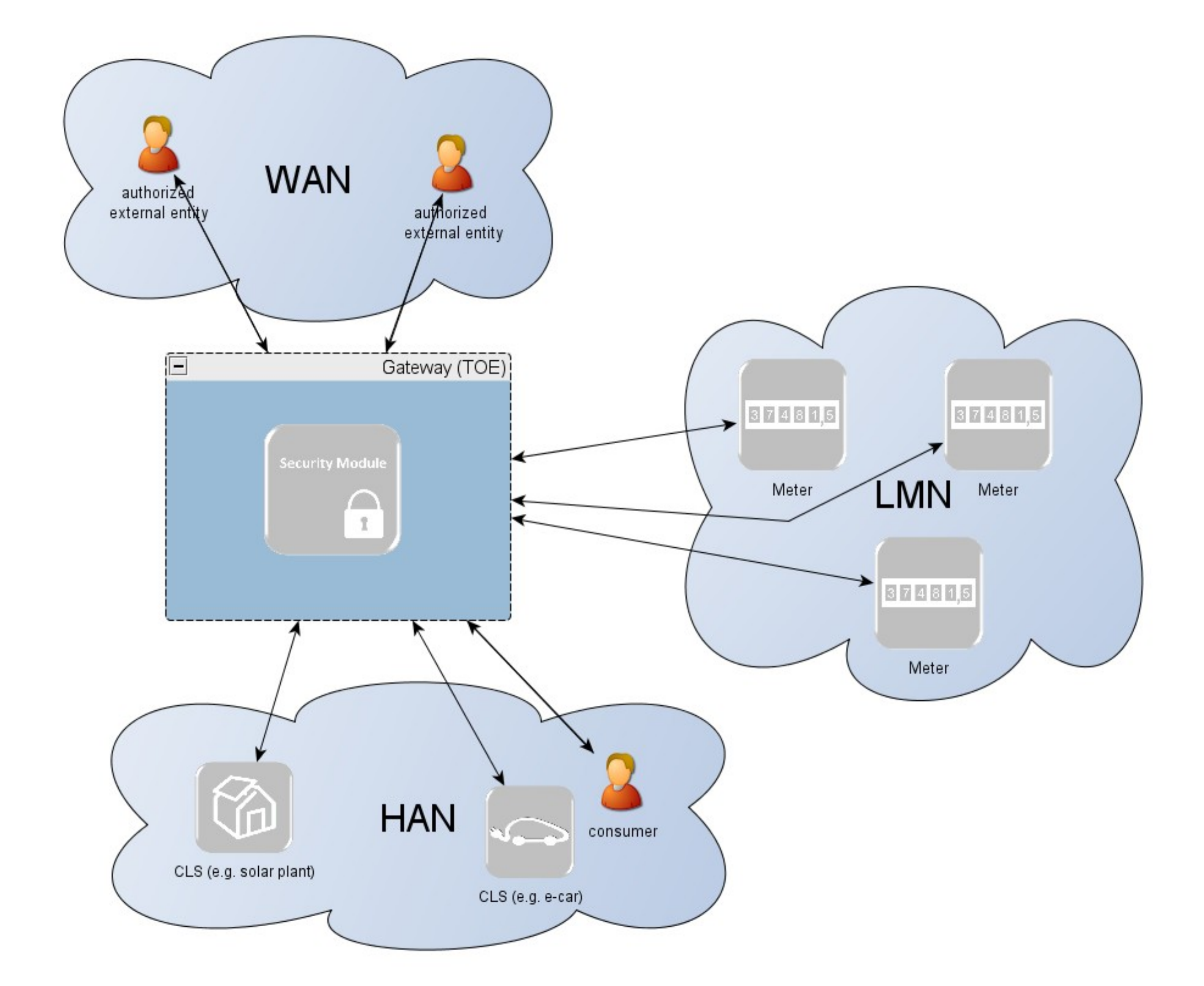


Figure 1: The TOE and its direct environment

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 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 relevant information[9] the information will be signed and encrypted 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) in defined intervals and submits those records to the Gateway. The Meter Data has to be signed before transfer in order to ensure its authenticity and integrity unless the transmission is physically protected due to the Meter and the Gateway being implemented within one device and utilising a wired or optical[10] connection. The Meter is comparable to a classical meter[11] and has comparable security requirements; it will be sealed

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

[10] Assuming that the technology for optical connection can be sufficiently protected against eavesdropping by the box of the TOE.

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

as classical meters are today according to the regulations of [PTB_A50.7]. The Meter further supports the encryption of its connection to the Gateway[12].

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

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

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

Please note that the arrows of the interfaces within the Smart Metering System as shown in Figure 2 indicate the flow of information (which is bi-directional). However, it does not indicate that a communication flow can be initiated bi-directionally. Indeed, the following chapters of this PP will place dedicated requirements on the way an information flow can be initiated[13].

[12] It should be noted that this PP does not imply that the connection 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.

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

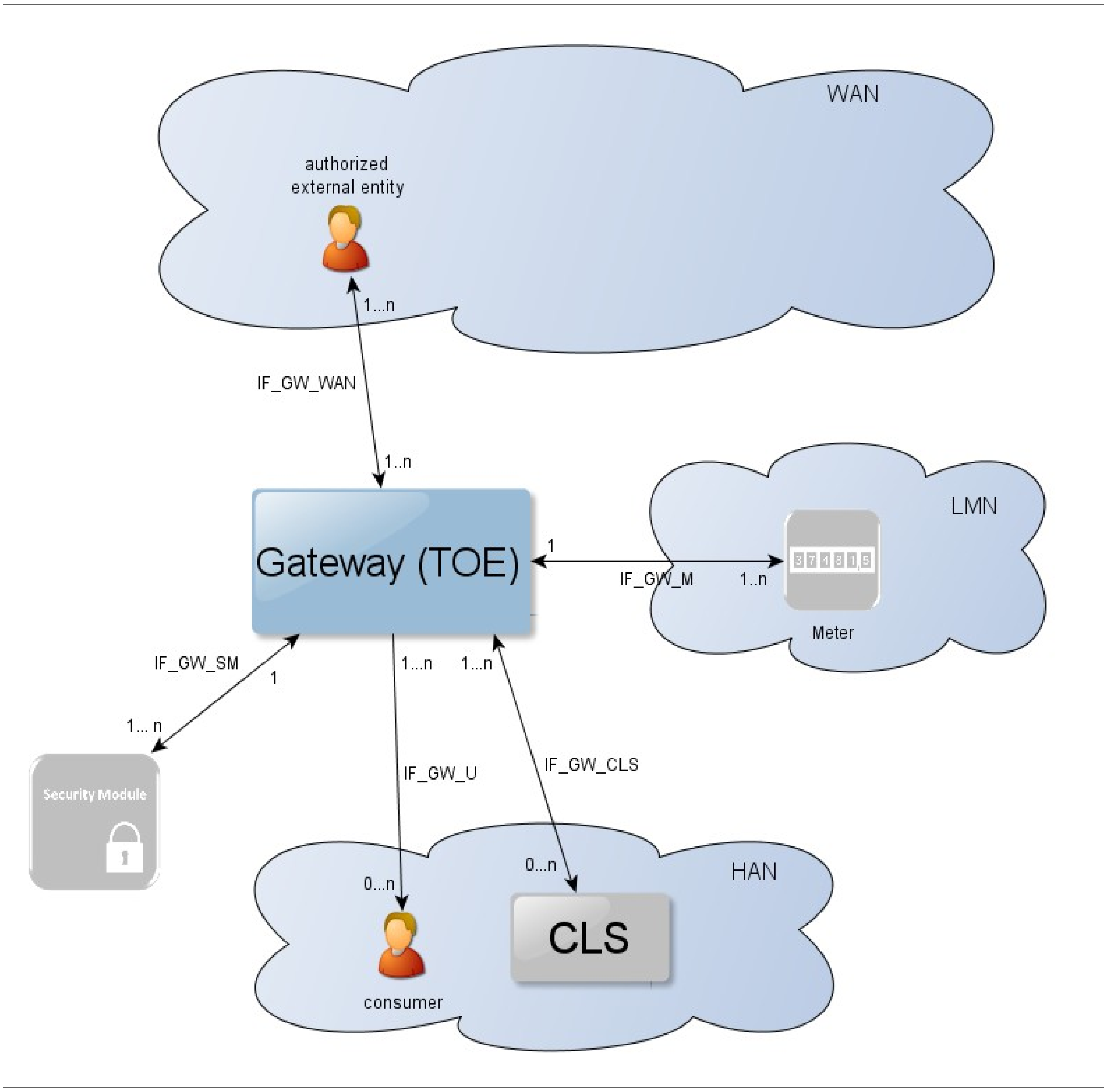


Figure 2: The logical interfaces of the TOE

The definition 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 transfered between LAN and WAN flows via the Gateway which makes it an ideal unit for implementing significant parts of the system's overall security functionality.

- Because a Gateway can be used to connect and protect multiple Meters (while a Meter will always be connected to exactly one Gateway) and CLSs with the WAN there might be more Meters and CLS in a Smart Metering System than there are Gateways.

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

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

Typically, the Gateway will be placed in the household or premises of the consumer[14] 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). Service providers in the context of the Gateway are the Gateway Operator, Meter Operator, Grid Operator, Commodity Supplier and others as introduced in chapter 3.1.

The TOE has a fail-safe design that specifically ensures that any malfunction can not impact the delivery of a commodity, e.g. energy, gas or water[15].

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.

[14] 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 or logical access to the Gateway.

[15] 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.

1.4.5 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[16].

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 TOE it is not possible to move security features from the scope of one TOE to another.

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[17]), 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.

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

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

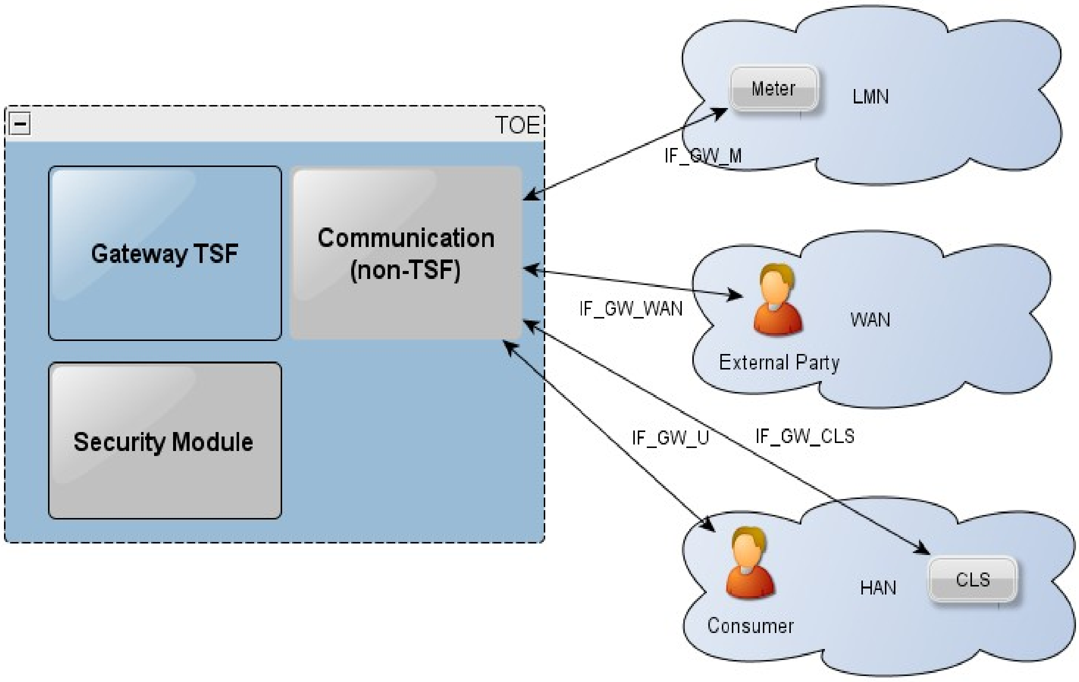


Figure 3: TOE design: A Gateway and multiple Meters (physical view)

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.

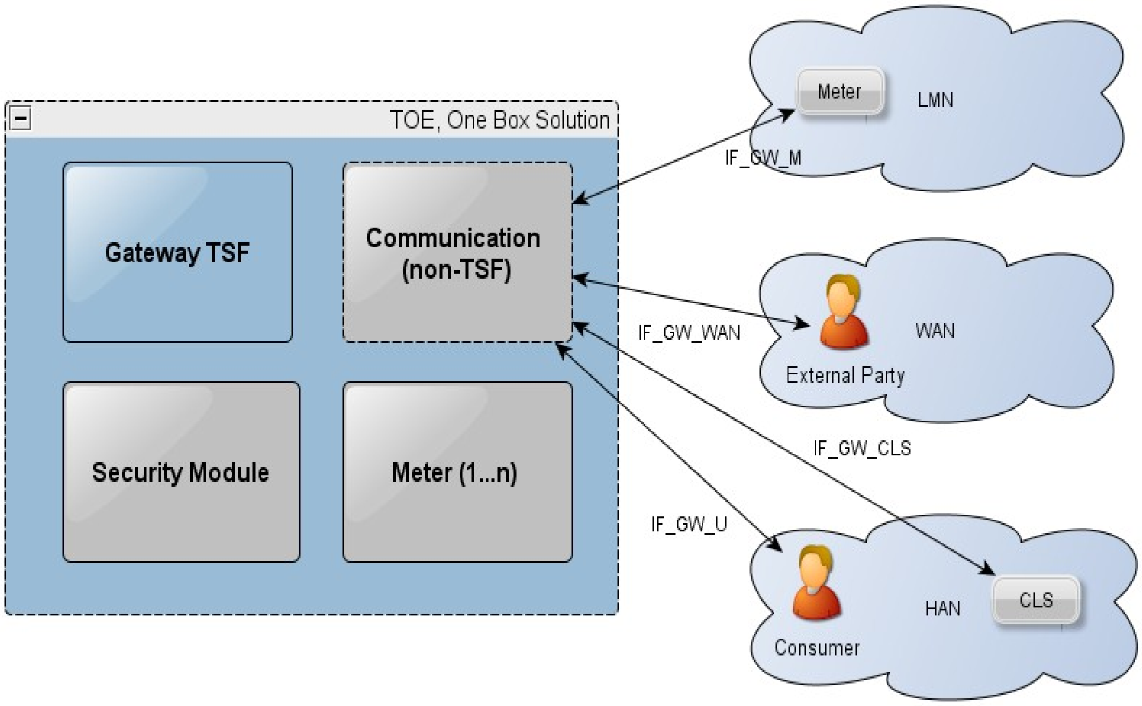


Figure 4: TOE design: One Box Solution (physical view)

From a security perspective this solution has the advantage that the communication between the Gateway unit and the meters inside happens in the protected area of the box (assuming that the connection is realised wired or by optical means that are protected by the box) and hence the communication does not require encryption.

In this context it is relevant that there is one physical unit (in form of a sealed box/cabinet) that provides an adequate level of physical protection over the Gateway, its Meters and the communication channel between.

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 component

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.

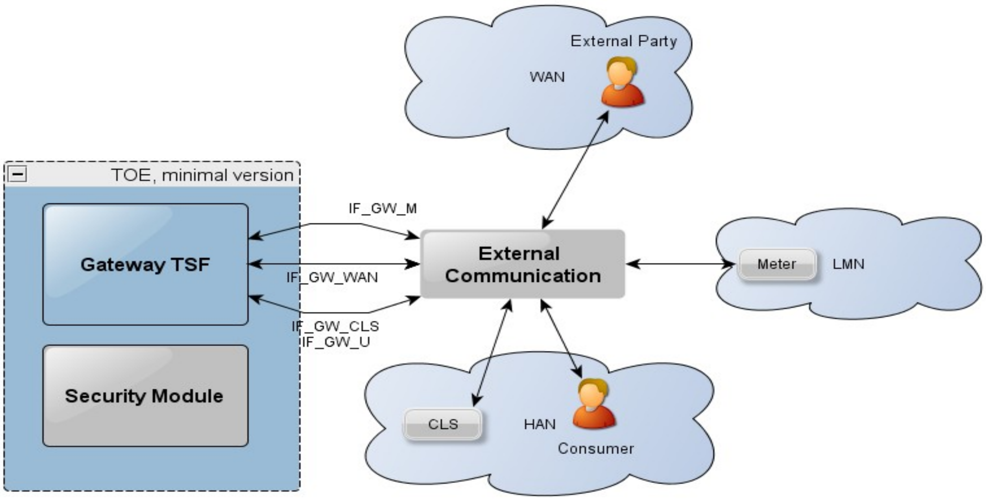


Figure 5: TOE design: Minimal implementation (physical view)

A classical example of such a functionality is the communication capability 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 component.

1.4.6 TOE logical boundary

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

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

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

1.4.6.1 Handling of Meter Data[18]

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 parties.

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

The TOE utilises access control profiles to determine which data shall be sent to which component or external entity. An access control 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 access control 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 access control profiles can be found in [BSI-TR-3109].

Please note that it is possible that a TOE enforces more than one access control profile, specifically if the communication and the contractual requirement for multiple external parties 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 accept data (e.g. configuration data, firmware updates) from correspondingly authorised Gateway Administrators or correspondingly authorised external entities only,
- the Gateway shall send processed Meter Data to correspondingly authorised external entities only.

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[19],
- 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[20],
- preserve the integrity of the system components and their configurations.

The TOE offers a local interface to the consumer (see also IF_GW_U 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_U 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)[21].

[19] 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.

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

[21] 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-3109] therefore may pose additional requirements on the way the consumer can

1.4.6.2 Confidentiality protection

The TOE protects data from unauthorised disclosure

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

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

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

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

1.4.6.4 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 or devices in the HAN may establish a connection to an external entity, connection establishment by an external entity in the WAN or a Meter in the LMN is not 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 parties in the WAN to trigger a connection establishment by the Gateway,

access this interface.

- connections are allowed to pre-configured addresses only,
- only cryptographically-protected (i.e. encrypted, integrity protected and mutually authenticated) connections are possible.

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

The communication flows that are enforced by the Gateway between parties in the HAN, LMN and WAN are summarized in the following table[22]:

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	No connection establishment allowed	- (see following list)

Table 2: Communication flows between devices in different networks

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

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

[22] 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.

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[23] 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 parties 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) or by devices in the HAN.

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

In order to allow this kind of re-activeness of the Gateway this PP allows the Gateway to keep existing connections to external parties open and to offer a so called wake-up service.

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

1. If the Gateway receives such a message it will decrypt it and verify the signature. The Gateway shall use the services of its Security Module for signature verification.
2. If the signature cannot be verified the message will be dropped/ignored. No feedback is given to the sending external party and the wake-up sequence terminates.
3. If the signature could be verified successfully the Gateway verifies the content of the message. This content includes a time-stamp. The Gateway verifies that the message has been sent within an acceptable period of time in order to prevent replayed messages.
4. If the content could not be verified as described in step #3 the message will be dropped/ignored. No further operations will be initiated and no feedback is provided.
5. If the content could be verified as described in step #3 the message will be dropped/ignored. No feedback is given to the sending external entity. However, in this case the Gateway initiates a connection to a pre-configured external entity.

More details on the exact implementation of this mechanism can be found in [BSI-TR-3109].

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 access control 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.

[23] Please note that [BSI-TR-3109] may pose additional requirements on the interaction with the Gateway in this context.

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 has been and will be authorised based on the previous and current access control 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 access control profile. The consumer log shall contain the configured addresses for internal and external entities including the CLS.

System Status

The TOE shall provide information on the current status of the TOE. Specifically it shall indicate whether the TOE operates normally or any errors have been detected that are of relevance for the consumer.

Audit Log and Monitoring

The TOE shall provide all audit data from the consumer log at the user interface IF_GW_U. 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.

1.4.7 The logical interfaces of the TOE

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

Interface Name	Description	Mandatory
IF_GW_U	Interface via which the Gateway provides the consumer with the possibility to review information that are relevant for billing or the privacy of the consumer. Specifically the access to the consumer log is only allowed via this interface.	yes
IF_GW_M	Interface between the Meter and the Gateway. The	yes[24]

	Gateway receives Meter Data via this interface.	
IF_GW_SM	The Gateway invokes the services of its Security Module via this interface.	yes
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.	yes
IF_GW_WAN	The Gateway submits information to authorised external entities via this interface.	yes

Table 3: TOE external interfaces

1.4.8 The cryptography of the TOE and its Security Module

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

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

[24] 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.

Aspect	TOE	Security Module
Communication with external entities	Encryption Decryption	Key Negotiation: • Authentication of the external entity • Hashing • Secure storage of the private key • Integrity protected and authentic storage of a public root or CA[25] key • Random Number Generation
Communication with the consumer	Encryption Decryption	Key Negotiation: • Authentication of the consumer • Secure storage of the private key • Integrity protected and authentic storage of an anchor of trust • Random Number Generation
Communication with the Meter	Encryption Decryption Hashing for Signature Generation/Verification	Key Negotiation: • Secure storage of the private key (in case of TLS connection) • Integrity protected and authentic storage of a public root or CA key • Random Number Generation
Verification of Meter Data received from the Meter	Hashing Secure storage of the Public Key	Verification of signature
Signing data before submission to an external entity	Hashing	Signature creation Secure Storage of the private key
Content data encryption	Encryption Decryption	Random Number Generation for key generation Key encryption

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

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

[25] Please note that the term CA key refers to the key that stands for the authenticity of the public key of the communication partner. This may also be given by the key itself in case of a relationship of direct trust. Please refer to [BSI-TR-3109] for more information on those aspects.

As a general rule all processed Meter Data that is prepared to be submitted to external entities is encrypted on a content level using PKCS#7.

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

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

The following figures introduce the communication process between the Meter, the TOE and external entities (focussing on billing-relevant Meter Data). Two cases can be distinguished:

1.4.8.1.1 Distributed Gateway and Meter

In the case that Meter and Gateway are realised in separate physical devices 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 signed (typically using the services of an integrated Security Module).
   b) The Meter Data is transmitted via an encrypted and mutually authenticated channel (case A) to the Gateway. Please note that the submission of this information may be triggered by the Meter or the Gateway.

   Or

   c) The Meter Data is encrypted using a 128bit AES and facilitating a defined data structure to ensure the authenticity and confidentiality (case B).
3. The authenticity and integrity of the Meter Data is verified by the Gateway invoking the services of its Security Module.
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 access control profile else the cryptographic information flow will be cancelled.
5. The processed Meter Data is signed using the services of the Security Module.
6. The processed and signed Meter Data may be stored for a certain amount of time.
7. The processed Meter Data is encrypted using PKCS#7 for the final recipient of the data.
8. The processed Meter Data is finally submitted to an authorised external entity in the WAN via an encrypted and mutually authenticated channel.

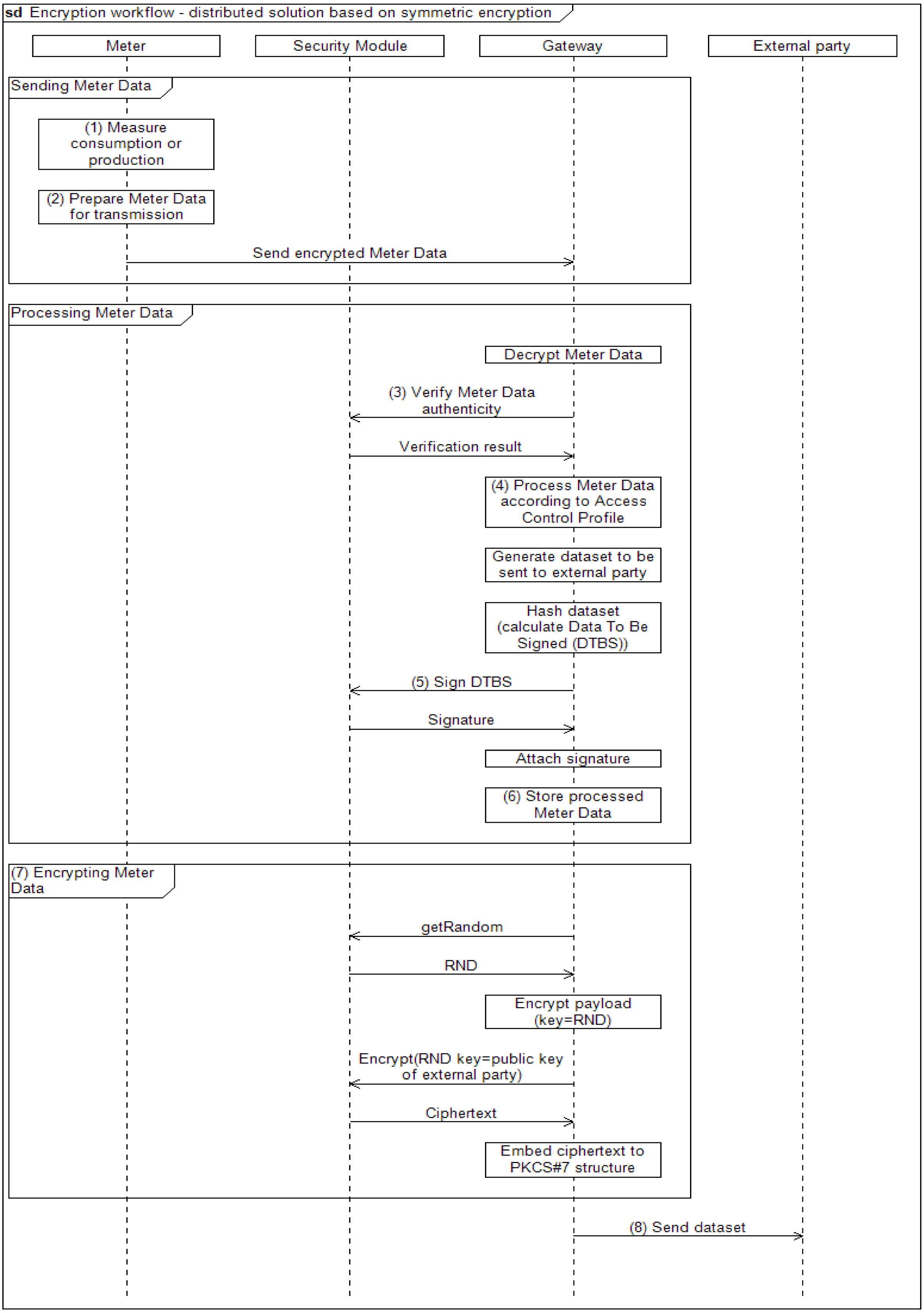

sd Encryption workflow - distributed solution based on symmetric encryption
Meter
Security Module
Gateway
External party
Sending Meter Data
(1) Measure consumption or production
(2) Prepare Meter Data for transmission
Send encrypted Meter Data
Processing Meter Data
Decrypt Meter Data
(3) Verify Meter Data authenticity
Verification result
(4) Process Meter Data according to Access Control Profile
Generate dataset to be sent to external party
Hash dataset (calculate Data To Be Signed (DTBS))
(5) Sign DTBS
Signature
Attach signature
(6) Store processed Meter Data
(7) Encrypting Meter Data
getRandom
RND
Encrypt payload (key=RND)
Encrypt(RND key=public key of external party)
Ciphertext
Embed ciphertext to PKCS#7 structure
(8) Send dataset

Figure 6: Cryptographic information flow for distributed Meter and Gateway (case B)

576

1.4.8.1.2 *Integrated Gateway and Meter*

In the case that Meter and Gateway are realised in one physical device the basic information flow for Meter Data is shown in Figure 7.

1. The Meter measures the consumption or production of a certain commodity.
2. The Meter Data is transmitted to the Gateway unit of the device. Please note that the submission of this information may be triggered by the Meter or the Gateway.
3. The Meter Data is further processed by the Gateway according to the regulations in the access control profiles.
4. The processed Meter Data is signed using the services of the Security Module.
5. The signed Meter Data may be stored for a certain amount of time.
6. The processed Meter Data is encrypted using PKCS#7 for the final recipient of the data.
7. The processed Meter Data is finally submitted to an authorised external entity in the WAN via an encrypted and mutually authenticated channel.

This scenario acknowledges the physical protection of the communication between the Meter and the Gateway that is achieved as both units are implemented within one device when utilising a wired or optical connection between the devices.

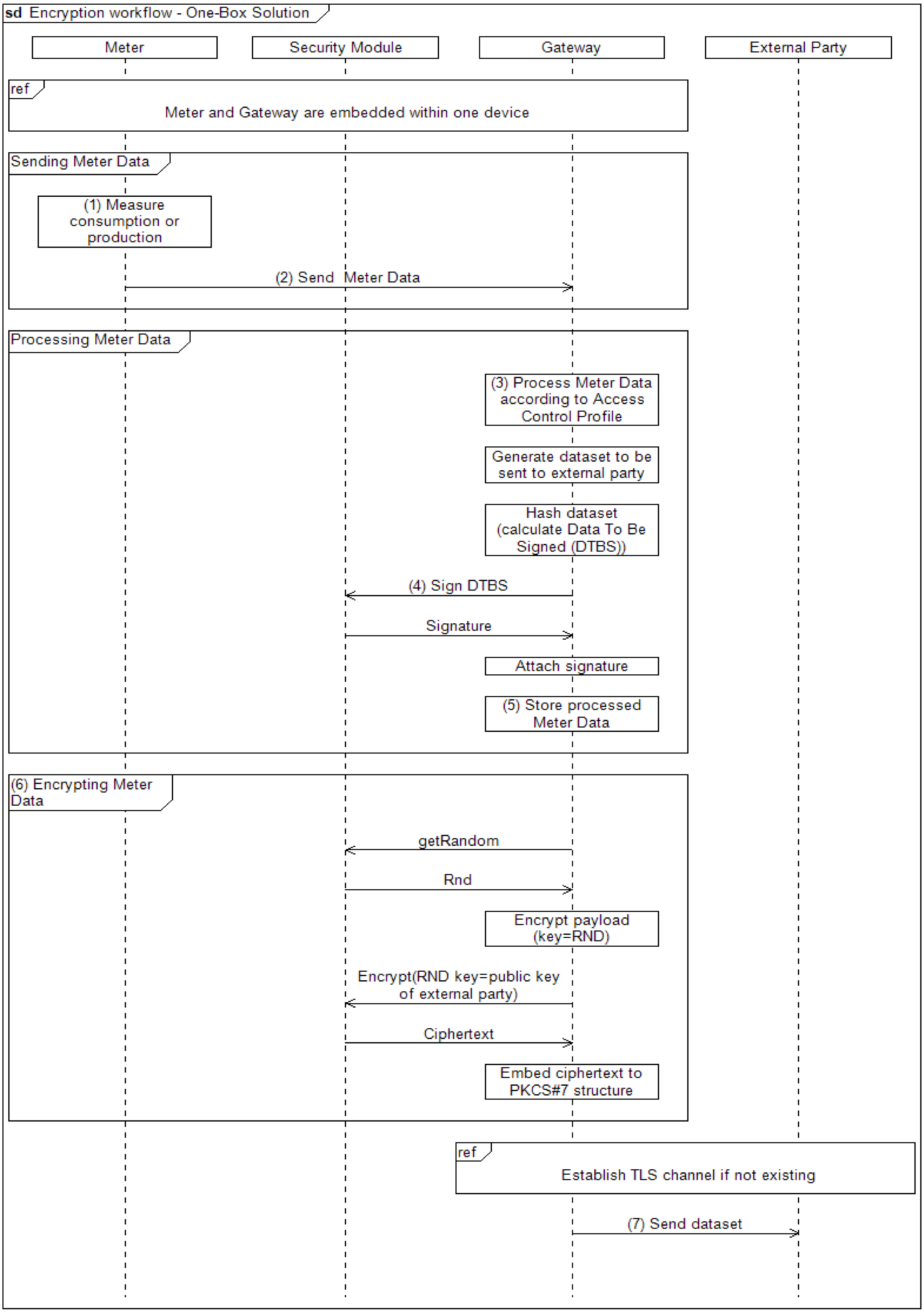

sd Encryption workflow - One-Box Solution
Meter
Security Module
Gateway
External Party
ref
Meter and Gateway are embedded within one device
Sending Meter Data
(1) Measure consumption or production
(2) Send Meter Data
Processing Meter Data
(3) Process Meter Data according to Access Control Profile
Generate dataset to be sent to external party
Hash dataset (calculate Data To Be Signed (DTBS))
(4) Sign DTBS
Signature
Attach signature
(5) Store processed Meter Data
(6) Encrypting Meter Data
getRandom
Rnd
Encrypt payload (key=RND)
Encrypt(RND key=public key of external party)
Ciphertext
Embed ciphertext to PKCS#7 structure
ref
Establish TLS channel if not existing
(7) Send dataset

Figure 7: Cryptographic information flow for integrated Meter and Gateway

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 3 of Common Criteria [CC].
- This PP is conformant to [CC] part 2 extended due to the use of FPR_CON.1.
- This PP is conformant 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 rationale

Since this PP does not claim conformance to any protection profile, this section is not applicable.

2.5 Package Claim

- This PP conforms to assurance package EAL4 augmented by AVA_VAN.5 and ALC_FLR.2 as defined in [CC] Part 3.

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.

Consumer: The 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).

Grid Operator: Operates the grid in which the commodity is distributed.

Supplier: Supplies the commodity to the consumer.

Producer: Produces the commodity.

Meter Operator: Responsible for installing and maintaining the Meter.

Gateway Operator: Responsible for installing and maintaining the Gateway. Responsible for gathering Meter Data from the Meter and for providing these data to the corresponding external entities.

Meter Admin: Administrator of the Meter, may be an agent of the Meter Operator.

Gateway Administrator: Administrator of the Gateway, may be an agent of the Gateway Operator.

Gateway Developer: Responsible for development of the Gateway and for providing signed firmware updates.

Profile Provider: This party is responsible for issuing the profiles that are used for information flow control. Please refer below to the assumption A.AccessProfile for more details on those profiles.

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 hyperonym for all entities mentioned before.

3.2 Assets

The following table introduces the relevant assets for this Protection Profile. The table focusses on the assets that are relevant for the Gateway and does not claim to provide an overview over all assets in the Smart Metering System or for other devices in the LMN.

Asset	Description	Need for Protection
Meter Data	Meter readings that allow calculation of the quantity of a commodity, e.g. electricity, gas, water or heat consumed over a period. Meter Data comprise Consumption or Production Data (billing-relevant) and grid status data (not billing-relevant). While billing 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)
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[26].	• Integrity and authenticity (comparable to the classical meter and its security requirements) • Confidentiality (due to privacy concerns)
Supplementary Data	The Gateway may be used for communication purposes by devices in the LMN or HAN. It may be that the functionality of the Gateway, that is used by such a device, is limited to pure (but secure) communication services. Data that is transmitted via the Gateway but that does not belong to one of the aforementioned data types is named Supplementary Data.	• Integrity and authenticity (comparable to the classical meter and its security requirements) • Confidentiality in the WAN (due to privacy concerns)
Data / User Data	The terms Data or User Data are used as a hyperonyms 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)
Meter config (secondary asset)	Configuration data of the Meter to control its behaviour including the Meter identity.	• Integrity and authenticity • Confidentiality
Gateway config (secondary asset)	Configuration data of the Gateway to control its behaviour including the	• Integrity and authenticity • Confidentiality

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

Asset	Description	Need for Protection
	Gateway identity and the access control profiles.	
CLS config (secondary asset)	Configuration data of a CLS to control its behaviour.	• Integrity and authenticity • Confidentiality
Firmware update (secondary asset)	Firmware update that is downloaded by the TOE to update the firmware of the TOE.	• Integrity and authenticity
Firmware (secondary asset)	The firmware of the TOE	• Integrity • Authenticity

Table 5: Assets

3.3 Assumptions

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

A.ExternalPrivacy It is assumed that 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 is 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[27] and the communication channel between the TOE and its Security Module.

A.AccessProfile The access control 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.

[27] The degree of protection for the communication channel between the Meter(s) and the TOE depends on the concrete realisation. For a One-Box-Solution this protection itself is sufficient while in the case that Meter and TOE are realised in separate physical units this protection can only provide a basic level that needs to be augmented by logical mechanisms (i.e. encryption).

A.Network

It is assumed that

- a WAN network connection with a sufficient reliability and bandwidth for the individual situation is available,
- one or more trustworthy sources for an update of the system time are available in the WAN,
- the Gateway is the only communication gateway for Meters in the LMN[28],
- if devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is appropriately protected.

Application Note:

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 requirements of [PTB_A50.7].

Application Note:

The profiles that are used for information flow control as referred to by A.AccessProfile are an essential factor for the preservation of the privacy of the consumer. The 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 profiles shall be visible for the consumer to allow a transparent communication.

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

3.4 Threats

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

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

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

- Attackers having physical access to Meter, Gateway, or a connection between these components (local attacker), trying to disclose or alter assets while stored in Meter or Gateway or while transmitted between meters in the LMN and the Gateway. Please note that the following threat model assumes that the local attacker has less motivation than the WAN attacker as a successful attack of a local attacker will always only impact one Gateway. Please further note that the local attacker includes the consumer.
- An attacker located in the WAN (WAN attacker) trying to compromise the confidentiality and/or integrity of the 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).

Even though in the concept of Common Criteria the attacker with the highest attack potential (which is the WAN attacker with a high attack potential) determines the level for the vulnerability analysis (please also refer to chapter 6.12.2) the definition of the following threats acknowledges that the local attacker has less attack potential than the remote attacker.

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 or Gateway and consumer. The objective of the attacker may be to alter billing-relevant information or grid status information.

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 unit that is protected by the TOE.

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

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

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

T.Infrastructure A WAN attacker may try to obtain control over Gateways, Meters or CLS via the TOE, which enables the WAN Attacker to cause damage to consumers or external entities or the grids used for commodity distribution (e.g. by sending wrong data to an external entity).

A WAN attacker may also try to conquer a CLS in the HAN first in order to logically attack the TOE from the HAN side.

T.ResidualData

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

T.ResidentData

A WAN or local attacker may try to access (i.e. read, alter, delete) information to which they don't have permission to while the information is stored in the TOE.

While the WAN attacker only uses the logical interface of the TOE that is provided into the WAN the local attacker may also physically access the TOE.

T.Privacy

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

3.5 Organizational Security Policies (OSPs)

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

OSP.SM

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

- verification of digital signatures,
- generation of digital signatures,
- key agreement,
- Random Number Generation ,
- asymmetric de- and encryption.

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

OSP.Log

The TOE shall maintain a set of log files 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 access control 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 and the calibration log shall only be allowed for an authorised Gateway Administrator via the WAN interface of the TOE.
2. Access to the information in the consumer log shall only be allowed for an authorised consumer via the user interface of the TOE. The consumer shall only have access to their own information.

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

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

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

4. Security Objectives

4.1 Security Objectives for the TOE

O.Firewall

The TOE shall serve as the connection point for internal devices or units in the Smart Metering System to external entities and shall provide firewall functionality in order to protect the devices or units of the LMN and HAN (as long as they use the Gateway) against threats from the WAN side.

The firewall:

- shall allow only connections established from internal network to external network (i.e. from systems 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 any other services being offered on the WAN side interface,
- 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

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 outside parties in the WAN in order to ensure that no privacy-relevant information may be obtained by analysing the frequency, load, size or the absence of external communication.[29]

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 for the communication with the Meter[30] if the Meter and Gateway are not implemented within a single device and the connection is realized using a wired or optical technology,
- the TOE shall verify the integrity and authenticity of the data received from a Meter if the Meter and Gateway are not implemented within a single device before handling it further,
- the TOE shall process the data according to the definition in the corresponding access control 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 access control 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 pseudonymize 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[31].

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

[30] It is acknowledged that the implementation of a secure channel between the Meter and the Gateway is a security function of both units. The TOE as defined in this 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. However, it should be noted that the encryption of this channel only needs to protect against the Local Attacker possessing a basic attack potential and that the Meter utilises the services of its Security Module to negotiate the channel.

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

In addition the TOE shall generate the required keys utilising the services of its Security Module[32], ensure that the keys are only used for an acceptable amount of time and destroy ephemeral[33] keys if not longer needed.[34]

O.Time

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

O.Protect

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

Specifically, the TOE shall

- overwrite any information that is not longer needed to ensure that it is not longer available via the external interfaces of the TOE[34],
- implement a self test,
- 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)[35],
- 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 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 access control profiles causing this information flow as well as

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

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

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

[35] 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.

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 and the calibration log shall only be allowed for an authorised Gateway Administrator via the WAN interface of the TOE.
2. Access to the information in the consumer log shall only be allowed for an authorised consumer via the user 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.

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 users to information and functions via its external interfaces[36].

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 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.

OE.Profile The access control 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,

[36] 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.

- generation of digital signatures,
- key agreement,
- Random Number Generation,
- asymmetric de- and encryption.

The Security Module used shall be certified according to [PP_SM] 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.

4.3 Security Objectives rationale

4.3.1 Overview

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

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access	OE.SM	OE.ExternalPrivacy	OE.TrustedAdmins	OE.PhysicalProtection	OE.Profile	OE.Update	OE.Network
T.DataModificationLocal				X	X		X	X	X				X	X			
T.DataModificationWAN	X				X		X	X					X				
T.TimeModification						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			
T.Privacy	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.AccessProfile															X		
A.Update																X	
A.Network																	X

Table 6: Rationale for Security Objectives

4.3.2 Countering the threats

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

4.3.2.1 General objectives

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

O.Management is indispensable as it defines the requirements around the management of the Security Functions. Without a secure management no TOE can be secure. Also **OE.TrustedAdmins**

contributes to this aspect as it provides the requirements on the availability of a trustworthy Gateway Administrator. **O.Protect** is present to ensure that all security functions are working as specified.

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

4.3.2.2 T.DataModificationLocal

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

O.Meter defines that the TOE will enforce the encryption of communication when receiving consumption or production data from the Meter. **O.Log** defines that the consumer may only read the log files via a secured (i.e. confidentiality and integrity protected) connection. **O.Crypt** defines the required cryptographic primitives for this encryption. Both 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 that the TOE will enforce the encryption of communication for each communication to the WAN. **O.Crypt** defines the required cryptographic primitives for this encryption. Both objectives together ensure that the communication between the Meter and the TOE cannot be modified.

4.3.2.4 T.TimeModification

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

O.Time defines that the TOE needs a reliable time stamp mechanism that is also updated from reliable sources regularly. Therewith, **O.Time** is 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 that the TOE will enforce the encryption of communication for each communication to the WAN. **O.Crypt** defines the required cryptographic primitives for this encryption. 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 of communication when polling or receiving consumption or production data from the Meter. **O.Crypt** defines the required cryptographic primitives for this encryption. 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 contains regulations on the access of consumers to information and functions of the TOE.

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 not longer used. Assuming that a TOE follows this requirement an attacker can not read out any residual information as it is simply not existing.

4.3.2.9 T.ResidentData

The logical aspects of the threat **T.ResidentData** are directly and completely covered by the requirements as defined by **O.Access** and **O.Firewall**. Further, the environment contributes to this.

The aspect of a local attacker with physical access to the TOE is covered by a combination of **O.Protect** (defining the passive physical security that the TOE has to provide) in combination with the environment of the TOE. Specifically 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** and **O.Firewall** as these objective ensures that the TOE will only distribute Meter data to external parties in the WAN as defined in the corresponding access control profiles and that the data will be protected for the transfer. **OE.Profile** is present to ensure that the access control profiles contain the correct information.

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 same 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 requirements 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.AccessProfile

The assumption **A.AccessProfile** 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.

5. Extended Component definition

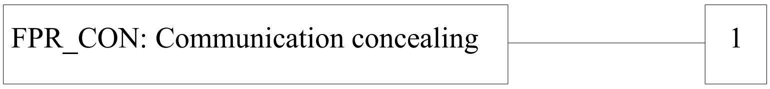
5.1 Communication concealing (FPR_CON)

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

5.2 Family behaviour

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

5.3 Component levelling



5.4 Management

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

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

5.5 Audit

There are no auditable events foreseen.

5.6 Communication concealing (FPR_CON.1)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6. Security Requirements

6.1 Overview

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

The following notations are used:

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

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/SYS.1	Security alarms for system log
FAU_GEN/SYS.1	Audit data generation for system log
FAU_SAA/SYS.1	Potential violation analysis for system log
FAU_SAR/SYS.1	Audit review for system log
FAU_STG/SYS.4	Prevention of audit data loss for the system log
FAU_GEN/CON.1	Audit data generation for consumer log
FAU_SAR/CON.1	Audit review for consumer log
FAU_STG/CON.2	Guarantees of audit data availability for consumer log
FAU_GEN/CAL.1	Audit data generation for calibration log
FAU_SAR/CAL.1	Audit review for calibration log
FAU_STG/CAL.4	Prevention of audit data loss for the calibration log
FAU_GEN.2	User identity association
FAU_STG.1	Protected audit trail storage for all logs
Class FCO: Communication	
FCO_NRO.2	Enforced proof of origin

Class FCS: Cryptographic Support	
FCS_CKM/TLS.1	Cryptographic key generation for TLS
FCS_COP/TLS.1	Cryptographic operation for TLS
FCS_CKM/PKCS.1	Cryptographic key generation for PKCS
FCS_COP/PKCS.1	Cryptographic operation for PKCS#7
FCS_COP/MTR.1	Cryptographic operation for Meter communication encryption
FCS_CKM.4	Cryptographic key destruction
FCS_COP/HASH.1	Cryptographic operation for Signatures
FCS_COP/MEM.1	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/FW.2	Complete information flow control for firewall
FDP_IFF/FW.1	Simple security attributes for Firewall
FDP_IFC/MTR.2	Complete information flow control for Meter information flow
FDP_IFF/MTR.1	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.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/AC.1	Management of security attributes for gateway access policy
FMT_MSA/AC.3	Static attribute initialisation for gateway access policy
FMT_MSA/FW.1	Management of security attributes for firewall policy

FMT_MSA/FW.3	Static attribute initialisation for Firewall policy
FMT_MSA/MTR.1	Management of security attributes for Meter policy
FMT_MSA/MTR.3	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/WAN.1	Inter-TSF trusted channel for WAN
FTP_ITC/MTR.1	Inter-TSF trusted channel for Meter
FTP_ITC/USR.1	Inter-TSF trusted channel for User

Table 7: List of Security Functional Requirements

6.2 Class FAU: Security Audit

6.2.1 Introduction

A TOE compliant to this Protection Profile shall implement three different audit logs as defined in OSP.Log and O.Log. The following table provides an overview over the three audit logs before the following chapters introduce the SFRs related to those audit logs.

	System-Log	Consumer-Log	Calibration-Log
Purpose	• Inform the Gateway Administrator about security relevant events • Log all events as defined by Common Criteria for the used SFR • Log all system relevant events on specific functionaltity • Automated alarms in case of a cumulation of certain events	• Inform the consumer about all information flows to the WAN • Inform the consumer about the access control profiles • Inform the consumer about other metering data (not billing-relevant) • Inform the consumer about all billing-	• Track changes that are relevant for the calibration of the TOE

		relevant data needed to verify an invoice	
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 access control profiles • Non-billing-relevant Meter Data • Information about the system status (including relevant errors)	• 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	• Access by authorised consumer and via IF_GW_U only to the data related to the current consumer	• Access by authorised Gateway Administrator and via IF_GW_WAN only
Deletion	• Ring buffer. • Overwriting old events is possible if the memory is full	• Ring buffer. • The availability of data has to be ensured for a sufficient amount of time • Overwriting old events is possible if the memory is full • Retention period is set by authorised Gateway Administrator on request by consumer, data older than this are deleted.	• The availability of data has to be ensured over the lifetime of the TOE.

Table 8: Overview over audit processes

6.2.2 Security Requirements for the System Log

6.2.2.1 Security audit automatic response (FAU_ARP)

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

FAU_ARP/SYS.1 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

6.2.2.2 Security audit data generation (FAU_GEN)

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

FAU_GEN/SYS.1.1 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/SYS.1.2 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

6.2.2.3 Security audit analysis (FAU_SAA)

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

FAU_SAA/SYS.1.1 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/SYS.1.2 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 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/SYS.1.

6.2.2.4 Security audit review (FAU_SAR)

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

FAU_SAR/SYS.1.1 The TSF shall provide [*only authorised Gateway Administrators via the IF_GW_WAN interface*] with the capability to read [*all information*] from the **system** audit records.

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

Hierarchical to: No other components

Dependencies: FAU_GEN.1

6.2.2.5 Security audit event storage (FAU_STG)

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

FAU_STG/SYS.4.1 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 The size of the audit trail that is available before the oldest events get overwritten is configurable for the Gateway Administrator.

6.2.3 Security Requirements for the Consumer Log

6.2.3.1 Security audit data generation (FAU_GEN)

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

FAU_GEN/CON.1.1 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 9 and* [assignment: ***additional events or none***]].

FAU_GEN/CON.1.2 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 9*].

Hierarchical to: No other components

Dependencies: FPT_STM.1

Application Note The possibility for the ST author to specify additional events in FAU_GEN/CON.1.1 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 need to be audited for a specific TOE.

Event	Additional Information
Any change to an access control profile	The new and the old value of the profile
Any submission of Meter Data to an external entity	The access control 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 9: Events for consumer log

6.2.3.2 Security audit review (FAU_SAR)

6.2.3.2.1 FAU_SAR/CON.1 Audit Review for consumer log

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

FAU_SAR/CON.1.2 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: FAU_SAR/CON.1.2 shall ensure that the consumer is able to interpret the information that is provided to him in a way that allows him to verify the invoice.

6.2.3.3 Security audit event storage (FAU_STG)

6.2.3.3.1 FAU_STG/CON.2: Guarantees of audit data availability for the consumer log

FAU_STG/CON.2.1 The TSF shall protect the stored audit records in the **consumer** audit trail from unauthorised deletion.

FAU_STG/CON.2.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the **consumer** audit trail.

FAU_STG/CON.2.3 The TSF shall ensure that [*a sufficient amount of*] stored **consumer** 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 The ST author may consider the regulations from [PTB_A50.7] in order to decide about the amount of information that needs to be available for the requirement in FAU_STG/CON.2.3.

876 6.2.4 Security Requirements for the Calibration Log

877 6.2.4.1 Security audit data generation (FAU_GEN)

878 *6.2.4.1.1 FAU_GEN/CAL.1: Audit data generation for calibration log*

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*all calibration-relevant information*].

FAU_GEN/CAL.1.2 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, [*other audit relevant information*].

Hierarchical to: No other components

Dependencies: FPT_STM.1

879

Application Note 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/CAL.1.1 and FAU_GEN/CAL.1.2 are left open to the ST author. The ST author is motivated to seek the guidance of the relevant national authority before deciding about those requirements.

880 6.2.4.2 Security audit review (FAU_SAR)

881 *6.2.4.2.1 FAU_SAR/CAL.1: Audit Review for calibration log*

FAU_SAR/CAL.1.1 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/CAL.1.2 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

882

883 **6.2.4.3 Security audit event storage (FAU_STG)**

884 *6.2.4.3.1 FAU_STG/CAL.4: Prevention of audit data loss for calibration log*

FAU_STG/CAL.4.1 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: 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 to choose a sufficient size so that the calibration log cannot become full.

885 6.2.5 Security Requirements that apply to all logs

886 **6.2.5.1 Security audit data generation (FAU_GEN)**

887 *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

888

Application Note: Please note that FAU_GEN.2 applies to both audit logs, the system log as well as the consumer log.

889 **6.2.5.2 Security audit event storage (FAU_STG)**

890 *6.2.5.2.1 FAU_STG.1: Protected audit trail storage for all logs*

FAU_STG.1.1 The TSF shall protect the stored audit records in ~~**the**~~ **all** audit trail**s** from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in ~~**the**~~ **all** audit trail**s**.

Hierarchical to: No other components

Dependencies: FAU_GEN.1

891

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*[37]] 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-3109*].

Hierarchical to: FCO_NRO.1 Selective proof of origin

Dependencies: FIA_UID.1 Timing of identification

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

To do so a hash value has to be created by the TOE over the Data To Be Signed (DTBS) as defined in FCS_COP/HASH.1. 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/TLS.1: Cryptographic key generation for TLS

FCS_CKM/TLS.1.1 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: [*Annex A of [BSI-TR-3109]*].

Hierarchical to: No other components.

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

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

FCS_CKM.4 Cryptographic key destruction

900

Application Note: As required by the SFR, the TOE *shall only* use cryptographic specifications and algorithms that are described in Annex A of [BSI-TR-3109].

Please note that the Security Module is used for parts of the TLS key negotiation.

901 6.4.1.2 Cryptographic operation (FCS_COP)

902 *6.4.1.2.1 FCS_COP/TLS.1: Cryptographic operation for TLS*

FCS_COP/TLS.1.1 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: [*Annex A of [BSI-TR-3109]].*

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/TLS.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

903

Application Note: As required by the SFR, the TOE *shall only* use cryptographic specifications and algorithms that are described in Annex A of [BSI-TR-3109].

904

905 6.4.2 Cryptographic support for PKCS

906 6.4.2.1 Cryptographic key management (FCS_CKM)

907 *6.4.2.1.1 FCS_CKM/PKCS.1: Cryptographic key generation for PKCS*

908

FCS_CKM/PKCS.1.1 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: [*Annex A of [BSI-TR-3109]*].

Hierarchical to: No other components.

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

Application Note: Please note that the TOE utilises the services of its Security Module for parts of the key generation procedure.

Application Note: As required by the SFR, the TOE *shall only* use cryptographic specifications and algorithms that are described in Annex A of [BSI-TR-3109].

6.4.2.2 Cryptographic operation (FCS_COP)

6.4.2.2.1 FCS_COP/PKCS.1: Cryptographic operation for PKCS#7

FCS_COP/PKCS.1.1 The TSF shall perform [*AES 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: [*Annex A of [BSI-TR-3109]*].

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/PKCS.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Application Note: As required by the SFR, the TOE *shall only* use cryptographic specifications and algorithms that are described in Annex A of [BSI-TR-3109].

6.4.3 Cryptographic support for Meter communication encryption

6.4.3.1 Cryptographic operation (FCS_COP)

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

FCS_COP/MTR.1.1 The TSF shall perform [*AES and 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: [*Annex A of [BSI-TR-3109]*].

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/TLS.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Application Note: Other than for the requirements in the previous chapters this PP does not contain dedicated requirements on key generation for Meter communication encryption. The reason for this is twofold:

1) If a TLS encryption is used the key generation/negotiation is as defined by FCS_CKM/TLS.1
2) If AES encryption is used the key has been brought into the Gateway via a management function during the pairing process for the Meter (See FMT_SMF.1)

Application Note: The communication between a physically separated Meter and the TOE can either be secured by the use of a symmetric AES encryption or by a TLS channel. As the TOE shall be interoperable with all kind of Meters FCS_COP/MTR.1 requires the implementation of both kinds of encryption.

Application Note: As required by the SFR, the TOE *shall only* use cryptographic specifications and algorithms that are described in Annex A of [BSI-TR-3109].

6.4.4 General Cryptographic support

6.4.4.1 Cryptographic key management (FCS_CKM)

6.4.4.1.1 FCS_CKM.4: Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [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/TLS.1 Cryptographic key generation]

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

6.4.4.2 Cryptographic operation (FCS_COP)

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

FCS_COP/HASH.1.1 The TSF shall perform [*hashing for signature creation and verification*] in accordance with a specified cryptographic algorithm [*SHA-256*] and cryptographic key sizes [*none*] that meet the following: [*Annex A of [BSI-TR-3109]]*

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/TLS.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

Application Note: 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: As required by the SFR, the TOE *shall only* use cryptographic specifications and algorithms that are described in Annex A of [BSI-TR-3109].

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

FCS_COP/MEM.1.1 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: [*Annex A of [BSI-TR-3109]]*

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/TLS.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

Application Note: Please note that the key generation functionality as defined by FCS_CKM/PKCS.1 can be used for this functionality as well.

Application Note: 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 encrypt the symmetric key that is used for the encryption of TSF and user data.

It shall be noted that this kind of encryption cannot provide an absolute protection against physical manipulation and does not aim to. It however contributes to the security concept that considers the protection that is provided by the environment.

6.5 Class FDP: User Data Protection

6.5.1 Introduction to the Security Functional Policies

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

- The Gateway access SFP is an access control policy to control the access to objects under the control of the TOE. The details of this access control policy highly depend on the concrete application a TOE and are therefore left to the ST author.
- The Firewall SFP implements an information flow policy to fulfil the objective O.Firewall. All requirements around the communication control that the TOE poses on communications between the different networks are defined in this policy.
- The Meter SFP implements an information flow policy to fulfil the objective O.Meter. It defines all requirements concerning how the TOE shall handle Meter Data.

6.5.2 Gateway Access SFP

6.5.2.1 Access control policy (FDP_ACC)

6.5.2.1.1 FDP_ACC.2: Complete access control

FDP_ACC.2.1 The TSF shall enforce the [*Gateway access SFP*] on [assignment: *list of subjects and objects*] and all operations among subjects and objects covered by the SFP.

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

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

6.5.2.1.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [*Gateway access SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

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: [*nobody must be allowed to read the symmetric keys used for encryption*].

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

6.5.3 Firewall SFP

6.5.3.1 Information flow control policy (FDP_IFC)

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

FDP_IFC/FW.2.1 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/FW.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

6.5.3.3 Information flow control functions (FDP_IFF)

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

FDP_IFF/FW.1.1 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), access control profile, destination_authenticated].

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

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

[assignment: other rules or none]].

FDP_IFF/FW.1.3 The TSF shall enforce the [*TOE shall establish a connection to a configured external party in the WAN after having received a wake-up message on the WAN interface*].

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

FDP_IFF/FW.1.5 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: It should be noted that the FDP_IFF/FW.1.1 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: The assignment in FDP_IFF/FW.1.2 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.

6.5.4 Meter SFP

6.5.4.1 Information flow control policy (FDP_IFC)

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

FDP_IFC/MTR.2.1 The TSF shall enforce the [*Meter SFP*] on [t*he TOE, attached Meters 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/MTR.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

6.5.4.2 Information flow control functions (FDP_IFF)

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

FDP_IFF/MTR.1.1 The TSF shall enforce the [*Meter SFP*] based on the following types of subject and information security attributes: [

s*ubjects: The TOE and external entities on the WAN or LMN side*

information: any information that is sent via the TOE

attributes: destination interface, source interface (LMN or WAN), access control profile

].

FDP_IFF/MTR.1.2 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 access control profile*].

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

- *Data received from Meters shall be processed as defined in the corresponding access control profiles,*
- *Results of processing of Meter Data shall be submitted to external parties as defined in the access control 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*[38] *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[39] *and*

      inform a Gateway Administrator].

FDP_IFF/MTR.1.4 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/MTR.1.5 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 that are not within the physical scope*[40] *of the TOE 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

961

Application Note: 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 PTB would be a good example for such a source[41])). 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

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

[39] 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.

[40] This description refers to a wired or optical connection in a One-Box Solution

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

For the question whether a deviation between the time source(s) in the WAN and the local system time is still acceptable, normative or legislative regulations shall be considered. If no regulation exists, a maximum deviation of 3% of the measuring period is allowed to be in conformance with 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: In FDP_IFF/MTR.1.5 the TOE is required to verify the authenticity, integrity and confidentiality of the Meter Data received by the Meter if the Meter is not implemented in the same physical device. 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/TLS.1.
2. To accept, decrypt and verify data that has been encrypted by the Meter using a 128bit AES. In this case the ST author shall add an appropriate SFR to describe the cryptographic functionality to their ST.

6.5.5 General Requirements on user data protection

6.5.5.1 Residual information protection (FDP_RIP)

6.5.5.1.1 FDP_RIP.2: Full residual information protection

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

Hierarchical to: FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

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

Please further note that this SFR has been used in order to ensure that information that is not longer used is made unavailable from a logical perspective. Specifically, it has to be ensured that this information is not longer available via an external interface (even if an access control or information flow policy would fail). However, this does not necessarily mean that the information is overwritten in a way that makes it impossible for an attacker to get access to is assuming a physical access to the memory of the TOE.

6.5.5.2 Stored data integrity (FDP_SDI)

6.5.5.2.1 FDP_SDI.2: Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [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: 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.

6.6 Class FIA: Identification and Authentication

6.6.1 User Attribute Definition (FIA_ATD)

6.6.1.1 FIA_ATD.1: User attribute definition

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

- *User Identity*
- *Status of Identity (Authenticated or not)*
- *Connecting network (WAN, HAN or LMN)*
- *Role membership*
- *[assignment: list of security attributes or none]*].

Hierarchical to: No other components.

Dependencies: No dependencies.

6.6.2 Authentication Failure handling (FIA_AFL)

6.6.2.1 FIA_AFL.1: User authentication before any action

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

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

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1 Timing of identification

6.6.3 User Authentication (FAI_UAU)

6.6.3.1 FIA_UAU.2: User authentication before any action

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	FIA_UAU.1
Dependencies:	FIA_UID.1 Timing of identification
Application Note:	It is essential for the security of the TOE that each user has been successfully authenticated before allowing any actions on behalf of that user. For consumer authentication (i.e. the authentication of a local consumer) the TOE shall implement an authentication mechanism. For authentication based on cryptographic means (specifically for the authentication of external parties in the WAN) the TOE may re-use a previous authentication result of its Security Module. Please refer to [BSI-TR-3109] for a more detailed overview on the authentication of consumers.

6.6.3.2 FIA_UAU.6: Re-authenticating

FIA_UAU.6.1	The TSF shall re-authenticate **an external entity** under the conditions [*after 1 hour*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application Note	This requirement specifically applies to the key material that is used for TLS communication with external parties in the WAN. The TLS channel shall be disconnected and rebuild after 1 hour.

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 10*].

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_U.
All other management functions as defined in FMT_SMF.1	The management functions must only be accessible for an authorised Gateway Administrator and only via the interface IF_GW_WAN[42].
Firmware Update	The firmware update must only be possible after the authenticity of the firmware update has been verified (using the services of the Security Module and the trust anchor of the Gateway developer) and if the version number of the new firmware is higher or equal to the version of the installed firmware.
Deletion of events from the Calibration Log	A deletion of events from the calibration log must not be possible.

Table 10: Restrictions on Management Functions

6.7.1.2 Specification of Management Functions (FMT_SMF)

6.7.1.2.1 FMT_SMF.1: Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*list of management functions as defined in Table 11 and Table 12 and [assignment: additional functionalities]*].

Hierarchical to: No other components.

Dependencies: No dependencies.

SFR	Management functionality
FAU_ARP/SYS.1	the management (addition, removal, or modification) of actions.
FAU_GEN/SYS.1	-
FAU_SAA/SYS.1	maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.
FAU_SAR/SYS.1 FAU_SAR/CON.1 FAU_SAR/CAL.1	maintenance (deletion, modification, addition) of the group of consumer with read access right to the audit records.
FAU_STG/SYS.4 FAU_STG/CAL.4	• maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure. • Administration of the size of the audit trail for consumer and system log
FAU_STG/CON.2	maintenance of the parameters that control the audit storage capability.

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

SFR	Management functionality
FAU_GEN/CON.1	-
FAU_GEN/CAL.1	-
FAU_GEN.2	-
FAU_STG.1	-
FCO_NRO.2	The management of changes to information types, fields, originator attributes and recipients of evidence.
FCS_CKM/TLS.1	-
FCS_COP/TLS.1	-
FCS_CKM/PKCS.1	-
FCS_COP/PKCS.1	-
FCS_CKM.4	-
FCS_COP/HASH.1	-
FCS_COP/MEM.1	-
FDP_ACC.2	·
FDP_ACF.1	Managing the attributes used to make explicit access or denial based decisions.
FDP_IFF/FW.1	• 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.
FDP_IFC/FW.2	-
FDP_IFF/MTR.1	Managing the attributes (including access control profiles) used to make explicit access based decisions.
FDP_IFC/MTR.2	-
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	• 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; • management of the authentication data by the user associated with this data.

SFR	Management functionality
FIA_UAU.6	- [43]
FIA_UID.2	the management of the user identities.
FIA_USB.1	• an authorised Gateway Administrator can define default subject security attributes. • an authorised Gateway Administrator can change subject security attributes.
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/AC.1	• managing the group of roles that can interact with the security attributes; • management of rules by which security attributes inherit specified values.
FMT_MSA/AC.3	• managing the group of roles that can specify initial values; • managing the permissive or restrictive setting of default values for a given access control SFP; • management of rules by which security attributes inherit specified values.
FMT_MSA/FW.1	• managing the group of roles that can interact with the security attributes; • management of rules by which security attributes inherit specified values.
FMT_MSA/FW.3	• managing the group of roles that can specify initial values; • managing the permissive or restrictive setting of default values for a given access control SFP; • management of rules by which security attributes inherit specified values.
FMT_MSA/MTR.1	• managing the group of roles that can interact with the security attributes; • management of rules by which security attributes inherit specified values.
FMT_MSA/MTR.3	• managing the group of roles that can specify initial values; • managing the permissive or restrictive setting of default values for a • given access control SFP; • management of rules by which security attributes inherit specified values.

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

SFR	Management functionality
FPR_CON.1	Definition of the interval in FAU_CON.1.2 if definable within the operational phase of the TOE
FPR_PSE.1	-
FPT_FLS.1	-
FPT_RPL.1	-
FPT_STM.1	management of the time.
FPT_TST.1	• management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions; • management of the time interval if appropriate.
FPT_PHP.1	• management of the user or role that determines whether physical tampering has occurred.
FTP_ITC/WAN.1	- [44]
FTP_ITC/MTR.1	- [44]
FTP_ITC/USR.1	- [44]

Table 11: 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 parties in the WAN for communication
Resetting of the TOE[45]

Table 12: Gateway specific Management Functionalities

6.7.2 Security management roles (FMT_SMR)

6.7.2.1 FMT_SMR.1: Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [

[44] 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.

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

authorised consumer
authorised Gateway Administrator
[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: The roles “authorised Gateway Administrator” 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.

6.7.3 Management of security attributes for gateway access SFP

6.7.3.1 Management of security attributes (FMT_MSA)

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

FMT_MSA/AC.1.1 The TSF shall enforce the [*Gateway access 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]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

FMT_MSA/AC.3.1 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/AC.3.2 The TSF shall allow the [*no role*] to specify alternative initial values to override the default values when an object or information is created.

Hierarchical to: No other components.

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

6.7.4 Management of security attributes for Firewall SFP

6.7.4.1 Management of security attributes (FMT_MSA)

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

FMT_MSA/FW.1.1 The TSF shall enforce the [*Firewall 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]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

6.7.4.2 FMT_MSA/FW.3: Static attribute initialisation for Firewall policy

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

FMT_MSA/FW.3.2 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: The definition of restrictive default rules for the firewall information flow policy refers to the rules as defined in FDP_IFF/FW.1.2 and FDP_IFF/FW.1.5. Those rules apply to all information flows and must not be overwritable by anybody.

6.7.5 Management of security attributes for Meter SFP

6.7.5.1 Management of security attributes (FMT_MSA)

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

FMT_MSA/MTR.1.1 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]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

FMT_MSA/MTR.3.1 The TSF shall enforce the [*Meter SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

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

Hierarchical to: No other components.

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

6.8 Class FPR: Privacy

6.8.1 Communication Concealing (FPR_CON)

6.8.1.1 FPR_CON.1: Communication Concealing

FPR_CON.1.1 The TSF shall enforce the [*Firewall SFP*] in order to ensure that no PII 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: 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 not relevant for billing sent to parties in the WAN*].

FPR_PSE.1.2 The TSF shall be able to provide [*aliases as defined by the access control profiles*] **for the Meter identity** to [*external parties 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: When the TOE submits information about the consumption or production of a certain commodity that is not relevant for the billing process, 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.

6.9 Class FPT: Protection of the TSF

6.9.1 Fail secure (FPT_FLS)

6.9.1.1 FPT_FLS.1: Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TS*F].

Hierarchical to: No other components.

Dependencies: No dependencies.

6.9.2 Replay Detection (FPT_RPL)

6.9.2.1 FPT_RPL.1: Replay detection

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

6.9.3 Time stamps (FPT_STM)

6.9.3.1 FPT_STM.1: Reliable time stamps

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

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note: 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 (which will result in an inoperative TOE).

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.

6.9.4 TSF self test (FPT_TST)

6.9.4.1 FPT_TST.1: TSF testing

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

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note: The self test suite as defined in FPT_TST.1 shall also contain a test that tries to detect 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 failed.

6.9.4.2 FPT_PHP.1: Passive detection of physical attack

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note: 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 [PTB_A50.7].

6.10 Class FTP: Trusted path/channels

6.10.1 Inter-TSF trusted channel (FTP_ITC)

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

FTP_ITC/WAN.1.1 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/WAN.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

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

Hierarchical to: No other components

Dependencies: No dependencies.

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

FTP_ITC/MTR.1.1 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/MTR.1.2 The TSF shall permit [**selection: *the Meter, the TOE***] to initiate communication via the trusted channel.

FTP_ITC/MTR.1.3 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: It should be noted that the requirement of an Inter-TSF trusted channel for Meter Data may be also be fulfilled by physical means. The classical example is an implementation in which the Meter and the Gateway are implemented within one physical device. Please also refer to chapter 1.4.5.3.

If the channel is implemented by cryptographic means the correspoding cryptographic primitives are defined by FCS_COP/MTR.1.

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

FTP_ITC/USR.1.1 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/USR.1.2 The TSF shall permit [**the consumer**] to initiate communication via the trusted channel.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note: Please note that the requirement on a trusted channel for the user interface e implicitly fulfilled for the case that the user interface is implemented via a local display at the TOE.

6.11 Security Assurance Requirements for the TOE

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

The following table lists the assurance components which are therefore applicable to this 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
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	**AVA_VAN.5**

Table 13: Assurance Requirements

6.12 Security Requirements rationale

6.12.1 Security Functional Requirements rationale

6.12.1.1 Fulfilment of the Security Objectives

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

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

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access
FCS_CKM.4					X					
FCS_COP/HASH.1					X					
FCS_COP/MEM.1					X		X			
FDP_ACC.2										X
FDP_ACF.1										X
FDP_IFC/FW.2	X	X								
FDP_IFF/FW.1	X	X								
FDP_IFC/MTR.2				X		X				
FDP_IFF/MTR.1				X		X				
FDP_RIP.2							X			
FDP_SDI.2							X			
FIA_ATD.1								X		
FIA_AFL.1								X		
FIA_UAU.2								X		
FIA_UAU.6					X					
FIA_UID.2								X		
FIA_USB.1								X		
FMT_MOF.1								X		
FMT_SMF.1								X		
FMT_SMR.1								X		
FMT_MSA/AC.1								X		
FMT_MSA/AC.3								X		
FMT_MSA/FW.1								X		
FMT_MSA/FW.3								X		
FMT_MSA/MTR.1								X		
FMT_MSA/MTR.3								X		

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access
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/WAN.1	X									
FTP_ITC/MTR.1				X						
FTP_ITC/USR.1									X	

Table 14: 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/FW.2** defines that the TOE shall implement an information flow policy for its firewall functionality.
- **FDP_IFF/FW.1** defines the concrete rules for the firewall information flow policy.

6.12.1.1.2 O.SeparateIF

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

- **FDP_IFC/FW.2** and **FDP_IFF/FW.1** implicitly require the TOE to implement physically separate ports for WAN and LMN.
- **FPT_TST.1** implements a self test that also tries to detect 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/MTR.2** and **FDP_IFF/MTR.1** define an information flow policy to introduce how the Gateway shall handle Meter data.
- **FCO_NRO.2** ensure that all Meter data will be signed by the Gateway (invoking the services of its security module) before being submitted to external parties.
- **FPR_PSE.1** defines requirements around the pseudonymization of Meter identities for Status data.
- **FTP_ITC/MTR.1** 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/TLS.1** defines the requirements on key negotiation for the TLS protocol.
- **FCS_CKM/PKCS.1** defines the requirements on key generation for symmertic encrytpion within PKCS#7.
- **FCS_COP/TLS.1** defines the requirements around the encryption and decryption capabilities of the Gateway for communications with external parties in the WAN and (if not implemented in one physical device) to Meters.
- **FCS_COP/PKCS.1** defines the requirements around the encryption and decryption of content data.
- **FCS_COP/MTR.1** defines the cryptographic primitives for meter communication encryption.
- **FCS_COP/HASH.1**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/MEM.1** defines the requirements around the encryption of TSF data.
- **FIA_UAU.6** ensure that external parties in the WAN are re-authenticated after the session key has been used for a certain amount of time.
- **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/MTR.2** and **FDP_IFF/MTR.1** 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/MEM.1** defines that the TOE shall encrypt its TSF and user data as long as it is not in use.
- **FDP_RIP.2** defines that the TOE shall make information unavailable as soon as it is not longer needed.

- **FDP_SDI.2** defines requirements around the integrity protection for stored data.
- **FPT_FLS.1** defines requirements that the TOE falls back to a safe state for specific error cases.
- **FPT_TST.1** defines the self testing functionality.
- **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/AC.1** defines requirements around the limitations for management of attributes used for the Gateway access SFP.
- **FMT_MSA/FW.1** defines requirements around the limitations for management of attributes used for the Firewall SFP.
- **FMT_MSA/MTR.1** defines requirements around the limitations for management of attributes used for the Meter SFP.
- **FMT_MSA/AC.3**defines the default values for the Gateway access SFP.
- **FMT_MSA/FW.3** defines the default values for the Firewall SFP.
- **FMT_MSA/MTR.3** 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/SYS.1**. **FAU_ARP/SYS.1** and **FAU_SAA/SYS.1** allow to define a set of criteria for automated analysis of the audit and a corresponding response. **FAU_SAR/SYS.1** 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. Finally, **FAU_STG/SYS.4** 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/CON.1**. **FAU_STG/CON.2** defines the requirements on what should happen if the audit log is full. **FAU_SAR/CON.1** 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_U interface. **FTP_ITC/USR.1**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/CAL.1.** **FAU_STG/CAL.4** defines the requirements on what should happen if the audit log is full. **FAU_SAR/CAL.1** 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_U interface.

FAU_GEN.2, FAU_STG.1 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.

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/SYS.1	FAU_SAA.1 Potential violation analysis	FAU_SAA/SYS.1
FAU_GEN/SYS.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAA/SYS.1	FAU_GEN.1 Audit data generation	FAU_GEN/SYS.1
FAU_SAR/SYS.1	FAU_GEN.1 Audit data generation	FAU_GEN/SYS.1
FAU_STG/SYS.4	FAU_STG.1 Protected audit trail storage	FAU_STG.1
FAU_GEN/CON.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAR/CON.1	FAU_GEN.1 Audit data generation	FAU_GEN/CON.1
FAU_STG/CON.2	FAU_GEN.1 Audit data generation	FAU_GEN/CON.1
FAU_GEN/CAL.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAR/CAL.1	FAU_GEN.1 Audit data generation	FAU_GEN/CAL.1
FAU_STG/CAL.4	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/SYS.1 FAU_GEN/CON.1 FIA_UID.2
FAU_STG.1	FAU_GEN.1 Audit data generation	FAU_GEN/SYS.1 FAU_GEN/CON.1 FAU_GEN/CAL.1
FCO_NRO.2	FIA_UID.1 Timing of identification	FIA_UID.2
FCS_CKM/TLS.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP/TLS.1 FCS_CKM.4

SFR	Dependencies	Fulfilled by
FCS_COP/TLS.1	[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/TLS.1 FCS_CKM.4
FCS_CKM/PKCS.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP/TLS.1 FCS_CKM.4
FCS_COP/PKCS.1	[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/PKCS.1 FCS_CKM.4
FCS_COP/MTR.1	[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/TLS.1 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/TLS.1
FCS_COP/HASH.1	[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/MEM.1	[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/PKCS.1 FCS_CKM.4
FDP_ACC.2	FDP_ACF.1 Security attribute based access control	FDP_ACF.1

SFR	Dependencies	Fulfilled by
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.2 FMT_MSA/AC.3
FDP_IFC/FW.2	FDP_IFF.1 Simple security attributes	FDP_IFF/FW.1
FDP_IFF/FW.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC/FW.2 FMT_MSA/FW.3
FDP_IFC/MTR.2	FDP_IFF.1 Simple security attributes	FDP_IFF/MTR.1
FDP_IFF/MTR.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC/MTR.2 FMT_MSA/MTR.3
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.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/AC.1	[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/AC.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA/AC.1 FMT_SMR.1
FMT_MSA/FW.1	[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/WAN.2 FMT_SMR.1 FMT_SMF.1
FMT_MSA/FW.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA/FW.1 FMT_SMR.1

SFR	Dependencies	Fulfilled by
FMT_MSA/MTR.1	[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/MTR.2 FMT_SMR.1 FMT_SMF.1
FMT_MSA/MTR.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA/MTR.1 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/WAN.1	-	-
FTP_ITC/MTR.1	-	-
FTP_ITC/USR.1	-	-

Table 15: SFR Dependencies

6.12.1.3 Justification for missing dependencies

The hash algorithm as defined in FCS_COP/HASH.1 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 developers side, specifically for such a new technology.

6.12.2.1 Dependencies of assurance components

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

7. Appendix

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
Gateway Operator	Betreiber der Kommunikationseinheit
Grid	Netz (für Strom/Gas/Wasser)
Grid Status Data	Zustandsdaten des Versorgungsnetzes
LAN, Local Area Network	Lokales Netz (für Kommunikation)
LMN, Local Metrological Network	Lokales Messeinrichtungsnetz
Meter	Messeinrichtung (Teil eines Messsystems)
Meter Operator	Betreiber der Messeinrichtung (Messstellenbetreiber)
Security Module	Sicherheitsmodul (z.B. eine Smart Card)
Service Provider	Diensteanbieter
Smart Meter Smart Metering System[46]	Intelligente, in ein Kommunikationsnetz eingebundene, elektronische Messeinrichtung (Messsytem)
TOE	EVG (Evaluierungsgegenstand)
WAN, Wide Area Network	Weitverkehrsnetz (für Kommunikation)

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])

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

Term	Description
CA	Certificate Authority or Certification Authority, an entity that issues digital certificates.
CLS config (secondary asset)	See chapter 3.2
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 Operator	See chapter 3.1
Gateway time	See chapter 3.2
Grid Operator	See chapter 3.1
Home Area Network (HAN)	In-house LAN which interconnects domestic equipment and can be used for energy management purposes. (according to [CEN])
Independent Service Provider	Company independent of grid operators, supply companies and metering companies that uses an infrastructure which supports smart metering (according to [CEN])
Integrity	property that sensitive data has not been modified or deleted in an unauthorised and undetected manner (according to [SD_6])
IT-System	Computersystem
LAN	Local Area Network
Local attacker	See chapter 3.4
Meter Admin	See chapter 3.1
Meter config (secondary asset)	See chapter 3.2
Meter Data	See chapter 3.2
Meter Data	Entity which offers services to aggregate metering data by grid supply point

Term	Description
Aggregator (MDA)	on a contractual basis. NOTE: The contract is with a supplier. The aggregate is of all that supplier's consumers connected to that particular grid supply point. The aggregate may include both metered data and data estimated by reference to standard load profiles (adopted from [CEN])
Meter Data Collector (MDC)	Entity which offers services on a contractual basis to collect metering data related to a supply and provide it in an agreed format to a data aggregator (that can also be the DNO). NOTE: The contract is with a supplier or a pool. The collection may be carried out by manual or automatic means. ([CEN])
Meter Data Management System (MDMS)	System for validating, storing, processing and analyzing large quantities of meter data. ([CEN])
Meter Operator	See chapter 3.1
Metrological Area Network	In-house LAN which interconnects metrological equipment (i.e. Meters) and can be used for energy management purposes. (according to [CEN])
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.
PKCS	Public-Key Cryptography Standards
Producer	See chapter 3.1
Profile Provider	See chapter 3.1
Supplier	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

[BSI-TR-3109] BSI TR-03109 Anforderungen an die Interoperabilität der

Kommunikationseinheit eines Messsystems

[CC] Common Criteria for Information Technology Security Evaluation –

- Part 1: Introduction and general model, dated July 2009, version 3.1, Revision 3
- Part 2: Security functional requirements, dated July 2009, version 3.1, Revision 3
- Part 3: Security assurance requirements, dated July 2009, version 3.1, Revision 3

equivalent to

- ISO/IEC 15408-1:2009
- ISO/IEC 15408-2:2008
- ISO/IEC 15408-3:2008

[CEM] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated July 2009, version 3.1 Revision 3

(equivalent to ISO/IEC 18045:2008)

[PP_SM] Common Criteria Protection Profile for a Security Module for Smart Metering Systems.

[CEN] SMART METERS CO-ORDINATION GROUP (SM-CG) Item 5. M/441 first phase deliverable – Communication – Annex: Glossary (SMCG/Sec0022/DC)

[PTB_A50.7] Anforderungen an elektronische und software-gesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme, PTB-A 50.7, April 2002

[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