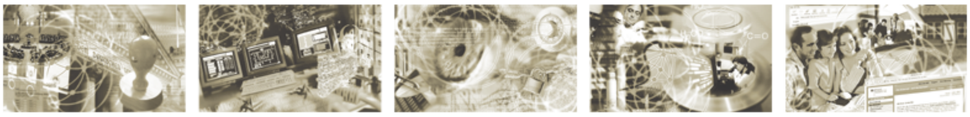
Federal Office
for Information Security



Protection Profile for the Security Module of a Smart Meter Mini-HSM (Mini-HSM Security Module PP)

Schutzprofil für das Sicherheitsmodul des Smart Meter Mini-HSM

Common Criteria

Mini-HSM SecMod-PP

Version 1.0 – 23 June 2017

Certification-ID BSI-CC-PP-0095

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: https://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 consumer's side and allows sending the information about the consumption or production to external entities, which is then the basis for e.g. billing the consumption or production. The central communication component of such a Smart Metering System (please refer to chapter 1.4.2 for a more detailed overview) is a Gateway that connects to the LAN of the consumer and the outside world. The Gateway collects, processes and stores the records from Meter(s) and ensures that only authorised parties have access to them or derivatives thereof. Relevant information will be signed and encrypted before sending using the cryptographic services of a Security Module, which is embedded as an integral part into a Gateway and switches the Gateway to a Smart Meter Gateway.

For cryptographic support of the different parties in a Smart Metering System that communicate with the Smart Meter Gateway (and its integrated Security Module), that communicate among themselves or that are involved in the development and production processes of a Smart Meter Gateway the so-called Smart Meter Mini-HSM[3] with an own integrated Security Module can be used. Such Smart Meter Mini-HSM is connected from technical point of view to an Application Server via which the Mini-HSM User can invoke and use the needed cryptographic services from the Security Module integrated in the Smart Meter Mini-HSM.

---

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 The term “Smart Meter Mini-HSM” is chosen to indicate that such technical component can be considered as a small, specific variant of a hardware security module (HSM) in the common sense.

Examples for the usage of the Smart Meter Mini-HSM:

For its personalisation and normal usage, the Smart Meter Gateway and its own integrated Security Module have to be administrated accordingly by the Gateway Administrator via WAN connection. For these issues, the Gateway Administrator can make use of the Smart Meter Mini-HSM that supports the Gateway Administrator for his specific tasks and cryptographic needs and provides certain cryptographic services that can be invoked and used by the Gateway Administrator for his administration tasks.

The Smart Meter Mini-HSM may as well be used by the Gateway Administrator as cryptographic service provider for his communication with the so-called Authorized External Entity (Autorisierter Externer Marktteilnehmer, EMT for short in the following) as e.g. a Metering Service Provider.

Furthermore, in the framework of normal usage of the Smart Meter Gateway the EMT may communicate via WAN connection with the Smart Meter Gateway or the Gateway Administrator for different specific purposes. For cryptographic support, such an entity can as well make use of a Smart Meter Mini-HSM with its integrated Security Module and invoke the needed cryptographic services.

Last but not least, the Gateway Developer may make use of the Smart Meter Mini-HSM in the framework of his development and production processes, e.g. concerning PKI-related tasks.

This Protection Profile defines the security objectives and corresponding security requirements for the Security Module (TOE) that is integrated as central cryptographic unit in the Smart Meter Mini-HSM. Such Smart Meter Mini-HSM with integrated Security Module is then intended to be used by the Mini-HSM User via the connected Application Server for cryptographic support.

The Target of Evaluation (TOE) described in this document is a Security Module as an electronic unit comprising hardware and software that is integrated in the Smart Meter Mini-HSM. Typically, a Security Module is realised in form of a smart card (but is not limited to that). The TOE or Smart Meter Mini-HSM integrating the TOE respectively provides central cryptographic services and serves as secure storage for cryptographic keys and further (sensitive) data as these are relevant for the Mini-HSM User in a Smart Metering System for his communication with other involved components or parties.

The Smart Meter Mini-HSM with its integrated Security Module (TOE) is intended to be used by the Application Server or the Mini-HSM User respectively as regular user of such Smart Meter Mini-HSM for their operation and support in a Smart Metering System. More detailed, the Smart Meter Mini-HSM with its integrated Security Module (TOE) serves as a cryptographic service provider for different cryptographic functionalities based on elliptic curve cryptography such as the generation and verification of digital signatures (e.g. for content data signature) and key agreement for TLS and content data encryption. The Security Module of the Smart Meter Mini-HSM contains the cryptographic identity of the Mini-HSM User, and it serves as a reliable source for random numbers as well as a secure storage for cryptographic keys and further (sensitive) data.

The PP is directed to developers of Smart Metering Systems and their related components and informs them about the security requirements that have to be implemented. It is further directed to stakeholders being responsible for purchasing Smart Metering Systems and their components.

1.2 PP Reference

Title:	Protection Profile for the Security Module of a Smart Meter Mini-HSM (Mini-HSM Security Module PP)
Version:	1.0
Date:	23 June 2017
Authors:	Bundesamt für Sicherheit in der Informationstechnik (BSI) / Federal Office for Information Security, Germany
Registration:	Bundesamt für Sicherheit in der Informationstechnik (BSI) / Federal Office for Information Security Germany
Certification-ID:	BSI-CC-PP-0095
Evaluation Assurance Level:	The assurance level for this PP is EAL 4 augmented by AVA_VAN.5.
CC Version:	V3.1 Revision 5
Keywords:	Smart Meter, Smart Metering System, Smart Meter Mini-HSM, Security Module, Gateway Administrator, Smart Meter Gateway, EMT, Gateway Developer, Protection Profile, 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 list of acronyms, a glossary and a mapping from English to German terms can be found in chapters 7.1 to 7.3.

Term	Definition	Source
Authorized External Entity (EMT)	So-called Autorisierter Externer Marktteilnehmer. External entity unlocked for communication with the Smart Meter Gateway.	[SM-CP]
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.	[PP 73]

Term	Definition	Source
Commodity	Electricity, gas, water or heat[4].	---
Consumer	End user or local producer of electricity, gas, water or heat (or other commodities).	[CEN]
Gateway Smart Meter Gateway	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 the Gateway). The Gateway is specified in [PP 73] 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. A Smart Meter Gateway is a Gateway that integrates a Security Module based on [TR-03109-2] and [PP 77].	---
HAN, Home Area Network	In-house data communication network which interconnects domestic equipment and can be used for energy management purposes.	[CEN], adopted
LAN, Local Area Network	Data communication network, connecting a limited number of communication devices (Meters and other devices) and covering a moderately sized geographical area within the premises of the consumer. In the context of this PP the term LAN is used as a hypernym for HAN and LMN.	[CEN], adopted
LMN, Local Metrological Network	In-house data communication network which interconnects metrological equipment.	---
Meter	The term Meter refers to a unit for measuring the consumption or production of a certain commodity with additional functionality. It collects consumption or production data and transmits these data to the gateway. As not all aspects of a Smart Meter according to [CEN] are implemented in the	[CEN], adopted

4 Please note that this list does not claim to be complete.

Term	Definition	Source
	descriptions within this document the term Meter is used. The Meter has to be able to encrypt and sign the data it sends and will typically deploy a Security Module for this. Please note that the term Meter refers to metering devices for all kinds of commodities.	
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[5] (such as quality data, events and alarms).	[CEN]
Security Module	Security Module that is utilised by the Smart Meter Gateway or by the Smart Meter Mini-HSM respectively for cryptographic support – e.g. realised in form of a smart card. The requirements for the Security Module of a Smart Meter Gateway are defined in [TR-03109-2] and [PP 77]. The requirements for the Security Module of a Smart Meter Mini-HSM are defined in [TR-03109-2 B] and in this PP.	---
Smart Meter Smart Metering Smart Metering System	The Smart Metering System consists of a Smart Meter Gateway that is connected to one or more meters. In addition, CLS (i.e. generation plants) may be connected with the Gateway for dedicated communication purposes.	---
User, external entity	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary.	[CC1]
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

5 Please note that these readings and data may require an explicit endorsement of the consumer.

1.4 TOE Overview

1.4.1 Introduction

The TOE as defined in this Protection Profile is the Security Module contained in the so-called Smart Meter Mini-HSM. Such Smart Meter Mini-HSM is intended to be used by different parties as cryptographic service provider in the framework of a Smart Metering System.

In the following chapters, the overall Smart Metering System will be described at first and afterwards the Smart Meter Mini-HSM with its integrated Security Module (TOE) itself.

1.4.2 Description of the Smart Metering System

The following figure provides an overview over the whole Smart Metering System from a purely functional perspective as needed for this PP.[6] Please note that the arrows of the interfaces within the Smart Metering System as shown in Figure 1 indicate the flow of information (which is bi-directional). However, it does not indicate that a communication flow can be initiated bi-directionally.

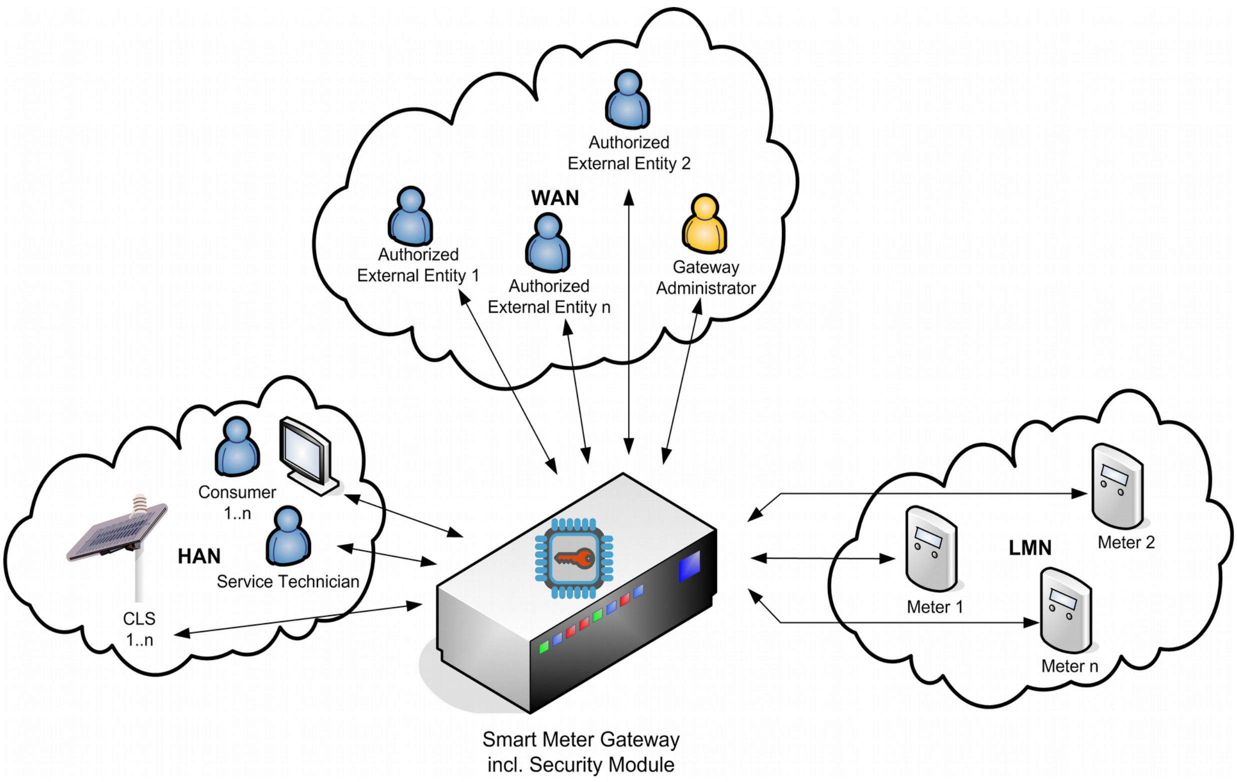


Figure 1: Smart Metering System

6 It should be noted that this description purely contains aspects that are relevant to motivate and understand the functionalities of the Smart Metering System and its components as far as needed for the present PP. It does not aim to provide a universal description of a Smart Metering System for all application cases.

As can be seen in Figure 1, a Smart Metering System comprises different functional units:

- The **Gateway** (as defined in [PP 73]) 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[7], the information will be signed and encrypted using the services of the Security Module that is integrated in the Gateway (see description below). The Gateway features a mandatory user interface, enabling authorised consumers to access the data relevant to them. The Gateways will be evaluated separately according to the requirements in the corresponding Protection Profile [PP 73].

  The Gateway utilises the services of an own **Security Module** as a cryptographic service provider for different cryptographic functionalities based on elliptic curve cryptography such as the generation and verification of digital signatures and key agreement which is used by the Gateway in the framework of TLS, content data signature and content data encryption. The Security Module contains the cryptographic identity of the Gateway, and it serves as a reliable source for random numbers as well as a secure storage for cryptographic keys and certificates. It is embedded into the Gateway and directly communicates with the Gateway. The administration of the Security Module is performed by the Gateway Administrator. An integrated Gateway consisting of the Gateway and its Security Module is called Smart Meter Gateway. The Security Module of the Smart Meter Gateway is addressed within the corresponding specification [TR-03109-2] and Protection Profile [PP 77].

- 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 their authenticity and integrity. The Meter is comparable to a classical meter[8] and has comparable security requirements; it will be sealed 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[9].

- **Controllable Local Systems** (CLS, as shown in Figure 1) 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.

1.4.3 Smart Meter Mini-HSM with integrated TOE in the Smart Metering System

As outlined in the preceding chapter 1.4.2, the Smart Meter Gateway (with its own integrated Security Module) is the central unit in the Smart Metering System that collects, processes and stores Meter Data and that communicates with external parties.

For cryptographic support of the different parties in a Smart Metering System that communicate with the Smart Meter Gateway (and its integrated Security Module), that

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

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

9 It should be noted that it is not implied 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.

communicate among themselves or that are involved in the development and production processes of a Smart Meter Gateway the so-called Smart Meter Mini-HSM with an own integrated Security Module can be used.

From a technical point of view, such Smart Meter Mini-HSM is connected to an appropriate Application Server. The Mini-HSM User can invoke the needed cryptographic services from the Security Module (TOE) integrated in the Smart Meter Mini-HSM via the Application Server. The components of the Smart Meter Mini-HSM beside the integrated TOE only provide power supply for the TOE and serve as a simple transport layer for the access of the Application Server to the TOE and its (security) functionality and for the transmission of communication data between the Application Server and the TOE.

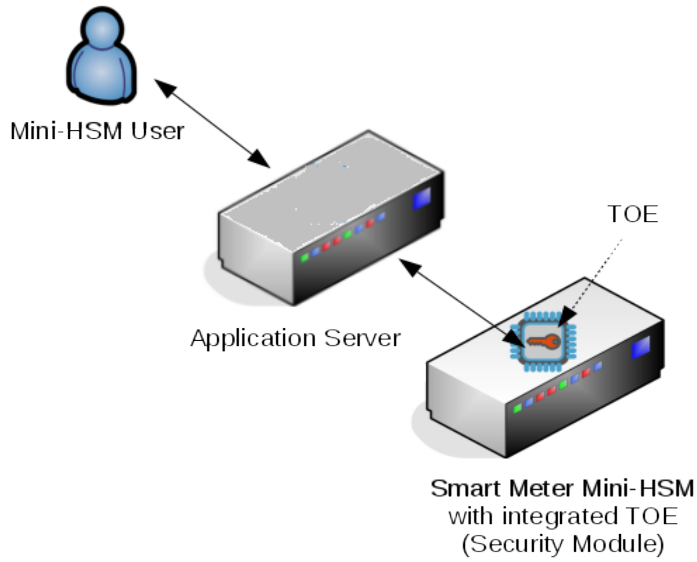


Figure 2: Smart Meter Mini-HSM

The Smart Meter Mini-HSM integrates a specific Security Module (TOE) as specified in [TR-03109-2 B]. Such Smart Meter Mini-HSM with its integrated Security Module serves in its operational phase as a cryptographic service provider for the Application Server or the Mini-HSM User respectively as regular user of the Smart Meter Mini-HSM and provides services in the following cryptographic areas:

- Digital Signature Generation,
- Digital Signature Verification,
- Key Agreement for TLS,
- Key Agreement for Content Data Encryption,
- Key Pair Generation,
- Random Number Generation,
- Component Authentication via the PACE Protocol with Negotiation of Session Keys,
- Secure Messaging, and
- Secure Storage of Key Material and further (sensitive) data relevant for the Application Server or the Mini-HSM User respectively and their communication with other components and parties involved in the Smart Metering System.

1.4.4 TOE Type

The Smart Meter Mini-HSM with its integrated Security Module (TOE) is a cryptographic service provider for the Application Server or the Mini-HSM User respectively as regular user of such Smart Meter Mini-HSM. The TOE's cryptographic functionality is provided in type of a hardware security module with appropriate software installed. The Smart Meter Mini-HSM with its integrated Security Module (TOE) supplies an external communication interface to the Application Server, so that the cryptographic service functionality provided by the TOE can be invoked and utilized by the Application Server via this interface. Moreover, the TOE serves as a secure storage for cryptographic keys and further (sensitive) data relevant for the Application Server or the Mini-HSM User respectively and their communication with other components and parties involved in the Smart Metering System.

1.4.5 TOE Physical Boundary

The TOE comprises the hardware and software that implement the security functionality of the Security Module as defined in [TR-03109-2 B] and in this PP.

Hint: The Security Module (TOE) is physically embedded into the Smart Meter Mini-HSM and is therefore in its integration and operational phase (refer for details to the description of phase 5 and 6 of the TOE life cycle model in chapter 1.5 and in [TR-03109-2 B]) protected by the same level of physical protection as assumed for and provided by the environment of the Smart Meter Mini-HSM within these two phases.

1.4.6 TOE Logical Boundary

The logical boundary of the Security Module (TOE) for a Smart Meter Mini-HSM can be defined by its major security functionality:

- Digital Signature Generation,
- Digital Signature Verification,
- Key Agreement for TLS,
- Key Agreement for Content Data Encryption,
- Key Pair Generation,
- Random Number Generation,
- Component Authentication via the PACE Protocol with Negotiation of Session Keys,
- Secure Messaging, and
- Secure Storage of Key Material and further (sensitive) data relevant for the Application Server or the Mini-HSM User respectively and their communication with other components and parties involved in the Smart Metering System.

All these security features are used by the Application Server or the Mini-HSM User respectively as regular user of such Smart Meter Mini-HSM with its integrated Security Module (TOE) in the operational phase to uphold the overall security of the Smart Metering System in general, and in particular of the Smart Meter Gateway that is handled by the Gateway Developer, that is administrated by the Gateway Administrator and that is communicated with by different parties.

The TOE and its (security) functionality is specified from a technical point of view in [TR-03109-2 B]. A detailed description of the (security) functionality provided by the TOE for use by the Application Server or the Mini-HSM User respectively as regular user of the Smart Meter Mini-HSM with such integrated Security Module (TOE) and in particular a detailed description of the Smart Meter Mini-HSM's and TOE's collaboration and interaction with the Application Server or the Mini-HSM User respectively can be found in [TR-03109-2 B].

This Protection Profile is written on the specification basis [TR-03109-2 B] for a Security Module intended to be integrated in the Smart Meter Mini-HSM, but is also applicable to a TOE conforming to an updated version of this specification if this update does not change the security functionality as specified in [TR-03109-2 B]. Please consult the certification body for further information related to the validity of the PP due to updates of the Security Module specification [TR-03109-2 B].

1.4.7 Interface of the TOE

Neither [TR-03109-2 B] nor this PP prescribe the technology for the communication between the Smart Meter Mini-HSM with its integrated Security Module (TOE) and the Application Server on the physical level.

In view of the Security Module (TOE), the components of the Smart Meter Mini-HSM beside the integrated TOE only provide power supply for the TOE and serve as a simple transport layer for the access of the Application Server to the TOE and its (security) functionality and for the transmission of communication data between the Application Server and the TOE.

On logical level the communication with the TOE follows the requirements outlined in [TR-03109-2 B] and is therefore oriented on [ISO 7816-4], [ISO 7816-8] and [ISO 7816-9].

1.4.8 Required non-TOE hardware/software/firmware

The TOE is the Security Module to be integrated in a Smart Meter Mini-HSM. Such Smart Meter Mini-HSM is intended to be used by the Application Server on behalf of the Mini-HSM User in a Smart Metering System.

The TOE is an independent product in the sense that it does not require any additional hardware, firmware or software to ensure its security. However, as the Security Module is physically embedded into the Smart Meter Mini-HSM and such Smart Meter Mini-HSM is connected to the Application Server the Security Module is in addition protected by the same level of environmental protection as assumed for and provided by the environment of the Smart Meter Mini-HSM and the Application Server.

In order to be powered up and to be able to communicate the TOE needs an appropriate device for power supply (here: Smart Meter Mini-HSM). For regular communication on logical level, the TOE requires a device (here: Application Server) whose implementation matches the TOE's interface specification, refer to [TR-03109-2 B]. Refer as well to chapter 1.4.7.

1.5 TOE Life Cycle Model

The TOE life cycle model is oriented on a life cycle model typically used for smart cards and similar devices and is adapated appropriately for the needs in the framework of Smart Metering Systems and in particular for the Smart Meter Mini-HSM that integrates the Security Module (TOE). Refer in addition to [TR-03109-2 B] where a detailed description of the overall life cycle of a Smart Meter Mini-HSM and its Security Module (TOE) can be found.

In detail, the TOE life cycle model covers the following life cycle phases:

Life Cycle Phase		Description
1	**Security Module Embedded Software Development**	The **Security Module Embedded Software Developer** is in charge of • the development of the Security Module Embedded Software of the TOE, • the development of the TOE related Application, and • the specification of the IC initialisation and pre-personalisation requirements. The purpose of the Security Module Embedded Software and Application designed and implemented during phase 1 is to control and protect the TOE during the following phases (product usage). The global security requirements of the TOE are such that it is mandatory during the development phase to anticipate the security threats of the other phases.
2	**IC Development**	The **IC Designer** • designs the IC, • develops the IC Dedicated Software, • provides information, software or tools to the Security Module Embedded Software Developer, and • receives the Security Module Embedded Software from the developer through trusted delivery and verification procedures (if applicable).
3	**IC Manufacturing, Packaging and Testing**	The **IC Manufacturer** and **IC Packaging Manufacturer** are responsible for producing the IC including • IC manufacturing, • IC pre-personalisation, • implementing/installing the Security Module Embedded Software in the IC, • IC testing, and • IC packaging (production of IC modules). Depending on the IC technology or IC type respectively, the concrete processes performed in this phase in combination with the preceding phase 2 and

Life Cycle Phase		Description
		the following phase 4 can vary. The delivery of the Security Module Embedded Software from the developer is done through trusted delivery and verification procedures.
4	**Security Module Product Finishing Process**	The **Security Module Product Manufacturer** is responsible for • the initialisation of the TOE, i.e. loading of the initialisation data into the TOE, and • testing of the TOE. Depending on the IC technology or IC type respectively, the concrete processes performed in this phase in combination with the preceding phases 2 and 3 can vary. The Security Module product finishing process comprises the embedding of the IC modules for the TOE (manufactured in phase 3) and the card production (if applicable, e.g. if the Security Module is realised as a smart card) what may be done alternatively by the Security Module Product Manufacturer or by his customer (e. g. Security Module Issuer).
5	**Security Module Integration** **(Integration Phase of the Mini-HSM and TOE)**	The **Integrator** is responsible for • the physical and technical integration of the initialised Security Module and the Mini-HSM and the electronic connection of both components, • the initial setting of the system PACE-PIN (HSM-System-PIN) in the Security Module, and • the pre-personalisation of the Security Module covering the installation of further directories / files / key objects and the generation / import of key material and further user data (as e.g. certificates, if applicable) for the Mini-HSM User on / to the Security Module, as far as allowed by the access control policy that is implemented in the Security Module. A detailed description of the integration process and its single steps can be found in [TR-03109-2 B]. Result of this integration phase is the Smart Meter

Life Cycle Phase		Description
		Mini-HSM, consisting of the Mini-HSM and its integrated Security Module (TOE). The Mini-HSM and the Security Module are physically connected and the Security Module is equipped with an initial HSM-System-PIN, key and further user data material (as far as applicable).
6	**Security Module End-Usage (Operational Phase of the Smart Meter Mini-HSM)**	In a first step, the *logical connection* of the Security Module integrated in the Smart Meter Mini-HSM and the Application Server, i.e. the pairing of the Security Module with the Application Server is carried out by changing the initial system PACE-PIN (HSM-System-PIN) to a new value. This HSM-System-PIN serves for the later component authentication and secured data transfer between the Application Server and the Security Module. For the *personalisation* of the Smart Meter Mini-HSM with its integrated Security Module, operational key material for the **Mini-HSM User** is generated and installed on the Security Module, as far as not already carried out in the preceding integration phase. This personalisation of the Smart Meter Mini-HSM with its integrated Security Module is task of the **Mini-HSM User**. Depending on the access control policy deposited in the Security Module, further administration of the Security Module and its file and object system can be performed by the **Mini-HSM User** in the framework of the personalisation process. In addition, further personalisation activities may be relevant for the Smart Meter Mini-HSM as whole. Afterwards for *normal usage*, the Smart Meter Mini-HSM with its integrated Security Module is used by the **Mini-HSM User** as cryptographic service provider for his communication and administration issues related to other components and parties in the Smart Metering System. Furthermore, administration of the Security Module itself is as well performed by the **Mini-HSM User** within this phase. All communication of the Mini-HSM User with the Smart Meter Mini-HSM and its integrated Security Module is performed via the so-called Application Server that is responsible for command pre- and post-processing in relation to the Security Module on behalf of the Mini-HSM User. A detailed description of the TOE's end-usage and the

Life Cycle Phase		Description
		TOE's collaboration and interaction with the Application Server or **Mini-HSM User** respectively in the operational phase can be found in [TR-03109-2 B]. Phase 6 for the "Operational Phase of the Smart Meter Mini-HSM" in this PP covers the phases "Installation + Putting in Service of the Smart Meter Mini-HSM", "Personalisation of the Smart Meter Mini-HSM" and "Normal usage (End-Usage) of the Smart Meter Mini-HSM" outlined in [TR-03109-2 B], chapter 2.

Table 2: TOE Life Cycle Model

The TOE life cycle model as described in Table 2 only depicts the main phases and steps as they are relevant for the TOE development, production and usage in the framework of the Smart Metering System and the Smart Meter Mini-HSM with its integrated Security Module (TOE). The Security Target (ST) author shall fill this generic TOE life cycle model with developer and manufacturer specific information and shall adjust the TOE life cycle model description in Table 2 accordingly.

The CC themselves do not prescribe any specific life cycle model. However, in order to define the application of the assurance classes, the CC assume the following implicit generic life cycle model consisting of the following three phases:

- TOE development (including the development as well as the production of the TOE)
- TOE delivery
- TOE operational use

These three generic phases in the sense of the CC are filled with the TOE life cycle model and its six phases as defined in Table 2 above in the following way:

- For the evaluation of the TOE, the phases 1 up to 3 of the TOE life cycle model as defined in Table 2 are part of the phase 'TOE development' in the sense of the CC.
- The phase 4 with the initialisation of the TOE as phase of the TOE life cycle model as defined in Table 2 may alternatively be part of the phase 'TOE development' or the phase 'TOE operational use' in the sense of the CC. The Security Target (ST) author shall define the exact boundary. However, this PP requires that the following conditions have to be met:
    - All executable software in the TOE has to be covered by the evaluation of the TOE.
    - The data structures and the access rights to these data as defined in the Security Module specification [TR-03109-2 B], in particular the initialisation file itself and its creation and handling are covered by the evaluation of the TOE.
    - The initialisation mechanisms and functions provided by the TOE and their security are as well in the scope of the evaluation of the TOE.
- The phases 5 and 6 with the integration and end-usage of the TOE as phases of the TOE life cycle model as defined in Table 2 are part of the phase 'TOE operational use' in the sense of the CC. These phases 5 and 6 are explicitly in focus of the current PP

and its modelling of the TOE's security functionality as carried out in the chapters for the Security Problem Definition, the Security Objectives and the Security Requirements (refer to chapters 3, 4 and 6).

The TOE delivery can take place before or after the TOE's initialisation in phase 4 of the TOE life cycle model as defined in Table 2 above is finished. The ST author has to define the TOE delivery and its time point in the TOE life cycle model exactly. Depending on the TOE delivery concerning the chosen life cycle step the corresponding guidances for the TOE's initialisation as well as the initialisation data have to be prepared and delivered too. It is assumed in this PP that the complete initialisation activities will take place in a secure environment.

The ST author may extend the TOE security functionality with respect to the TOE's initialisation if this takes place after delivery. If not and since the specific production steps of the initialisation are of major security relevance these initialisation steps have to be part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body. All production, generation and installation procedures after TOE delivery up to the end-usage have to be considered in the product evaluation process under the AGD assurance class.

2. Conformance Claim

2.1 CC Conformance Claim

This Protection Profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001 ([CC1])
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002 ([CC2])
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003 ([CC3])

as follows

- Part 2 extended,
- Part 3 conformant.

This Protection Profile has been developed using Version 3.1 Revision 5 of Common Criteria [CC1], [CC2], [CC3].

This Protection Profile is conformant to CC Part 2 [CC2] extended due to the use of FCS_RNG.1, FMT_LIM.1, FMT_LIM.2, and FPT_EMS.1.

This Protection Profile is conformant to CC Part 3 [CC3]. No extended assurance components have been defined.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004 ([CEM])

has to be taken into account.

2.2 PP Claim

This Protection Profile does not claim conformance to any other Protection Profile.

2.3 Package Claim

This Protection Profile conforms to assurance package EAL 4 augmented by AVA_VAN.5 as defined in CC Part 3 [CC3].

2.4 Conformance Claim Rationale

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

2.5 Conformance Statement

The Protection Profile requires **strict conformance** of any PP/ST claiming conformance to this PP.

3. Security Problem Definition

3.1 Subjects and External Entities

The Smart Meter Mini-HSM consists of the Mini-HSM with its integrated Security Module (TOE) according to the specification in [TR-03109-2 B] and is intended to be used by the Mini-HSM User for support of his cryptographic needs in the framework of the Smart Metering System. The role of a Mini-HSM User in the operational phase may be taken e.g. by the Smart Meter Gateway Administrator (called Gateway Administrator for short in the following), the Authorized External Entity (Autorisierter Externer Marktteilnehmer, called EMT for short in the following) or the Gateway Developer.

In its operational phase (phase 6 of the TOE life cycle model), the only external entity that directly interacts with the Smart Meter Mini-HSM and its integrated Security Module (TOE) is the connected Application Server. In particular, the pairing of the Security Module with the Application Server is set up within this phase (via changing the initial HSM-System-PIN from the integration phase). Indirect interaction with the Smart Meter Mini-HSM including the TOE is given by the Mini-HSM User via the Application Server for personalisation and normal usage of the Smart Meter Mini-HSM and its integrated Security Module. Hereby, in view of the TOE, the Application Server is responsible for sending and receiving TOE commands including the necessary data preparation and post-processing on behalf of the Mini-HSM User. The Application Server communicates on logical level directly with the TOE whereby the other HW-/SW-parts of the Smart Meter Mini-HSM beside the TOE serve as simple transport layer for data transmission to or from the TOE inside the Smart Meter Mini-HSM. Refer for details to the description of phase 6 of the TOE life cycle model in chapter 1.5 and [TR-03109-2 B].

During its integration phase (phase 5 of the TOE life cycle model), the TOE interacts indirectly with the Integrator via his integration tools for the related integration activities. Depending on the concrete integration processes, communication with the TOE is performed directly or in case of a preceding integration of the TOE into the Mini-HSM via the Smart Meter Mini-HSM interface. In particular, the initial HSM-System-PIN is set in the TOE within this phase. Refer for details to the description of phase 5 of the TOE life cycle model in chapter 1.5 and [TR-03109-2 B].

The TOE's (security) mechanisms and functionalities used by the Integrator in the integration phase build a subset of those that are used in the operational phase. In the following, for the sake of convenience, the Integrator will be considered therefore as a specific type of Mini-HSM User, and his integration tools will be addressed as a specific type of Application Server.

For the integration phase and operational phase, this PP considers the following external entities and subjects:

External Entity / Subject	Role	Definition
External World	User	Human or IT entity, possibly unauthenticated.
Application Server in the operational phase: HW/SW tool for the regular	Authenticated Application Server	Successful authentication via PACE protocol between Application Server and TOE.

External Entity / Subject	Role	Definition
Mini-HSM User in the integration phase: HW/SW tool for the Integrator		
Mini-HSM User in the operational phase: e.g. Gateway Administrator, Authorized External Entity (EMT), Gateway Developer et al. in the integration phase: Integrator	Authenticated Mini-HSM User	Successful authentication via PACE protocol between Application Server and TOE. The Mini-HSM User is considered as regular, i.e. intended user of the Smart Meter Mini-HSM and its Security Module (TOE). Hint: There is no explicit authentication of the Mini-HSM User against the TOE designed. Authentication of the Mini-HSM User is based instead on the component authentication between the Application Server and the TOE, assuming the secured environment at the Mini-HSM User and usage of the Application Server and of the Smart Meter Mini-HSM and its (integrated) Security Module under the control of the Mini-HSM User.

Table 3: External Entities and Subjects

This table defines external entities and subjects in the sense of [CC1]. Subjects can be recognised by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entity – an 'image' inside and 'works' then with this TOE internal image (also called subject in [CC1]). From this point of view, the TOE itself perceives only 'subjects' and, for them, does not differ between 'subjects' and 'external entities'. There is no dedicated subject with the role 'attacker' within the current security policy, whereby an attacker might 'capture' any subject role recognised by the TOE.

3.2 Assets

In the operational phase, the Smart Meter Mini-HSM with its integrated Security Module (TOE) serves as a cryptographic service provider for the Application Server or the Mini-HSM User respectively as regular user of such Smart Meter Mini-HSM for support of their needs concerning the intended communication with other components and parties involved in the Smart Metering System. The TOE provides different cryptographic functionalities based on elliptic curve cryptography, implements the cryptographic identities of the Mini-HSM User, and serves as a secure storage for cryptographic keys and other (sensitive) data. More detailed, the main cryptographic services provided by the TOE for usage by the Application Server or the Mini-HSM User respectively cover the following issues:

- Digital Signature Generation,
- Digital Signature Verification,
- Key Agreement for TLS,
- Key Agreement for Content Data Encryption,
- Key Pair Generation,
- Random Number Generation,
- Component Authentication via the PACE Protocol with Negotiation of Session Keys,
- Secure Messaging, and
- Secure Storage of Key Material and further (sensitive) data relevant for the Application Server or the Mini-HSM User respectively and their communication with other components and parties involved in the Smart Metering System.

The exact scope of the functionality of the Smart Meter Mini-HSM with its integrated Security Module (TOE) in cooperation with the Application Server or the Mini-HSM User respectively in the operational phase has been outlined in the chapters 1.1 and 1.4.

The sum of that information lead to the relevant assets for this Protection Profile, which are summarized in Table 4 and Table 5. The tables focus on the assets that are relevant for the TOE and its intended usage and do not claim to provide an overview over all assets in the whole Smart Metering System. In the tables, for the assets a distinction related to their need for protection in view of confidentiality (Conf.), integrity (Int.) and authenticity (Auth.) is made.

In the following Table 4 the User Data to be protected by the TOE (as long as in scope of the TOE) are described:

Asset / User Data	**Description**	**Need for Protection**		
		Conf.	**Int.**	**Auth.**
Key Pair	A key pair object contains for the TOE's asymmetric cryptographic functionality the private key data and optionally the corresponding public key data of a key pair. In addition, the corresponding key attributes (as e.g. information on the related elliptic curve, on the key usage etc.) are stored. A key pair object can be used for the following purposes: • TLS • SIG (content data signature) • ENC (content data encryption)	X	X	X

Asset / User Data	Description	Need for Protection		
		Conf.	Int.	Auth.
	• AUTH (support of authentication purpose)			
Public Key	A public key object contains for the TOE's asymmetric cryptographic functionality the public key data of a public key. In addition, the corresponding key attributes (as e.g. information on the related elliptic curve, on the key usage etc.) are stored. A public key object can be used for the following purposes: • TLS • SIG (content data signature) • ENC (content data encryption) In particular, public keys of the SM-PKI-Root, of CAs and of the Smart Meter Gateway can be stored in and processed by the TOE.		X	X
Certificate	Data fields in the TOE may be used as storage for X.509 certificates that belong to public keys of the SM-PKI-Root, of CAs or of the Smart Meter Gateway. A certificate and its contained public key of the SM-PKI-Root is to be considered as a trust anchor.		X	X

Table 4: Assets / User Data

In the following Table 5 the TSF Data to be protected by the TOE (as long as in scope of the TOE) are described:

Asset / TSF Data	Description	Need for Protection		
		Conf.	Int.	Auth.
Ephemeral Key	Negotiated during the PACE protocol between the Application Server and the TOE, during the DH key agreement protocol (ECKA-DH) or during the ElGamal key agreement protocol (ECKA-EG) respectively.	X	X	X

Asset / TSF Data	Description	Need for Protection		
		Conf.	Int.	Auth.
Shared Secret Value / ECKA-DH	Value Z_{AB} negotiated in the framework of the DH key agreement protocol (ECKA-DH). Used by the Application Server on behalf of the Mini-HSM User for the TLS handshake.	X	X	X
Shared Secret Value / ECKA-EG	Value Z_{AB} negotiated in the framework of the ElGamal key agreement protocol (ECKA-EG). Used by the Application Server on behalf of the Mini-HSM User for content data encryption.	X	X	X
Session Key	Negotiated during the PACE protocol between the Application Server and the TOE and used afterwards for a trusted channel (secure messaging) between the Application Server and the TOE.	X	X	X
Domain Parameters of Elliptic Curve	Domain Parameters of the elliptic curves that are used by the key objects (key pair objects, public key objects) or by the cryptographic functionality provided by the TOE respectively.		X	X
HSM-System-PIN	Reference value of the system PACE-PIN of the Application Server / Mini-HSM User for use in the PACE protocol between the Application Server and the TOE.	X	X	X

Table 5: Assets / TSF Data

3.3 Assumptions

In the following, according to the threat model as outlined in the following chapter 3.4, assumptions about the environment of the TOE that need to be taken into account in order to ensure a secure operation of the TOE are listed.

The assumptions for the TOE (A) will be defined in the following manner:

A.Name **Short title**

Description of the assumption.

A.Integration	**Integration phase of the Mini-HSM and TOE** It is assumed that appropriate technical and/or organisational security measures in the phase of the integration of the Mini-HSM and the TOE in the TOE life cycle model guarantee for the confidentiality, integrity and authenticity of the assets of the TOE to be protected with respect to their protection need (see also Table 4 and Table 5 in chapter 3.2). In particular, this holds for the generation, installation and import of key and PIN material as far as handled in the framework of the integration of the Mini-HSM and the TOE. The Integrator in particular takes care for the consistency of key material in key objects and associated certificates if handled in the framework of the integration of the Mini-HSM and the TOE.
A.OperationalPhase	**Operational phase of the Smart Meter Mini-HSM (Mini-HSM with integrated Security Module)** It is assumed that appropriate technical and/or organisational security measures in the operational phase of the Smart Meter Mini-HSM with its integrated Security Module (TOE) guarantee for the confidentiality, integrity and authenticity of the assets of the TOE to be protected with respect to their protection need (see also Table 4 and Table 5 in chapter 3.2). In particular, this holds for key and PIN objects stored, generated and processed in the operational phase of the Smart Meter Mini-HSM with its integrated Security Module. Furthermore, the Mini-HSM User is in particular in charge of the administration of the TOE that is integrated in the Smart Meter Mini-HSM, i.e. the administration of the TOE's file and object system consisting of folders, data files and key objects. The Mini-HSM User is responsible for the appropriate key management in the integrated TOE and, if applicable, takes in particular care for the consistency of key material in key objects and associated certificates.
A.Implementation	**Implementation of the Smart Meter Mini-HSM and Application Server** It is assumed that the TOE is physically and logically embedded into a Mini-HSM (whereby the integration is performed during the integration phase of the TOE life cycle model) taking the specification in [TR-03109-2 B] and the requirements in the TOE user guidances into account. It is assumed that the Smart Meter Mini-HSM with its integrated Security Module (TOE) is physically and logically connected to the Application Server via which the Mini-HSM User communicates in the operational phase with the Smart Meter Mini-HSM and its integrated Security Module (TOE). This Application

Server and its implementation takes the specification in [TR-03109-2 B] and the requirements in the Smart Meter Mini-HSM and TOE user guidances into account.

A.Protection **Protection of the TOE, Smart Meter Mini-HSM and Application Server**

It is assumed that the TOE, the Smart Meter Mini-HSM with its integrated Security Module (TOE) and the connected Application Server are installed and applied in a non-public, secured environment at the Mini-HSM User with sufficient security measures.

Usage of the TOE, of the Smart Meter Mini-HSM with its integrated Security Module (TOE) and of the connected Application Server takes place under the control of the Mini-HSM User and under consideration of the user guidances for the Smart Meter Mini-HSM, its (integrated) Security Module (TOE) and the connected Application Server.

This assumption addresses the operational phase as well as the integration phase.

A.TrustedUser **Trustworthiness of the Mini-HSM User**

It is assumed that the Mini-HSM User is trustworthy and well-trained, in particular in view of the correct and secure usage of the Smart Meter Mini-HSM and its (integrated) TOE and of the Application Server.

This assumption addresses the Mini-HSM User in the operational phase as well as in the integration phase.

3.4 Threats

In the following, the threats that are posed against the assets handled by the TOE are defined. Those threats are the result of a threat model that has been developed for the whole Smart Metering System at first and then has been focussed on the threats against the TOE.

In spite of the assumption that in the operational phase usage of the Smart Meter Mini-HSM with its integrated Security Module (TOE) and the connected Application Server takes place within the secured environment at the trustworthy Mini-HSM User and under control of this user the following attack scenarios are considered:

Goal of the attack on the Smart Meter Mini-HSM with its integrated TOE and the connected Application Server is to try to disclose or alter data while stored in, while processed in, while generated by or while transmitted between the TOE, the Smart Meter Mini-HSM and the Application Server. In particular, as the Smart Meter Mini-HSM with its integrated TOE serves as central cryptographic service provider and as secure storage for key and further (sensitive) data for the Application Server on behalf of the Mini-HSM User to support his needs in the framework of the Smart Metering System, the assets stored, processed, generated and transmitted by the TOE are in focus of the attacker.

Beside a local attacker having physical access to the Smart Meter Mini-HSM and its integrated TOE and to the Application Server as well remote attacks on the TOE on logical level via further interfaces of the Smart Meter Mini-HSM or the Application Server, if existing, have to be taken into account.

These considerations hold in analogy for the integration phase of the Mini-HSM and the TOE.

Taking the preceding considerations into account, the following threats to the TOE are of relevance.

The threats to the TOE (T) will be defined in the following manner:

T.Name	**Short title** Description of the threat.
T.ForgeInternalData	**Forgery of User Data or TSF Data** An attacker with high attack potential tries to forge internal User Data or TSF Data via the regular communication interface of the TOE. This threat comprises several attack scenarios of forgery of internal User Data or TSF Data. The attacker may try to alter User Data e.g. by deleting and replacing persistently stored key objects or adding data to data already stored in elementary files. The attacker may misuse the TSF management function to change the user authentication data (HSM-System-PIN) to a known value.
T.CompromiseInternalData	**Compromise of confidential User Data or TSF Data** An attacker with high attack potential tries to compromise confidential User Data or TSF Data via the regular communication interface of the TOE. This threat comprises several attack scenarios of revealing confidential internal User Data or TSF Data. The attacker may try to compromise the user authentication data (HSM-System-PIN), to reconstruct a private signing key by using the regular command interface and the related response codes, or to compromise generated shared secret values or ephemeral keys.
T.Misuse	**Misuse of TOE functions** An attacker with high attack potential tries to use the TOE functions to gain access to access control protected assets without knowledge of user authentication data or any implicit authorisation. This threat comprises several attack scenarios. The attacker may try to circumvent the user authentication mechanism to access assets or functionality of the TOE that underlie the TOE's access control and require user authentication. The

attacker may try to alter the TSF data e.g. to extend the user rights after successful authentication.

T.Intercept	**Interception of communication** An attacker with high attack potential tries to intercept the communication between the TOE and the Application Server to disclose, to forge or to delete transmitted (sensitive) data or to insert data in the data exchange. This threat comprises several attack scenarios. An attacker may read data during data transmission in order to gain access to user authentication data (HSM-System-PIN) or sensitive material as generated ephemeral keys or shared secret values. An attacker may try to forge public keys during their import to respective export from the TOE.
T.Leakage	**Leakage** An attacker with high attack potential tries to launch a cryptographic attack against the implementation of the cryptographic algorithms or tries to guess keys using a brute-force attack on the function inputs. This threat comprises several attack scenarios. An attacker may try to predict the output of the random number generator in order to get information about a generated session key, shared secret value or ephemeral key. An attacker may try to exploit leakage during a cryptographic operation in order to use SPA, DPA, DFA, SEMA or DEMA techniques with the goal to compromise the processed keys, the HSM-System-PIN or to get knowledge of other sensitive TSF or User Data. Furthermore an attacker could try guessing the processed key by using a brute-force attack. In addition, timing attacks have to be taken into account. The sources for this leakage information can be the measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines (side channels).
T.PhysicalTampering	**Physical tampering** An attacker with high attack potential tries to manipulate the TOE through physical tampering, probing or modification in order to extract or alter User Data or TSF Data stored in or processed by the TOE. Alternatively, the attacker tries to change TOE functions (as e.g. cryptographic functions provided by the TOE) by physical means (e.g. through fault injection).

T.AbuseFunctionality **Abuse of functionality**

An attacker with high attack potential tries to use functions of the TOE which shall not be used in TOE operational phase in order (i) to disclose or manipulate sensitive User Data or TSF Data, (ii) to manipulate the TOE's software or (iii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE.

In particular, the TOE shall ensure that functionality that shall not be usable in the operational phase, but which is present during the phases of the TOE's manufacturing and initialisation as well as during the integration phase of the Mini-HSM and the TOE, is deactivated before the TOE enters the operational phase. Such functionality includes in particular testing, debugging and initialisation functions.

T.Malfunction **Malfunction of the TOE**

An attacker with high attack potential tries to cause a malfunction of the TSF or of the IC Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify security functions of the IC Embedded Software.

This may be achieved e.g. by operating the IC outside the normal operating conditions, exploiting errors in the IC Embedded Software or misuse of administration function. To exploit this an attacker needs information about the functional operation.

3.5 Organisational Security Policies

This section specifies the organisational security policies (OSP) that the TOE and its environment shall comply with in order to support the Application Server or the Mini-HSM User respectively for their needs in the framework of the Smart Metering System.

The organisational security policies for the TOE (P) will be defined in the following manner:

P.Name **Short title**

Description of the organisational security policy.

P.Sign **Signature generation and verification**

The TOE shall generate and verify digital signatures according to [TR-03109-3], [TR-03109-2 B].

The explicit generation and verification of digital signatures is used by the Application Server on behalf of the Mini-HSM User especially in the framework of the TLS handshake, the content data signature and the verification of certificates and certificate chains.

P.KeyAgreementDH **DH key agreement**

The TOE and the Application Server shall implement the DH key agreement (ECKA-DH) according to [TR-03109-3], [TR-03109-2 B].

The DH key agreement is used by the Application Server on behalf of the Mini-HSM User in the framework of the TLS handshake. The Application Server uses the shared secret value Z_{AB} generated by the TOE for the generation of the pre-master secret and with random numbers as well generated by the TOE afterwards to create the master secret.

P.KeyAgreementEG **ElGamal key agreement**

The TOE and the Application Server shall implement the ElGamal key agreement (ECKA-EG) according to [TR-03109-3], [TR-03109-2 B].

The ElGamal key agreement is used by the Application Server on behalf of the Mini-HSM User in the framework of the content data encryption. The Application Server uses the shared secret value Z_{AB} generated by the TOE for the generation of the symmetric encryption keys (hybrid encryption/decryption scheme).

P.Random **Random number generation**

The TOE shall generate random numbers for its own use (e.g. for the generation of ECC key pairs and session keys) and for use by the Application Server itself according to [TR-03109-3], [TR-03109-2 B].

Randoms generated by the TOE are used by the Application Server on behalf of the Mini-HSM User for its different cryptographic needs.

P.PACE **PACE**

The TOE and the Application Server shall implement the PACE protocol according to [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3], [TR-03109-2 B] for component authentication between the Application Server and the TOE. In the framework of the PACE protocol session keys for securing the data exchange between the Application Server and the TOE (trusted channel) are negotiated.

4. Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the operational environment.

The security objectives for the TOE (O) and the security objectives for the operational environment (OE) will be defined in the following manner:

O/OE.Name	**Short title** Description of the objective.

4.1 Security Objectives for the TOE

This chapter describes the security objectives for the TOE which address the aspects of the identified threats to be countered by the TOE independent of the operational environment as well as the organisational security policies to be met by the TOE independent of the operational environment.

O.Integrity	**Integrity of User Data and TSF Data** The TOE shall ensure the integrity of the User Data, the security services provided by the TOE and the TSF Data under the TSF scope of control.
O.Confidentiality	**Confidentiality of User Data and TSF Data** The TOE shall ensure the confidentiality of private keys and other confidential User Data and confidential TSF Data (especially the user authentication data as the HSM-System-PIN) under the TSF scope of control.
O.Authentication	**Authentication of external entities** The TOE shall support the authentication of the Application Server or the Mini-HSM User respectively. The TOE shall be able to authenticate itself to the Application Server or the Mini-HSM User respectively.
O.AccessControl	**Access control for functionality and objects** The TOE shall provide and enforce the functionality of access right control. The access right control shall cover the functionality provided by the TOE (including its management functionality) and the objects stored in or processed by the TOE. The TOE shall enforce that only authenticated entities with sufficient access control rights can access restricted objects and services. The access control policy of the TOE shall bind the access control right to an object to authenticated entities.

O.KeyManagement **Key management**

The TOE shall enforce the secure generation, import, distribution, access control and destruction of cryptographic keys. The TOE shall support the public key import from and export to the Application Server.

O.TrustedChannel **Trusted channel**

The TOE shall establish a trusted channel for protection of the confidentiality and the integrity of the transmitted data between the TOE and the successfully authenticated Application Server. The TOE shall enforce the use of a trusted channel if defined by the access condition of an object.

O.Leakage **Leakage protection**

The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

The TOE shall provide side channel resistance, i.e. shall be able to prevent appropriately leakage of information, e.g. electrical characteristics like power consumption or electromagnetic emanations that would allow an attacker to learn about

- private key material,
- confidential results or intermediate results of cryptographic computations,
- the HSM-System-PIN.

O.PhysicalTampering **Protection against physical tampering**

The TOE shall provide system features that detect physical tampering, probing and manipulation of its components against an attacker with high attack potential, and uses those features to limit security breaches.

The TOE shall prevent or resist physical tampering, probing and manipulation with specified system devices and components.

O.AbuseFunctionality **Protection against abuse of functionality**

The TOE shall prevent that functions intended for the testing and production of the TOE and which must not be accessible after TOE delivery can be abused in order (i) to disclose or manipulate sensitive User Data or TSF Data, (ii) to manipulate the TOE's software or (iii) to bypass, deactivate, change or explore security features or functions of the TOE.

> **Application Note 1:** Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

In particular, the TOE shall ensure that functionality that shall not be usable in the operational phase, but which is present during the phases of the TOE's manufacturing and initialisation as well as during the integration phase of the Mini-HSM and the TOE, is deactivated before the TOE enters the operational phase. Such functionality includes in particular testing, debugging and initialisation functions.

O.Malfunction	**Protection against malfunction of the TOE** The TOE shall ensure its correct operation. The TOE shall prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. The TOE shall preserve a secure state to prevent errors and deactivation of security features of functions. The environmental conditions include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, and temperature.
O.Sign	**Signature generation and verification** The TOE shall securely generate and verify digital signatures according to [TR-03109-3], [TR-03109-2 B]. The explicit generation and verification of digital signatures is used by the Application Server on behalf of the Mini-HSM User especially in the framework of the TLS handshake, the content data signature and the verification of certificates and certificate chains.
O.KeyAgreementDH	**DH key agreement** The TOE shall securely implement the DH key agreement (ECKA-DH) according to [TR-03109-3], [TR-03109-2 B]. The DH key agreement is used by the Application Server on behalf of the Mini-HSM User in the framework of the TLS handshake. The Application Server uses the shared secret value Z_{AB} generated by the TOE for the generation of the pre-master secret and with random numbers as well generated by the TOE afterwards to create the master secret.
O.KeyAgreementEG	**ElGamal key agreement** The TOE shall securely implement the ElGamal key agreement (ECKA-EG) according to [TR-03109-3], [TR-03109-2 B]. The ElGamal key agreement is used by the Application Server on behalf of the Mini-HSM User in the framework of the content data encryption. The Application Server uses the shared secret value Z_{AB} generated by the TOE for the generation of the symmetric encryption keys (hybrid encryption/decryption scheme).
O.Random	**Random number generation** The TOE shall securely generate random numbers for its own use (e.g. for the generation of ECC key pairs and session keys) and for

use by the Application Server itself according to [TR-03109-3], [TR-03109-2 B].

Randoms generated by the TOE are used by the Application Server on behalf of the Mini-HSM User for its different cryptographic needs.

O.PACE **PACE**

The TOE shall securely implement the PACE protocol according to [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3], [TR-03109-2 B] for component authentication between the Application Server and the TOE. In the framework of the PACE protocol session keys for securing the data exchange between the Application Server and the TOE (trusted channel) are negotiated.

4.2 Security Objectives for the Operational Environment

The following security objectives for the operational environment of the TOE are defined:

OE.Integration **Integration phase of the Mini-HSM and TOE**

Appropriate technical and/or organisational security measures in the phase of the integration of the Mini-HSM and the TOE in the TOE life cycle model shall be applied in order to guarantee for the confidentiality, integrity and authenticity of the assets of the TOE to be protected with respect to their protection need (see also Table 4 and Table 5 in chapter 3.2).

In particular, for the TOE, this shall hold for the generation, installation and import of key and PIN material as far as handled in the framework of the integration of the Mini-HSM and the TOE.

The Integrator shall in particular take care for the consistency of key material in key objects and associated certificates if handled in the framework of the integration of the Mini-HSM and the TOE.

OE.OperationalPhase **Operational phase of the Smart Meter Mini-HSM (Mini-HSM with integrated Security Module)**

Appropriate technical and/or organisational security measures in the operational phase of the Smart Meter Mini-HSM with its integrated Security Module (TOE) shall be applied in order to guarantee for the confidentiality, integrity and authenticity of the assets of the TOE to be protected with respect to their protection need (see also Table 4 and Table 5 in chapter 3.2).

In particular, this shall hold for key and PIN objects stored, generated and processed in the operational phase of the Smart Meter Mini-HSM with its integrated Security Module.

Furthermore, the Mini-HSM User shall in particular be in charge of the administration of the TOE that is integrated in the Smart Meter Mini-HSM, i.e. the administration of the TOE's file and object system consisting of folders, data files and key objects. The Mini-HSM User shall be responsible for the appropriate key management in the integrated TOE and, if applicable, shall take in particular care for the consistency of key material in key objects and associated certificates.

OE.Implementation **Implementation of the Smart Meter Mini-HSM and Application Server**

The TOE shall be physically and logically embedded into a Mini-HSM (whereby the integration is performed during the integration phase of the TOE life cycle model) taking the specification in [TR-03109-2 B] and the requirements in the TOE user guidances into account.

The Smart Meter Mini-HSM with its integrated Security Module (TOE) shall be physically and logically connected to the Application Server via which the Mini-HSM User communicates in the operational phase with the Smart Meter Mini-HSM and its integrated Security Module (TOE). This Application Server and its implementation shall take the specification in [TR-03109-2 B] and the requirements in the Smart Meter Mini-HSM and TOE user guidances into account.

OE.Protection **Protection of the TOE, Smart Meter Mini-HSM and Application Server**

The TOE, the Smart Meter Mini-HSM with its integrated Security Module (TOE) and the connected Application Server shall be installed and applied in a non-public, secured environment at the Mini-HSM User with sufficient security measures.

Usage of the TOE, of the Smart Meter Mini-HSM with its integrated Security Module (TOE) and of the connected Application Server shall take place under the control of the Mini-HSM User and under consideration of the user guidances for the Smart Meter Mini-HSM, its (integrated) Security Module (TOE) and the connected Application Server.

This objective addresses the operational phase as well as the integration phase.

OE.TrustedUser **Trustworthiness of the Mini-HSM User**

The Mini-HSM User shall be trustworthy and well-trained, in particular in view of the correct and secure usage of the Smart Meter Mini-HSM and its (integrated) TOE and of the Application Server.

This objective addresses the Mini-HSM User in the operational phase as well as in the integration phase.

OE.Sign **Signature generation and verification**

The Application Server on behalf of the Mini-HSM User shall make use of the TOE's signature generation and verification functionality, especially in the framework of the TLS handshake, the content data signature and the verification of certificates and certificate chains.

OE.KeyAgreementDH **DH key agreement**

The Application Server shall securely implement the DH key agreement (ECKA-DH) according to [TR-03109-3], [TR-03109-2 B].

The DH key agreement is used by the Application Server on behalf of the Mini-HSM User in the framework of the TLS handshake. The Application Server uses the shared secret value Z_{AB} generated by the TOE for the generation of the pre-master secret and with random numbers as well generated by the TOE afterwards to create the master secret.

OE.KeyAgreementEG **ElGamal key agreement**

The Application Server shall securely implement the ElGamal key agreement (ECKA-EG) according to [TR-03109-3], [TR-03109-2 B].

The ElGamal key agreement is used by the Application Server on behalf of the Mini-HSM User in the framework of the content data encryption. The Application Server uses the shared secret value Z_{AB} generated by the TOE for the generation of the symmetric encryption keys (hybrid encryption/decryption scheme).

OE.Random **Random number generation**

The Application Server on behalf of the Mini-HSM User shall make use of the TOE's random number generation functionality for its different cryptographic needs.

OE.PACE **PACE**

The Application Server shall securely implement the PACE protocol according to [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3], [TR-03109-2 B] for component authentication between the Application Server and the TOE. In the framework of the PACE protocol session keys for securing the data exchange between the Application Server and the TOE (trusted channel) are negotiated.

OE.TrustedChannel **Trusted channel**

The Application Server shall perform a trusted channel between the Application Server and the TOE for protection of the confidentiality and integrity of the sensitive data transmitted between the authenticated Application Server and the TOE.

4.3 Security Objectives Rationale

4.3.1 Overview

The following tables give an overview how the assumptions, threats and organisational security policies are addressed by the security objectives for the TOE and its operational environment. Because of the amount of security objectives for the TOE and its operational environment, the mapping between the assumptions, threats and organisational security policies on the one hand and the security objectives for the TOE and its operational environment on the other hand is split into two tables. Hence, there is one mapping table covering the security objectives for the TOE (see Table 6) and a further table addressing the security objectives for the operational environment (see Table 7).

The following tables provide an overview for the security objectives coverage (TOE and its operational environment) also giving evidence for sufficiency and necessity of the security objectives defined for the TOE and its operational environment. It shows that all threats are addressed by the security objectives for the TOE and its operational environment, that all organisational security policies are addressed by the security objectives for the TOE and its operational environment, and that all assumptions are addressed by the security objectives for the operational environment.

	O.Integrity	O.Confidentiality	O.Authentication	O.AccessControl	O.KeyManagement	O.TrustedChannel	O.Leakage	O.PhysicalTampering	O.AbuseFunctionality	O.Malfunction	O.Sign	O.KeyAgreementDH	O.KeyAgreementEG	O.Random	O.PACE
T.ForgeInternalData	X														
T.CompromiseInternalData		X													
T.Misuse	X	X	X	X											
T.Intercept				X		X									X
T.Leakage							X		X						
T.PhysicalTampering								X	X						
T.AbuseFunctionality									X						
T.Malfunction										X					
P.Sign					X						X				
P.KeyAgreementDH					X							X			
P.KeyAgreementEG					X								X		
P.Random														X	

	O.Integrity	O.Confidentiality	O.Authentication	O.AccessControl	O.KeyManagement	O.TrustedChannel	O.Leakage	O.PhysicalTampering	O.AbuseFunctionality	O.Malfunction	O.Sign	O.KeyAgreementDH	O.KeyAgreementEG	O.Random	O.PACE
P.PACE															X

Table 6: Rationale for Security Objectives for the TOE

	OE.Integration	OE.OperationalPhase	OE.Implementation	OE.Protection	OE.TrustedUser	OE.Sign	OE.KeyAgreementDH	OE.KeyAgreementEG	OE.Random	OE.PACE	OE.TrustedChannel
T.ForgeInternalData											
T.CompromiseInternalData											
T.Misuse											
T.Intercept										X	X
T.Leakage											
T.PhysicalTampering											
T.AbuseFunctionality											
T.Malfunction											
P.Sign						X					
P.KeyAgreementDH							X				
P.KeyAgreementEG								X			
P.Random									X		
P.PACE										X	
A.Integration	X										
A.OperationalPhase		X									
A.Implementation			X								
A.Protection				X							
A.TrustedUser					X						

Table 7: Rationale for Security Objectives for the Operational Environment

The following chapters provide a detailed justification for this mapping as required to show the suitability and sufficiency of the security objectives to cope with the security problem definition.

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 the operational environment.

T.ForgeInternalData

The threat **T.ForgeInternalData** is countered by the security objective **O.Integrity**.

The security objective **O.Integrity** directly cares for the integrity of the User Data and the TSF Data under the TSF scope of control as well as for the integrity of the security services provided by the TOE.

T.CompromiseInternalData

The threat **T.CompromiseInternalData** is countered by the security objective **O.Confidentiality**.

The security objective **O.Confidentiality** directly cares for the confidentiality of the User Data and the TSF Data under the TSF scope of control.

T.Misuse

The threat **T.Misuse** is countered by a combination of the security objectives **O.AccessControl**, **O.Authentication**, **O.Integrity** and **O.Confidentiality**.

The security objective **O.AccessControl** prescribes the access control policy defined for the TOE and ensures for its enforcement. Authentication as needed for regulating the access to the TOE's functionality and the assets stored in and processed by the TOE is addressed by the security objective **O.Authentication**. The security objectives **O.Integrity** and **O.Confidentiality** ensure the protection of the assets independent of the TOE functionality used by the attack.

T.Intercept

The threat **T.Intercept** is countered by a combination of the security objectives **O.TrustedChannel**, **OE.TrustedChannel**, **O.PACE**, **OE.PACE** and **O.AccessControl**.

The security objectives **O.TrustedChannel** and **OE.TrustedChannel** provide support for a secure communication channel between the TOE and the Application Server in view of integrity and confidentiality of the data exchange. Compromise, forgery, deletion and insertion of data transmitted between the TOE and the Application Server is countered by an integrity- and confidentiality-preserving communication channel. The session keys used for the trusted channel between the Application Server and the TOE are negotiated via the PACE protocol carried out between the Application Server and the TOE. This is covered by the security objectives **O.PACE** and **OE.PACE**. In addition, the requirement for an integrity- and confidentiality-preserved exchange of sensitive data between the Application Server and the TOE is prescribed in the access control policy defined for the TOE. This access control policy and its enforcement is part of the security objective **O.AccessControl**.

T.Leakage

The threat **T.Leakage** is countered by a combination of the security objectives **O.Leakage** and **O.AbuseFunctionality**.

The security objective **O.Leakage** ensures for the resistance of the TOE against side channel attacks and appropriately prevents leakage of information. The security objective **O.AbuseFunctionality** directly averts the threat by ensuring that functions intended for the testing and production of the TOE and which must not be accessible after TOE delivery cannot be abused in order (i) to disclose or manipulate sensitive User Data or TSF Data, (ii) to manipulate the TOE's software or (iii) to bypass, deactivate, change or explore security features or functions of the TOE.

Both objectives together ensure for the TOE's security in view of the emanation of side channel information and therefore contribute to the security of the internal User Data and TSF Data stored in and processed by the TOE as well as contribute to the security of the (cryptographic) services provided by the TOE.

T.PhysicalTampering

The threat **T.PhysicalTampering** is countered by a combination of the security objectives **O.PhysicalTampering** and **O.AbuseFunctionality**.

The security objective **O.PhysicalTampering** ensures for the detection of and the prevention or resistance respectively of the TOE against physical tampering, probing and manipulation. The security objective **O.AbuseFunctionality** directly averts the threat by ensuring that functions intended for the testing and production of the TOE and which must not be accessible after TOE delivery cannot be abused in order (i) to disclose or manipulate sensitive User Data or TSF Data, (ii) to manipulate the TOE's software or (iii) to bypass, deactivate, change or explore security features or functions of the TOE.

Both objectives together ensure for the TOE's physical security and therefore contribute to the security of the internal User Data and TSF Data stored in and processed by the TOE as well as contribute to the security and correct functioning of the (cryptographic) services provided by the TOE.

T.AbuseFunctionality

The threat **T.AbuseFunctionality** is countered by the security objective **O.AbuseFunctionality**.

The security objective **O.AbuseFunctionality** directly averts the threat by ensuring that functions intended for the testing and production of the TOE and which must not be accessible after TOE delivery cannot be abused in order (i) to disclose or manipulate sensitive User Data or TSF Data, (ii) to manipulate the TOE's software or (iii) to bypass, deactivate, change or explore security features or functions of the TOE.

T.Malfunction

The threat **T.Malfunction** is countered by the security objective **O.Malfunction**.

The security objective **O.Malfunction** directly averts the threat by ensuring the TOE's correct operation and preservation of a secure state to prevent errors and deactivation of security features of functions even under abnormal environmental conditions.

4.3.3 Coverage of Organisational Security Policies

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

P.Sign

The organisational security policy **P.Sign** that mandates that the TOE implements digital signature generation and verification according to [TR-03109-3], [TR-03109-2 B] is directly addressed by the security objective **O.Sign**. The security objective **O.KeyManagement** serves for the availability of the keys as necessary for the cryptographic operation. The security objective **OE.Sign** covers the use of the TOE's signature generation and verification functionality by the Application Server, especially in the framework of the TLS handshake, the content data signature and the verification of certificates and certificate chains.

P.KeyAgreementDH

The organisational security policy **P.KeyAgreementDH** that mandates that the TOE and the Application Server implement the DH key agreement according to [TR-03109-3], [TR-03109-2 B] is directly addressed by the security objectives **O.KeyAgreementDH** and **OE.KeyAgreementDH**. The security objective **O.KeyManagement** serves for the availability of the keys as necessary for the cryptographic operation.

P.KeyAgreementEG

The organisational security policy **P.KeyAgreementEG** that mandates that the TOE and the Application Server implement the ElGamal key agreement according to [TR-03109-3], [TR-03109-2 B] is directly addressed by the security objectives **O.KeyAgreementEG** and **OE.KeyAgreementEG**. The security objective **O.KeyManagement** serves for the availability of the keys as necessary for the cryptographic operation.

P.Random

The organisational security policy **P.Random** that mandates that the TOE implements random number generation for its own use and for use by the Application Server according to [TR-03109-3], [TR-03109-2 B] is directly addressed by the security objective **O.Random**. The security objective **OE.Random** covers the use of the TOE's random number generation functionality by the Application Server for its different cryptographic needs.

P.PACE

The organisational security policy **P.PACE** that mandates that the TOE and the Application Server implement the PACE protocol according to [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3], [TR-03109-2 B] for component authentication between the Application Server and the TOE with negotiation of session keys for securing the following data exchange between the Application Server and the TOE is directly addressed by the security objectives **O.PACE** and **OE.PACE**.

4.3.4 Coverage of Assumptions

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

A.Integration

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

A.OperationalPhase

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

A.Implementation

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

A.Protection

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

A.TrustedUser

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

5. Extended Component Definition

This Protection Profile uses components defined as extensions to CC Part 2 [CC2]. The components FPT_EMS, FCS_RNG and FMT_LIM are common in Protection Profiles for smart cards and similar devices.

5.1 Definition of the Family FPT_EMS

The family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of the TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC Part 2 [CC2].

Family Behaviour

This family defines requirements to mitigate intelligible emanations.

Component Levelling

FPT_EMS.1 TOE Emanation defines limits of TOE emanation related to TSF and user data.

Management

FPT_EMS.1 There are no management activities foreseen.

Audit

FPT_EMS.1 There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

FPT_EMS.1	TOE Emanation
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMS.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

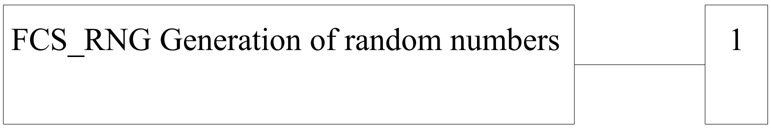
5.2 Definition of the Family FCS_RNG

To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (Cryptographic Support) is defined here. This extended family FCS_RNG describes an SFR for random number generation used for cryptographic purposes.

Family Behaviour

This family defines quality requirements for the generation of random numbers, which are intended to be used for cryptographic purposes.

Component Levelling:



FCS_RNG.1 Generation of random numbers requires that the random number generator implements defined security capabilities and the random numbers meet a defined quality metric.

Management

FCS_RNG.1 There are no management activities foreseen.

Audit

FCS_RNG.1 There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

FCS_RNG.1	Random number generation
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].
FCS_RNG.1.2	The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

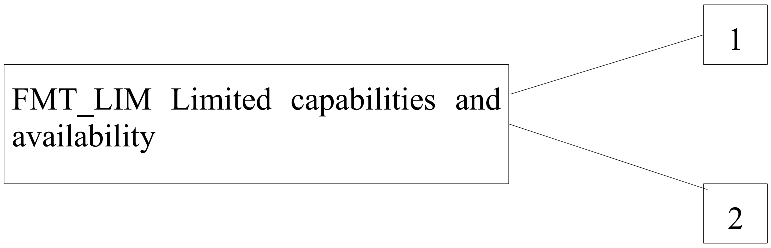
5.3 Definition of the Family FMT_LIM

To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

Family Behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component Levelling



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restricts the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life cycle.

Management

FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.

Audit

FMT_LIM.1, FMT_LIM.2 There are no actions defined to be auditable.

FMT_LIM.1 Limited capabilities

FMT_LIM.1	Limited capabilities
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: *Limited capability and availability policy*].

FMT_LIM.2 Limited availability

FMT_LIM.2	Limited availability
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: *Limited capability and availability policy*].

Application Note 2: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

i. the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced,

   or conversely,

ii. the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both requirements shall enforce the policy.

6. Security Requirements

6.1 Overview

This part of the PP defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional security requirements (SFRs) and the assurance security requirements (SARs) that the TOE needs to satisfy in order to meet the security objectives for the TOE. These requirements comprise functional components from CC Part 2 [CC2], extended components as defined in chapter 5, and the assurance components as defined for the Evaluation Assurance Level EAL 4 from CC Part 3 [CC3] augmented by AVA_VAN.5.

The CC allows several operations to be performed on security requirements (on the component level); refinement, selection, assignment and iteration are defined in sec. 8.1 of CC Part 1 [CC1].

The **refinement** operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed words are ~~crossed out~~. In some cases an interpretation refinement is given. In such a case an extra paragraph starting with “Refinement” is given.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicised*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicised*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicised like *this*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier. For the sake of a better readability, the iteration operation may also be applied to some single components (being not repeated) in order to indicate belonging of such SFRs to same functional cluster. In such a case, the iteration operation is applied to only one single component.

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 (SFR) of this PP:

SFRs	
Class FCS: Cryptographic Support	
FCS_CKM.1/ECC	Cryptographic key generation / ECC-Key Pairs
FCS_CKM.1/ECKA-DH	Cryptographic key generation / DH key agreement (for TLS)
FCS_CKM.1/ECKA-EG	Cryptographic key generation / ElGamal key agreement (for content data encryption)
FCS_CKM.1/PACE	Cryptographic key generation / PACE
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/SIG-ECDSA	Cryptographic operation / ECDSA Signature generation
FCS_COP.1/VER-ECDSA	Cryptographic operation / ECDSA Signature verification
FCS_COP.1/IMP	Cryptographic operation / Import of Public Keys
FCS_COP.1/PACE-ENC	Cryptographic operation / AES in CBC mode for secure messaging
FCS_COP.1/PACE-MAC	Cryptographic operation / AES-CMAC for secure messaging
FCS_RNG.1	Random number generation
Class FDP: User Data Protection	
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_SDI.2	Stored data integrity monitoring and action
FDP_RIP.1	Subset residual information protection
FDP_ETC.1	Export of user data without security attributes
FDP_ITC.1	Import of user data without security attributes
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
Class FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.4	Single-use authentication mechanisms

SFRs	
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
Class FMT: Security Management	
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
Class FPT: Protection of the TSF	
FPT_EMS.1	TOE emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing
Class FTP: Trusted path/channels	
FTP_ITC.1	Inter-TSF trusted channel

Table 8: List of Security Functional Requirements

6.2 Class FCS: Cryptographic Support

The Smart Meter Mini-HSM with its integrated Security Module (TOE) serves in the operational phase as a cryptographic service provider for the Application Server or the Mini-HSM User respectively as regular user of such Smart Meter Mini-HSM and provides services in the following cryptographic areas:

- Signature Generation (ECDSA),
- Signature Verification (ECDSA),
- Key Agreement for TLS (ECKA-DH),
- Key Agreement for Content Data Encryption (ECKA-EG),
- Key Pair Generation,
- Random Number Generation,
- Component Authentication via the PACE Protocol with Negotiation of Session Keys (PACE),
- Secure Messaging, and

- Secure Storage of Key Material and further (sensitive) data relevant for the Application Server or the Mini-HSM User respectively and their communication with other components and parties involved in the Smart Metering System.

The exact scope of the functionality of the Smart Meter Mini-HSM with its integrated Security Module (TOE) in cooperation with the Application Server or the Mini-HSM User respectively in the operational phase has been outlined in the chapters 1.1 and 1.4.

The cryptographic algorithms that shall be supported by the Security Module (TOE) of the Smart Meter Mini-HSM are the same as those that are defined in [TR-03109-3] or in [TR-03116-3] respectively for the Smart Meter Gateway and its Security Module.

[TR-03109-3] or [TR-03116-3] respectively distinguish between mandatory key sizes and domain parameters for elliptic curves, and key sizes and domain parameters for elliptic curves that are optional to support. **It is however essential that the Security Module (TOE) for the Smart Meter Mini-HSM supports for ECC key generation, ECDSA signature generation and verification, ECKA-DH, ECKA-EG and PACE all the key sizes and domain parameters for elliptic curves that are defined in [TR-03109-3] or in [TR-03116-3] respectively.**

Cryptographic Key Management (FCS_CKM)

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1/ECC)" as specified below:

FCS_CKM.1/ECC	Cryptographic key generation / ECC-Key Pairs
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/ECC	The TSF shall generate cryptographic **ECC** 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: <u>[TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively</u>.

Application Note 3: Based on [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively, the ST author shall exactly reference the applied cryptographic key generation algorithm (as refinement operation for the generic references given in the PP at present).

Application Note 4: [TR-03109-2 B] or [TR-03109-2] respectively require the TOE to implement the command GENERATE ASYMETRIC KEY PAIR. The generated key pairs are used by the Mini-HSM User in the operational phase for TLS and for content data encryption and signature. Furthermore, in case of the Gateway Administrator as

Mini-HSM User the generated key pairs are used for generation of the authentication token that is requested within his user authentication against the Security Module integrated in the Smart Meter Gateway.

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1/ECKA-DH)" as specified below:

FCS_CKM.1/ECKA-DH Cryptographic key generation / DH key agreement

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/ECKA-DH	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECKA-DH and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively.

Application Note 5: Based on [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively, the ST author shall exactly reference the applied cryptographic key generation algorithm (as refinement operation for the generic references given in the PP at present). In [TR-03116-3] a reference to [TR-03111] is given where the specification of ECKA-DH can be found.

Application Note 6: [TR-03109-2 B] or [TR-03109-2] respectively require the TOE to implement the command GENERAL AUTHENTICATE / variant ECKA-DH. Please note that the TOE is used by the Mini-HSM User in the operational phase for parts of the TLS key negotiation between the Mini-HSM User and another component or party in the framework of the Smart Metering System. The TOE creates for the Application Server on behalf of the Mini-HSM User the so-called shared secret value Z_{AB} for the pre-master secret. The key derivation function is not part of the TOE.

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1/ECKA-EG)" as specified below:

FCS_CKM.1/ECKA-EG Cryptographic key generation / ElGamal key agreement

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/ECKA-EG The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECKA-EG and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively.

Application Note 7: Based on [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively, the ST author shall exactly reference the applied cryptographic key generation algorithm (as refinement operation for the generic references given in the PP at present). In [TR-03116-3] a reference to [TR-03111] is given where the specification of ECKA-EG can be found.

Application Note 8: [TR-03109-2 B] or [TR-03109-2] respectively require the TOE to implement the command GENERAL AUTHENTICATE / variant ECKA-EG. Please note that the TOE is used in the operational phase for parts of the key agreement of keys that are used afterwards in the framework of content data encryption. The TOE creates for the Application Server on behalf of the Mini-HSM User the so-called shared secret value Z_{AB}. The key derivation function is not part of the TOE.

The TOE shall meet the requirement “Cryptographic key generation (FCS_CKM.1/PACE)” as specified below:

FCS_CKM.1/PACE Cryptographic key generation / PACE

Hierarchical to: No other components.

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

FCS_CKM.1.1/PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm PACE and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively.

Application Note 9: Based on [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively, the ST author shall exactly reference the applied cryptographic key generation algorithm (as refinement operation for the generic references given in the PP at present). In [TR-03116-3] a reference to [TR-03110-2] and [TR-03110-3] with information on the PACE-algorithm specification as relevant for the TOE can be found.

Application Note 10: [TR-03109-2 B] or [TR-03109-2] respectively require the TOE to implement the command GENERAL AUTHENTICATE / variant PACE. The TOE exchanges a shared secret with the Application Server during the PACE protocol. The shared secret is used for deriving the AES session keys for message encryption and authentication (secure messaging) as required by FCS_COP.1/PACE-ENC and FCS_COP.1/PACE-MAC. Secure messaging is carried out for the main data exchange between the Application Server and the TOE.

Application Note 11: This SFR implicitly contains the requirements for the hashing functions used for the key derivation by demanding compliance to [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively.

The TOE shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below:

FCS_CKM.4	Cryptographic key destruction
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	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*].

Application Note 12: The TOE shall destroy the encryption session keys and the message authentication keys negotiated via the PACE protocol after reset or termination of the secure messaging session (trusted channel) or reaching fail secure state according to FPT_FLS.1. The TOE shall clear the memory area of any session keys before starting a new communication with an external entity in a new after-reset-session as required by FDP_RIP.1.

Application Note 13: Explicit deletion of a secret using the DELETE KEY command should also be taken into account by the ST writer.

Application Note 14: This SFR requires that the negotiated shared secret value Z_{AB} as required by FCS_CKM.1/ECKA-DH shall be destroyed after it has been transmitted to the Application Server.

Further, the negotiated shared secret value Z_{AB} as required by

FCS_CKM.1/ECKA-EG shall be destroyed after it has been transmitted to the Application Server.

Cryptographic Operation (FCS_COP)

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1/SIG-ECDSA)" as specified below:

FCS_COP.1/SIG-ECDSA	Cryptographic operation / ECDSA Signature generation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SIG-ECDSA	The TSF shall perform signature generation for the commands PSO COMPUTE DIGITAL SIGNATURE and INTERNAL AUTHENTICATE in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively.

Application Note 15: Based on [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively, the ST author shall exactly reference the applied cryptographic algorithms (as refinement operation for the generic references given in the PP at present). In [TR-03116-3] a reference to [TR-03111] is given where the specification of ECDSA (in particular, signature generation) can be found.

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1/VER-ECDSA)" as specified below:

FCS_COP.1/VER-ECDSA	Cryptographic operation / ECDSA Signature verification
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/VER-ECDSA	The TSF shall perform signature verification for the command PSO VERIFY DIGITAL SIGNATURE in accordance with a

specified cryptographic algorithm ECDSA and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively.

Application Note 16: Based on [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively, the ST author shall exactly reference the applied cryptographic algorithms (as refinement operation for the generic references given in the PP at present). In [TR-03116-3] a reference to [TR-03111] is given where the specification of ECDSA (in particular, signature verification) can be found.

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1/IMP)" as specified below:

FCS_COP.1/IMP Cryptographic operation / Import of Public Keys

Hierarchical to: No other components.

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

FCS_COP.1.1/IMP The TSF shall perform signature verification for the import of Public Keys for the command PSO VERIFY CERTIFICATE in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively.

Application Note 17: Based on [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively, the ST author shall exactly reference the applied cryptographic algorithms (as refinement operation for the generic references given in the PP at present). In [TR-03116-3] a reference to [TR-03111] is given where the specification of ECDSA (in particular, signature verification) can be found.

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1/PACE-ENC)" as specified below:

FCS_COP.1/PACE-ENC Cryptographic operation / AES in CBC mode for secure messaging

Hierarchical to: No other components.

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

FCS_COP.1.1/PACE-ENC The TSF shall perform decryption and encryption for secure messaging and encryption of the nonce in the PACE protocol in accordance with a specified cryptographic algorithm AES in CBC mode and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively.

Application Note 18: Based on [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively, the ST author shall exactly reference the applied cryptographic algorithms (as refinement operation for the generic references given in the PP at present). In [TR-03116-3] a reference to [NIST 197] and [ISO 10116] is given where the specification of AES and the CBC mode can be found.

Application Note 19: This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data and for encrypting the nonce in the first step of PACE. The related session keys (for secure messaging) and key for encryption of the PACE nonce are agreed between the TOE and the Application Server as part of the PACE protocol according to the FCS_CKM.1/PACE.

The TOE shall meet the requirement “Cryptographic operation (FCS_COP.1/PACE-MAC)” as specified below:

FCS_COP.1/PACE-MAC Cryptographic operation / AES-CMAC for secure messaging

Hierarchical to: No other components.

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

FCS_COP.1.1/PACE-MAC The TSF shall perform computation and verification of cryptographic checksum for secure messaging and PACE protocol in accordance with a specified cryptographic algorithm AES-CMAC and cryptographic key sizes [assignment:

cryptographic key sizes] that meet the following: [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively.

Application Note 20: Based on [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively, the ST author shall exactly reference the applied cryptographic algorithms (as refinement operation for the generic references given in the PP at present). In [TR-03116-3] a reference to [NIST 197] and [RFC 4493] is given where the specification of AES and the AES-CMAC can be found.

Application Note 21: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data and for MAC calculation in the fourth step of PACE. The related session keys (for secure messaging and the fourth PACE step) are agreed between the TOE and the Application Server as part of the PACE protocol according to the FCS_CKM.1/PACE.

Random Number Generation (FCS_RNG)

The TOE shall meet the requirement "Random number generation (FCS_RNG.1)" as specified below:

FCS_RNG.1	Random number generation
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].
FCS_RNG.1.2	The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

Application Note 22: Based on [TR-03109-3] or [TR-03116-3] respectively, the ST author shall exactly reference the applied RNG class. The quality metric assigned in element FCS_RNG.1.2 shall be chosen to resist attacks with high attack potential.

Application Note 23: Random numbers are generated for the Application Server and for TOE internal use, in particular for

- support of the TLS handshake (prevention of replay attacks),
- PACE protocol,
- DH key agreement,
- ElGamal key agreement,

- generation of ECC key pairs.

In particular, [TR-03109-2 B] or [TR-03109-2] respectively require the TOE to implement the command GET CHALLENGE for the generation of random numbers that are exported to the external world (here: the Application Server).

In the case that the Application Server implements a deterministic RNG and tears the seed for this RNG (as random number) from the TOE sufficient quality or entropy respectively of the seed has to be taken into account.

6.3 Class FDP: User Data Protection

Access Control Smart Meter Mini-HSM SFP

The **Access Control Smart Meter Mini-HSM SFP** for the Security Module (TOE) in its integration phase and operational phase (see phase 5 and 6 of the TOE life cycle model) is based on the specification of access rules in [TR-03109-2 B].

The SFP takes the following subjects, objects, security attributes and operations into account (refer as well to chapters 3.1 and 3.2):

<u>Subjects:</u>

- external world
- Application Server
- Mini-HSM User

<u>Security attributes for subjects:</u>

- “authenticated via PACE protocol”

<u>Objects:</u>

- key pair
- public key
- certificate

as presented in Table 4.

<u>Security attributes for objects:</u>

- “access rule” (see below)

<u>Operations:</u>

- TOE commands as specified in [TR-03109-2 B] or [TR-03109-2] respectively

The Access Control Smart Meter Mini-HSM SFP controls the access of subjects to objects on the basis of security attributes as for subjects and objects described above. An access rule defines the conditions under which a TOE command sent by a subject is allowed to access the demanded object. Hence, an access rule bound to an object specifies for the TOE commands the necessary permission for their execution on this object.

For the Access Control Smart Meter Mini-HSM SFP, the access rules are defined as prescribed in [TR-03109-2 B]. Please notice that in [TR-03109-2 B] two different options for such Access Control Smart Meter Mini-HSM SFP are specified. The ST author has to choose at least one of those pre-defined options.

In the following the two SFRs directly related to the access control policy and functionality are given:

Access Control Policy (FDP_ACC)

The TOE shall meet the requirement "Complete access control (FDP_ACC.2)" as specified below:

FDP_ACC.2	Complete access control
Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.2.1	The TSF shall enforce the Access Control Smart Meter Mini-HSM SFP on Subjects: • external world • Application Server • Mini-HSM User • [assignment: *list of further subjects, or none*] Objects: • key pair, public key, certificate as presented in Table 4 • [assignment: *list of further objects, or none*] 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.

Access Control Functions (FDP_ACF)

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below:

FDP_ACF.1	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce the Access Control Smart Meter Mini-HSM SFP to objects based on the following:

	Subjects: • external world • Application Server with security attribute “authenticated via PACE protocol” • Mini-HSM User with security attribute “authenticated via PACE protocol” • [assignment: *list of further subjects as listed in FDP_ACC.2 with security attributes, or none*] Objects: • key pair, public key, certificate as presented in Table 4 each with security attribute “access rule” • [assignment: *list of further objects as listed in FDP_ACC.2 with security attribute, or none*].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: Access rules defined in the Access Control Smart Meter Mini-HSM SFP (refer to the definition of the SFP above).
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: No entity shall be able to read out private keys from the TOE.

Stored data integrity (FDP_SDI)

The TOE shall meet the requirement “Stored data integrity monitoring and action (FDP_SDI.2)” as specified below:

FDP_SDI.2	Stored data integrity monitoring and action
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors on all objects, based on the following attributes: [assignment: *user data attributes*].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall not use the data and stop the corresponding process accessing the data, warn the entity connected, [assignment: *other action to be taken, or none*].

Application Note 24: The requirements in FDP_SDI.2.1 specifically apply to the assets as defined in Table 4.

Residual Information Protection (FDP_RIP)

The TOE shall meet the requirement "Subset residual information protection (FDP_RIP.1)" as specified below:

FDP_RIP.1	Subset residual information protection
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: PIN, session keys (immediately after closing related communication session), private cryptographic keys, shared secret value Z_{AB}, ephemeral keys, [assignment: *other data objects, or none*].

Application Note 25: The ST author may want to use iterations of FDP_RIP.1 in order to distinguish between data which must be deleted already upon deallocation and those which can be deleted upon allocation. It is recommended to delete secret/private cryptographic keys and all PIN upon deallocation. For secret user data, deletion upon allocation should be sufficient (depending on the resistance of the concrete TOE against physical attacks).

Application Note 26: Note that the specification of the Security Module allows – in dependency of the chosen access control policy (see Access Control Smart Meter Mini-HSM SFP and its options) – the creation and deletion of key objects during production and operational use. Theoretically it could be possible that a newly created key object uses memory areas which belonged to another key object before. Therefore the Security Module must ensure that contents of the old key object are not accessible by using the new key object.

Export from the TOE (FDP_ETC)

The TOE shall meet the requirement "Export of user data without security attributes (FDP_ETC.1)" as specified below:

FDP_ETC.1	Export of user data without security attributes
Hierarchical to:	No other components.

Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.1.1	The TSF shall enforce the Access Control Smart Meter Mini-HSM SFP when exporting user data, controlled under the SFP, outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.

Import from outside of the TOE (FDP_ITC)

The TOE shall meet the requirement "Import of user data without security attributes (FDP_ITC.1)" as specified below:

FDP_ITC.1	Import of user data without security attributes
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ITC.1.1	The TSF shall enforce the Access Control Smart Meter Mini-HSM SFP when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none.

Inter-TSF User Data Confidentiality Transfer Protection (FDP_UCT)

The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below:

FDP_UCT.1	Basic data exchange confidentiality
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1	The TSF shall enforce the Access Control Smart Meter Mini-HSM SFP to transmit, receive user data in a manner protected

from unauthorised disclosure.

Inter-TSF User Data Integrity Transfer Protection (FDP_UIT)

The TOE shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below:

FDP_UIT.1	Data exchange integrity
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FDP_UIT.1.1	The TSF shall enforce the Access Control Smart Meter Mini-HSM SFP to transmit, receive user data in a manner protected from modification, deletion, insertion, replay errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, replay has occurred.

6.4 Class FIA: Identification and Authentication

User Attribute Definition (FIA_ATD)

The TOE shall meet the requirement "User attribute definition (FIA_ATD.1)" as specified below:

FIA_ATD.1	User attribute definition
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: • for device (Application Server): authentication state gained via PIN (PACE-PIN or HSM-System-PIN respectively used within the PACE protocol), • for human user (Mini-HSM User): authentication state gained via PIN (PACE-PIN or HSM-System-PIN respectively used within the PACE protocol),.

Application Note 27: Mutual authentication between the Application Server or the Mini-HSM User respectively is performed via the PACE protocol between the Application Server and the TOE, refer to the SFR

FCS_CKM.1/PACE.

Specification of Secrets (FIA_SOS)

The TOE shall meet the requirement "Verification of secrets (FIA_SOS.1)" as specified below:

FIA_SOS.1	Verification of secrets
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets **provided by the Application Server for the PACE-PIN or HSM-System-PIN respectively** meet [assignment: *a defined quality metric*].

Application Note 28: Mutual authentication between the Application Server or the Mini-HSM User respectively is performed via the PACE protocol between the Application Server and the TOE, refer to the SFR FCS_CKM.1/PACE. For the PACE-PIN (or HSM-System-PIN respectively) that is required for the PACE protocol the ST author shall define on base of the requirements made in [TR-03109-2 B] the required minimum length for the PACE-PIN (as defined quality metric).

User Authentication (FIA_UAU)

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below:

FIA_UAU.1	Timing of authentication
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow • Establishing a communication channel between the TOE and the external world, • Reading the ATR/ATS, • Reading of data fields containing technical information, • Usage of the TOE's cryptographic functionality and access to assets as far as allowed according to the Access Control Smart Meter Mini-HSM SFP with its access rules defined in [TR-03109-2 B],

- [assignment: *list of TSF-mediated actions, or none*]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 29: Authentication of the Application Server or the Mini-HSM User respectively is performed via the PACE protocol between the Application Server and the TOE, refer to the SFR FCS_CKM.1/PACE.

Application Note 30: Please note that the requirement in FIA_UAU.1 defines that the user (here: the Application Server or the Mini-HSM User respectively) has to be successfully authenticated before allowing use of the TOE's cryptographic functionality or access to the assets stored in and processed by the TOE except where the Access Control Smart Meter Mini-HSM SFP (see chapter 6.3) does not require such preceding authentication. The Access Control Smart Meter Mini-HSM SFP prescribes in detail the access rules for the objects stored in and processed by the TOE. In particular, it is defined for which objects and functions authentication of the Application Server or the Mini-HSM User respectively is required by the TOE.

The TOE shall meet the requirement “Single-use authentication mechanisms (FIA_UAU.4)” as specified below:

FIA_UAU.4	Single-use authentication mechanisms
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to • PACE authentication mechanism.

The TOE shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below:

FIA_UAU.5	Multiple authentication mechanisms
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide • authentication via the PACE protocol,

	• secure messaging in encrypt-then-authenticate mode using PACE session keys to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the following rules: • PACE/PIN based authentication shall be used for authenticating a device (Application Server) or Mini-HSM User respectively and secure messaging in encrypt-then-authenticate mode using PACE session keys shall be used to authenticate its commands if required by the Access Control Smart Meter Mini-HSM SFP.

User Identification (FIA_UID)

The TOE shall meet the requirement “Timing of identification (FIA_UID.1)” as specified below:

FIA_UID.1	Timing of identification
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow • Establishing a communication channel between the TOE and the external world, • Reading the ATR/ATS, • Reading of data fields containing technical information, • Carrying out the PACE protocol according to [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3] or [TR-03116-3] respectively, [TR-03109-2 B] or [TR-03109-2] respectively (by means of command GENERAL AUTHENTICATE), • [assignment: *list of TSF-mediated actions, or none*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

User-Subject Binding (FIA_USB)

The TOE shall meet the requirement “User-subject binding (FIA_USB.1)” as specified below:

FIA_USB.1	User-subject binding
Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: • authentication state for the Application Server or the Mini-HSM User respectively.
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: initial authentication state is set to “not authenticated”.
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: • for device (Application Server): the authentication state is changed to “authenticated Application Server” when the device has successfully authenticated itself by the PACE protocol, • for human user (Mini-HSM User): the authentication state is changed to “authenticated Mini-HSM User” when the user has successfully authenticated himself by the PACE protocol.

6.5 Class FMT: Security Management

Limited Capabilities and Availability (FMT_LIM)

The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1)” as specified below:

FMT_LIM.1	Limited capabilities
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF Data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below:

FMT_LIM.2	Limited availability
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF Data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.

Application Note 31: The SFRs FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF Data to prevent misuse of test features of the TOE over the life cycle phases. The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

(1) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced

or conversely

(2) the TSF is designed with high functionality but is removed or disabled in the product in its user environment.

(3) The combination of both requirements shall enforce the policy.

Specification of Management Functions (FMT_SMF)

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below:

FMT_SMF.1	Specification of Management Functions
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: • Management of key objects by means of commands CREATE KEY, DELETE KEY, ACTIVATE KEY, DEACTIVATE KEY, GENERATE ASYMMETRIC

KEY PAIR, PSO VERIFY CERTIFICATE,
- Management of DFs and EFs by means of commands CREATE DF/EF, ACTIVATE DF/EF, DEACTIVATE DF/EF, DELETE DF/EF, TERMINATE DF/EF, APPEND RECORD (if implemented)
- Management of PIN objects by means of command CHANGE REFERENCE DATA,
- Life cycle management of the TOE by means of command TERMINATE CARD USAGE,
- Update of keys by means of commands GENERATE ASYMMETRIC KEY PAIR, PSO VERIFY CERTIFICATE,
- Update of data by means of commands UPDATE BINARY, UPDATE RECORD,
- [assignment: *list of further management functions to be provided by the TSF, or none*].

Application Note 32: A detailed description of the commands that have to be implemented in the TOE can be found in [TR-03109-2 B] or [TR-03109-2] respectively.

Security Management Roles (FMT_SMR)

The TOE shall meet the requirement "Security Roles (FMT_SMR.1)" as specified below:

FMT_SMR.1	Security Roles
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles • user • authenticated Application Server • authenticated Mini-HSM User • [assignment: *additional authorised identified roles, or none*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.6 Class FPT: Protection of the TSF

TOE Emanation (FPT_EMS)

The TOE shall meet the requirement "TOE Emanation (FPT_EMS.1)" as specified below:

FPT_EMS.1	TOE Emanation
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to PIN, session keys, shared secret value Z_{AB}, ephemeral keys, [assignment: *list of types of TSF data, or none*] and private asymmetric keys of the user, [assignment: *list of types of user data, or none*].
FPT_EMS.1.2	The TSF shall ensure any users are unable to use the following interface circuit surface to gain access to PIN, session keys, shared secret value Z_{AB}, ephemeral keys, [assignment: *list of types of TSF data, or none*] and private asymmetric keys of the user, [assignment: *list of types of user data, or none*].

Application Note 33: The ST writer shall perform the operation in FPT_EMS.1.1 and FPT_EMS.1.2. The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the security module.

Fail Secure (FPT_FLS)

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below:

FPT_FLS.1	Failure with preservation of secure state
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: • power loss, • exposure to operating conditions where therefore a

malfunction could occur,
- detection of physical manipulation or physical probing,
- integrity errors according to FDP_SDI.2,
- insufficient entropy during random number generation,
- failure detected by the TSF according to FPT_TST.1,
- errors during processing cryptographic operations,
- errors during evaluation of access rules, and
- [assignment*: list of other types of failures in the TSF, or none*].

TSF Physical Protection (FPT_PHP)

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below:

FPT_PHP.3	Resistance to physical attack
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing to the all TOE components implementing the TSF by responding automatically such that the SFRs are always enforced.

Application Note 34: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

TSF Self Test (FPT_TST)

The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below:

FPT_TST.1	TSF testing
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up, 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.

6.7 Class FTP: Trusted path/channels

Inter-TSF trusted channel (FTP_ITC)

The TOE shall meet the requirement “Inter-TSF trusted channel (FTP_ITC.1)” as specified below:

FTP_ITC.1	Inter-TSF trusted channel
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.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.1.2	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Application Server according to the Access Control Smart Meter Mini-HSM SFP with its access rules defined in [TR-03109-2 B].

6.8 Security Assurance Requirements for the TOE

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

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

Assurance Class	Assurance Component	
Class ADV: Development	Architectural design	(ADV_ARC.1)
	Functional specification	(ADV_FSP.4)
	Implementation representation	(ADV_IMP.1)
	TOE design	(ADV_TDS.3)
Class AGD: Guidance documents	Operational user guidance	(AGD_OPE.1)
	Preparative user guidance	(AGD_PRE.1)

Assurance Class	Assurance Component	
Class ALC: Life-cycle support	CM capabilities	(ALC_CMC.4)
	CM scope	(ALC_CMS.4)
	Delivery	(ALC_DEL.1)
	Development security	(ALC_DVS.1)
	Life-cycle definition	(ALC_LCD.1)
	Tools and techniques	(ALC_TAT.1)
Class ASE: Security Target evaluation	Conformance claims	(ASE_CCL.1)
	Extended components definition	(ASE_ECD.1)
	ST introduction	(ASE_INT.1)
	Security objectives	(ASE_OBJ.2)
	Derived security requirements	(ASE_REQ.2)
	Security problem definition	(ASE_SPD.1)
	TOE summary specification	(ASE_TSS.1)
Class ATE: Tests	Coverage	(ATE_COV.2)
	Depth	(ATE_DPT.1)
	Functional tests	(ATE_FUN.1)
	Independent testing	(ATE_IND.2)
Class AVA: Vulnerability Assessment	Vulnerability analysis	(AVA_VAN.5)

Table 9: Assurance Requirements

6.8.1 Refinements of the TOE Security Assurance Requirements

The following refinements shall support the comparability of evaluations according to this Protection Profile. The mandatory documents themselves mentioned below shall be consulted for exact details and overrule the refinements in case of any inconsistency (e.g. due to updates).

The Refinement is pointed out by using the **bold** type.

The Common Criteria assurance component of the family AVA_VAN (Advanced methodical vulnerability analysis) addresses "A methodical vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities."

Since [CEM] does not describe a specific methodical approach available guidance for the present product type shall be used for the vulnerability analysis of the TOE. Especially supporting documents for this product type available for the application of the Common Criteria or being part of the SOG-IS MRA respectively shall be considered.

The following text reflects the requirements of the selected component AVA_VAN.5:

Developer action elements:

AVA_VAN.5.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.5.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.5.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.5.3E The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.5.4E The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

Refinement

For the vulnerability analysis of the TOE the JIWG approved supporting documents for the IT-Technical Domain “Smart cards & similar devices” shall be taken into account.

In addition, for the evaluation and assessment of the TOE's random number generation functionality for the random number generator classes DRG.3, DRG.4, PTG.2 and PTG.3 the scheme documents [AIS 20] or [AIS 31] respectively or an evaluation approach agreed under the umbrella of the SOG-IS MRA shall be applied.

6.9 Security Requirements Rationale

6.9.1 Security Functional Requirements Rationale

6.9.1.1 Overview

This chapter proves that the set of security functional requirements (SFR) is suited to fulfil the security objectives for the TOE as described in chapter 4.1 and that each SFR can be traced back to the security objectives for the TOE. Each security objective for the TOE is reached by the SFRs, and at least one security objective exists for each security functional requirement.

The following table gives an overview how the security objectives for the TOE are addressed by the security functional requirements.

	O.Integrity	O.Confidentiality	O.Authentication	O.AccessControl	O.KeyManagement	O.TrustedChannel	O.Leakage	O.PhysicalTampering	O.AbuseFunctionality	O.Malfunction	O.Sign	O.KeyAgreementDH	O.KeyAgreementEG	O.Random	O.PACE
FCS_CKM.1/ECC					X						X			X	
FCS_CKM.1/ECKA-DH												X		X	
FCS_CKM.1/ECKA-EG													X	X	
FCS_CKM.1/PACE	X	X	X	X		X								X	X
FCS_CKM.4					X						X	X	X		X
FCS_COP.1/SIG-ECDSA											X				
FCS_COP.1/VER-ECDSA											X				
FCS_COP.1/IMP					X						X				
FCS_COP.1/PACE-ENC		X				X									X
FCS_COP.1/PACE-MAC	X					X									X
FCS_RNG.1												X	X	X	X
FDP_ACC.2		X		X											
FDP_ACF.1		X		X											
FDP_SDI.2	X										X	X	X		X
FDP_RIP.1					X						X	X	X	X	X
FDP_ETC.1					X										
FDP_ITC.1					X										
FDP_UCT.1		X				X									
FDP_UIT.1	X					X									
FIA_ATD.1				X											
FIA_SOS.1			X												
FIA_UAU.1				X											

	O.Integrity	O.Confidentiality	O.Authentication	O.AccessControl	O.KeyManagement	O.TrustedChannel	O.Leakage	O.PhysicalTampering	O.AbuseFunctionality	O.Malfunction	O.Sign	O.KeyAgreementDH	O.KeyAgreementEG	O.Random	O.PACE
FIA_UAU.4			X												
FIA_UAU.5			X												
FIA_UID.1				X											
FIA_USB.1				X											
FMT_LIM.1									X						
FMT_LIM.2									X						
FMT_SMF.1				X	X										
FMT_SMR.1				X											
FPT_EMS.1		X					X	X			X	X	X	X	X
FPT_FLS.1	X						X	X		X	X	X	X	X	X
FPT_PHP.3		X					X	X		X	X	X	X	X	X
FPT_TST.1	X						X	X		X	X	X	X	X	X
FTP_ITC.1	X	X				X									

Table 10: Fulfilment of Security Objectives

The following chapter provides a detailed justification for this mapping as required to show the suitability and sufficiency of the security functional requirements to cope with the security objectives for the TOE.

6.9.1.2 Rationale for the Fulfilment of the Security Objectives for the TOE

In the following, a detailed justification as required to show the suitability and sufficiency of the security functional requirements to achieve the security objectives defined for the TOE is given.

O.Integrity

The security objective **O.Integrity** is met by the SFR **FDP_SDI.2** that defines requirements around the integrity protection for data stored in the TOE. In addition, the SFRs **FPT_TST.1** and **FPT_FLS.1** which guarantee for self testing by the TOE in particular in view of integrity and preservation of a secure failure state in the case of a detected integrity error are present in order to reach this security objective. Furthermore, the trusted channel between the TOE and the Application Server used for the exchange of sensitive data contributes to the data integrity at the TOE's interface. Herefore, the SFRs **FCS_COP.1/PACE-MAC, FDP_UIT.1**, **FTP_ITC.1** and **FCS_CKM.1/PACE** are involved.

O.Confidentiality

The security objective **O.Confidentiality** is met by the SFRs **FDP_ACC.2** and **FDP_ACF.1** controlling the access to objects stored in or processed by the TOE. The security objective is in addition supported by the SFRs **FPT_EMS.1** and **FPT_PHP.3**. Furthermore, the trusted channel between the TOE and the Application Server used for the exchange of sensitive data contributes to the data confidentiality at the TOE's interface. Herefore, the SFRs **FCS_COP.1/PACE-ENC, FDP_UCT.1**, **FTP_ITC.1** and **FCS_CKM.1/PACE** are involved.

O.Authentication

The security objective **O.Authentication** is addressed by the SFRs **FIA_UAU.4** and **FIA_UAU.5**. Furthermore, in view of the cryptographic functionality of the authentication mechanism: For the PACE authentication between the TOE and the Application Server or the Mini-HSM User respectively the SFRs **FCS_CKM.1/PACE** and **FIA_SOS.1** are of relevance.

O.AccessControl

The security objective **O.AccessControl** is directly addressed by the SFRs **FDP_ACC.2** and **FDP_ACF.1** which enforce the Access Control Smart Meter Mini-HSM SFP defined in chapter 6.3. The SFR **FMT_SMF.1** covers the management functions provided by the TOE. A successful authentication for the access to objects as deposited in the Access Control Smart Meter Mini-HSM SFP is realised via the SFR **FCS_CKM.1/PACE** for performing the authentication process. The SFRs **FIA_ATD.1**, **FIA_USB.1**, **FIA_UID.1**, and **FIA_UAU.1** regulate in addition the access to the TOE's functionality and the objects stored in and processed by the TOE. Distinguishing between different roles is realised via the SFR **FMT_SMR.1**. Refer in addition to the SFRs that are assigned to the security objective **O.Authentication**.

O.KeyManagement

The security objective **O.KeyManagement** is directly addressed by the SFR **FMT_SMF.1** which covers in particular the management functions related to key management and by the SFR **FCS_CKM.1/ECC** for the generation of ECC key pairs. The export or import respectively of public keys is reached by the SFRs **FCS_COP.1/IMP**, **FDP_ITC.1** and **FDP_ETC.1**. The deletion of keys is realised by the SFRs **FDP_RIP.1** and **FCS_CKM.4**.

O.TrustedChannel

The security objective **O.TrustedChannel** is directly realised by the SFRs **FCS_COP.1/PACE-ENC** and **FDP_UCT.1** (for confidentiality of the data exchange between the TOE and the Application Server) and **FCS_COP.1/PACE-MAC** and **FDP_UIT.1** (for integrity of the data exchange between the TOE and the Application Server). Setting up the trusted channel is addressed by the SFR **FTP_ITC.1**, and the session keys used for the trusted channel are negotiated via the SFR **FCS_CKM.1/PACE**.

O.Leakage

The security objective **O.Leakage** is directly addressed by the SFR **FPT_EMS.1** and is supported by the SFRs **FPT_FLS.1**, **FPT_PHP.3** and **FPT_TST.1** which support the correct and secure operation of the TOE.

O.PhysicalTampering

The security objective **O.PhysicalTampering** is directly addressed by the SFR **FPT_PHP.3** and is supported by the SFRs **FPT_EMS.1**, **FPT_FLS.1** and **FPT_TST.1** which support the correct and secure operation of the TOE.

O.AbuseFunctionality

The security objective **O.AbuseFunctionality** is directly met by a combination of the SFRs **FMT_LIM.1** and **FMT_LIM.2** which prevent misuse of test functionality of the TOE or other features which may not be available during the TOE operational use phase. **FMT_LIM.1** further ensures that the TOE does not provide any untested functionality.

O.Malfunction

The security objective **O.Malfunction** is directly addressed by the SFRs **FPT_FLS.1, FPT_PHP.3** and **FPT_TST.1** which support the correct and secure operation of the TOE.

O.Sign

The security objective **O.Sign** is covered in view of its cryptographic functionality by the SFRs **FCS_COP.1/SIG-ECDSA** and **FCS_COP.1/VER-ECDSA**. The key generation for signature keys is covered by the SFR **FCS_CKM.1/ECC**, the import of signature verification keys is covered by the **SFR FCS_COP.1/IMP**. In addition, the correct functioning and security of the digital signature generation and verification operation is addressed by the SFRs **FPT_EMS.1**, **FPT_FLS.1**, **FPT_PHP.3**, **FPT_TST.1**, **FDP_RIP.1**, **FDP_SDI.2** and **FCS_CKM.4** which support the correct and secure operation of the TOE including memory preparation and key destruction.

O.KeyAgreementDH

The security objective **O.KeyAgreementDH** is covered in view of its cryptographic functionality by the SFRs **FCS_CKM.1/ECKA-DH** and **FCS_RNG.1**. In addition, the correct functioning and security of the DH key agreement operation is addressed by the SFRs **FPT_EMS.1**, **FPT_FLS.1**, **FPT_PHP.3**, **FPT_TST.1**, **FDP_RIP.1**, **FDP_SDI.2** and **FCS_CKM.4** which support the correct and secure operation of the TOE including memory preparation and key destruction.

O.KeyAgreementEG

The security objective **O.KeyAgreementEG** is covered in view of its cryptographic functionality by the SFRs **FCS_CKM.1/ECKA-EG** and **FCS_RNG.1**. In addition, the correct functioning and security of the ElGamal key agreement operation is addressed by the SFRs **FPT_EMS.1**, **FPT_FLS.1**, **FPT_PHP.3**, **FPT_TST.1**, **FDP_RIP.1**, **FDP_SDI.2** and **FCS_CKM.4** which support the correct and secure operation of the TOE including memory preparation and key destruction.

O.Random

The security objective **O.Random** is covered in view of its functionality directly by the SFR **FCS_RNG.1** and implicitly by the SFRs **FCS_CKM.1/ECC**, **FCS_CKM.1/ECKA-DH**, **FCS_CKM.1/ECKA-EG** and **FCS_CKM.1/PACE**. In addition, the correct functioning and security of the random number generation operation is addressed by the SFRs **FPT_EMS.1**, **FPT_FLS.1**, **FPT_PHP.3**, **FPT_TST.1** and **FDP_RIP.1** which support the correct and secure operation of the TOE.

O.PACE

The security objective **O.PACE** is covered in view of its cryptographic functionality by the SFRs **FCS_CKM.1/PACE**, **FCS_COP.1/PACE-ENC, FCS_COP.1/PACE-MAC** and **FCS_RNG.1**. In addition, the correct functioning and security of the PACE protocol operation is addressed by the SFRs **FPT_EMS.1**, **FPT_FLS.1**, **FPT_PHP.3**, **FPT_TST.1**, **FDP_RIP.1**, **FDP_SDI.2** and **FCS_CKM.4** which support the correct and secure operation of the TOE including memory preparation and key destruction.

6.9.1.3 SFR Dependency Rationale

The following table summarises all TOE security functional requirements dependencies of this PP and demonstrates that they are either fulfilled, or a reference to the following chapter 6.9.1.4 is given where a justification for the non-fulfilment of the respective dependency can be found.

SFR	Dependencies	Fulfilled by
FCS_CKM.1/ECC	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/SIG-ECDSA FCS_CKM.4 Please refer to chapter 6.9.1.4 for missing dependencies.
FCS_CKM.1/ECKA-DH	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 Please refer to chapter 6.9.1.4 for missing dependencies.
FCS_CKM.1/ECKA-EG	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 Please refer to chapter 6.9.1.4 for missing dependencies.
FCS_CKM.1/PACE	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/PACE-ENC FCS_COP.1/PACE-MAC FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1/ECC FCS_CKM.1/ECKA-DH FCS_CKM.1/ECKA-EG FCS_CKM.1/PACE FDP_ITC.1

SFR	Dependencies	Fulfilled by
FCS_COP.1/SIG-ECDSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/ECC FCS_CKM.4
FCS_COP.1/VER-ECDSA	[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	FDP_ITC.1 FCS_CKM.4
FCS_COP.1/IMP	[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	FDP_ITC.1 FCS_CKM.4
FCS_COP.1/PACE-ENC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/PACE FCS_CKM.4
FCS_COP.1/PACE-MAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/PACE FCS_CKM.4
FCS_RNG.1	-	-
FDP_ACC.2	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.2 Please refer to chapter 6.9.1.4 for missing dependencies.
FDP_SDI.2	-	-
FDP_RIP.1	-	-
FDP_ETC.1	[FDP_ACC.1 Subset access control, or	FDP_ACC.2

SFR	Dependencies	Fulfilled by
	FDP_IFC.1 Subset information flow control]	
FDP_ITC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.2 Please refer to chapter 6.9.1.4 for missing dependencies.
FDP_UCT.1	[FTP_ICT.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FTP_ICT.1 FDP_ACC.2
FDP_UIT.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ICT.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	FDP_ACC.2 FTP_ICT.1
FIA_ATD.1	-	-
FIA_SOS.1	-	-
FIA_UAU.1	FIA_UID.1 Timing if identification	FIA_UID.1
FIA_UAU.4	-	-
FIA_UAU.5	-	-
FIA_UID.1	-	-
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_LIM.1	FMT_LIM.2 Limited availability	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1 Limited capability	FMT_LIM.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1 Timing if identification	FIA_UID.1
FPT_EMS.1	-	-
FPT_FLS.1	-	-
FPT_PHP.3	-	-
FPT_TST.1	-	-
FTP_ITC.1	-	-

Table 11: SFR Dependencies

6.9.1.4 Justification for Missing Dependencies

FCS_CKM.1/ECC:

The ECC key pairs generated via the SFR FCS_CKM.1/ECC can be used afterwards by the Application Server or the Mini-HSM User respectively for digital signature generation, DH key agreement or ElGamal key agreement respectively. The related cryptographic operation is covered by the SFR FCS_COP.1/SIG-ECDSA, FCS_CKM.1/ECKA-DH or FCS_CKM.1/ECKA-EG respectively. For signature keys, the required dependency of FCS_CKM.1/ECC to [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] is directly fulfilled by the SFR FCS_COP.1/SIG-ECDSA. For key pairs intended to be used for DH key agreement or ElGamal key agreement, the required dependency of FCS_CKM.1/ECC to [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] is replaced without loss of security information by the SFRs FCS_CKM.1/ECKA-DH or FCS_CKM.1/ECKA-EG respectively.

FCS_CKM.1/ECKA-DH:

The dependency to [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] is omitted as the TOE only generates and emits the shared secret value Z_{AB} and the key derivation function for deriving the keys is carried out by the Application Server. Ephemeral keys generated by the TOE during the key agreement protocol are not used anymore by the TOE for further cryptographic operations.

FCS_CKM.1/ECKA-EG:

The dependency to [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] is omitted as the TOE only generates and emits the shared secret value Z_{AB} and the key derivation function for deriving the keys is carried out by the Application Server. Ephemeral keys generated by the TOE during the key agreement protocol are not used anymore by the TOE for further cryptographic operations.

FDP_ACF.1:

The dependency to FMT_MSA.3 is omitted as the security attributes for the security policy are fixed during development of the TOE and cannot be altered afterwards.

FDP_ITC.1:

The dependency to FMT_MSA.3 is omitted as the security attributes for the security policy are fixed during development of the TOE and cannot be altered afterwards.

6.9.2 Security Assurance Requirements Rationale

6.9.2.1 Reasoning for Choice of Assurance Level

The decision on the assurance level has been mainly driven by the assumed attack potential. In order to be state-of the-art and even if intended to be integrated as a security module in a Smart Meter Mini-HSM and to be applied by the Mini-HSM User in a secured environment and under control of this user it is assumed that 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.

6.9.2.2 Dependencies of Assurance Components

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

6.9.3 Security Requirements – Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form an internally consistent whole.

a) SFRs

The dependency analysis in chapter 6.9.1.4 for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in the chapters 6.1 to 6.7 are also treated in a consistent way: The SFRs impacting them do not require any contradictory property and behaviour of these ‘shared’ items.

b) SARs

The assurance package EAL 4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in chapter 6.9.2.2 shows that the assurance requirements are internally consistent, because all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met – an opportunity having been shown not to arise in chapters 6.9.1.4 and 6.9.2. Furthermore, as also discussed in chapter 6.9.2, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

7. Appendix

7.1 Acronyms

Term	Description
ATR	Answer To Reset
ATS	Answer To Select
AUTH	External Authentication
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DEMA	Differential Electromagnetic Analysis
DF	Dedicated File
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECKA	Elliptic Curve Key Agreement
ECKA-DH	Elliptic Curve Key Agreement - Diffie-Hellman
ECKA-EG	Elliptic Curve Key Agreement - ElGamal
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary File
EMT	Autorisierter Externer Marktteilnehmer
Enc	Encryption
ENC	Content Data Encryption
GW	Gateway
GWA	Smart Meter Gateway Administrator, Gateway Administrator
GWH	Gateway-Hersteller, Gateway Developer
HAN	Home Area Network
HSM	Hardware Security Module
ID	Identifier
IT	Information Technology
JIWG	Joint Interpretation Working Group

Term	Description
KDF	Key Derivation Function
LMN	Local Metrological Network
MRA	Mutual Recognition Agreement
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PKI	Public Key Infrastruktur / Public Key Infrastructure
PP	Protection Profile
SAR	Security Assurance Requirement
SecMod	Security Module / Sicherheitsmodul
SEMA	Simple Electromagnetic Analysis
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SIG	Content Data Signature
Sign	Signature
SM	Smart Meter
SMGW	Smart Meter Gateway
SM-PKI	Smart Metering - Public Key Infrastruktur (SM-PKI)
SOG-IS	Senior Officials Group Information Systems Security
SPA	Simple Power Analysis
ST	Security Target
TLS	Transport Layer Security
TOE	Target Of Evaluation
TR	Technische Richtlinie
TSF	TOE Security Functionality
WAN	Wide Area Network

Table 12: Acronyms

7.2 Glossary

Term	Description
Authenticity	Property that an entity is what it claims to be.

Term	Description
Authorized External Entity	Autorisierter Externer Marktteilnehmer (EMT).
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Consumer	End user of electricity, gas, water or heat (according to [CEN]).
External Entity	See chapter 3.1.
Gateway Administrator	Smart Meter Gateway Administrator. See chapter 1.5 and 3.1.
Home Area Network (HAN)	In-house LAN which interconnects domestic equipment and can be used for energy management purposes (according to [CEN]).
Integrator	See chapter 1.5 and 3.1.
Integrity	Property that sensitive data has not been modified or deleted in an unauthorised and undetected manner.
IT-System	Computersystem.
LAN, Local Area Network	Data communication network, connecting a limited number of communication devices (Meters and other devices) and covering a moderately sized geographical area within the premises of the consumer. In the context of this PP the term LAN is used as a hypernym for HAN and LMN.
Local Metrological Network (LMN)	In-house LAN which interconnects metrological equipment (i.e. Meters) (according to [CEN]).
Metering Service Provider	Service provider responsible for installing and operating measuring devices in the area of Smart Metering.

Table 13: Glossary

7.3 Mapping from English to German Terms

English Term	German Term
Authorized External Entity	Autorisierter Externer Marktteilnehmer (EMT)
CLS, Controllable Local System	Energiemanagementsysteme und dezentral steuerbare Verbraucher- oder Erzeugersysteme

English Term	German Term
Consumer	Anschlussnutzer, Letztverbraucher (im verbrauchenden Sinne), u. U. auch Einspeiser
Gateway	Kommunikationseinheit
Gateway Operator	Betreiber der Kommunikationseinheit
Grid	Netz (für Strom/Gas/Wasser)
LAN, Local Area Network	Lokales Netz (für Kommunikation)
LMN, Local Metrological Network	Lokales Messeinrichtungsnetz
Meter	Messeinrichtung (Teil eines Messsystems)
Meter Operator	Messstellenbetreiber
MSP, Metering Service Provider	Messdienstleister
Security Module	Sicherheitsmodul (z.B. eine Smart Card)
Smart Meter Smart Metering Smart Metering System[10]	Intelligente, in ein Kommunikationsnetz eingebundene, elektronische Messeinrichtung (Messsystem)
TOE	EVG (Evaluierungsgegenstand)
WAN, Wide Area Network	Weitverkehrsnetz (für Kommunikation)

Table 14: Mapping of Terms

7.4 References

7.4.1 Common Criteria

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

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

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

[AIS 20] Anwendungshinweise und Interpretationen zum Schema (AIS): Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, BSI, current version

[AIS 31] Anwendungshinweise und Interpretationen zum Schema (AIS): Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, BSI, current version

7.4.2 Protection Profiles

[PP 73] Common Criteria Protection Profile for the Gateway of a Smart Metering System, registered under BSI-CC-PP-0073(-Vx), BSI, current version

[PP 77] Common Criteria Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), registered under BSI-CC-PP-0077(-Vx), BSI, current version

7.4.3 Technical Guidelines and Specifications

[TR-03109] BSI TR-03109 (Dachdokument), BSI, current version

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

[TR-03109-2] BSI TR-03109-2 Smart Meter Gateway - Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, BSI, Version 1.1, 2014

[TR-03109-2 B] BSI TR-03109-2 Anhang B: Smart Meter Mini-HSM - Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, BSI, Version 1.0, 2017

[TR-03109-3] BSI TR-03109-3 Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, BSI, current version

[TR-03109-4] BSI TR-03109-4 Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways, BSI, current version

[TR-03109-6] BSI TR-03109-6 Smart Meter Gateway Administration, BSI, current version

[SM-CP] Certificate Policy der Smart Metering PKI, BSI, current version

[ISO 7816-4] ISO/IEC 7816-4: Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange, ISO/IEC, IS 2013

[ISO 7816-8] ISO/IEC 7816-8: Identification cards - Integrated circuit cards - Part 8: Commands for security operations, ISO/IEC, IS 2004

[ISO 7816-9] ISO/IEC 7816-9: Identification cards - Integrated circuit cards - Part 9: Commands for card management, ISO/IEC, IS 2004

[TR-03111] BSI TR-03111 Elliptic Curve Cryptography, BSI, Version 2.0, 2012

[TR-03110-1] BSI TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 1 - eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.20, 2015

[TR-03110-2] BSI TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS), BSI, Version 2.20, 2015

[TR-03110-3] BSI TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, BSI, Version 2.20, 2015

[TR-03116-3] BSI TR-03116-3 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3: Intelligente Messsysteme, BSI, current version

[NIST 197] NIST FIPS 197 - Advanced Encryption Standard (AES), 2001

[ISO 10116] ISO/IEC 10116 Information technology - Security techniques - Modes of operation for an n-bit block cipher, 2006

[RFC 4493] IETF RFC 4493 J. H. Song, J. Lee, T. Iwata: The AES-CMAC Algorithm, 2006

7.4.4 Other Sources

[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