T · · Systems ·

Specification of the Security Target TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE

Version: 1.0.1/20170929

Dokumentenkennung:	CD.TCOS.ASE
Dateiname:	ASE TCOS Secure Crypto Module Version 1.0 Release 1.docm
Stand:	29.09.2017
Version:	1.0.1
Hardware Basis:	P60C144PVE
Autor:	Ernst-G. Giessmann, Markus Blick
Geltungsbereich:	TeleSec Entwicklungsgruppe
Vertraulichkeitsstufe:	**Öffentlich**

History

Version	Date	Remark
1.0.1	2017-09-29	Final version

Contents

1 ST Introduction 5
1.1 ST Reference 5
1.2 TOE Reference 5
1.3 TOE Overview 5
1.4 TOE Description 7
1.4.1 TOE Definition 7
1.4.2 TOE security features for operational use 7
1.4.3 TOE Type 7
1.4.4 TOE Boundaries 8
1.4.5 Non-TOE hardware/software/firmware 8
1.5 Life Cycle Phases Mapping 9
2 Conformance Claim 12
2.1 CC Conformance Claims 12
2.2 PP Claims 12
2.3 Package Claims 12
2.4 Conformance Rationale 12
3 Security Problem Definition 14
3.1 Subjects and external entities 14
3.2 Assets 15
3.3 Assumptions 17
3.4 Threats 18
3.5 Organizational Security Policies 21
4 Security Objectives 23
4.1 Security Objectives for the TOE 23
4.2 Security Objectives for the Operational Environment 25
4.3 Security Objective Rationale 28
5 Extended Components Definition 30
5.1 FCS_RNG Generation of random numbers 30
5.2 FMT_LIM Limited capabilities and availability 31
5.3 FPT_EMS TOE Emanation 32
6 Security Requirements 33
6.1 Security Functional Requirements for the TOE 33
6.1.1 Overview 33
6.1.2 Class FCS Cryptographic Support 34
6.1.3 Class FDP User Data Protection 43
6.1.4 Class FIA Identification and Authentication 47
6.1.5 Class FMT Security Management 50
6.1.6 Class FPT Protection of the Security Functions 51
6.1.7 Class FTP Trusted Path/Channels 53
6.2 Security Assurance Requirements for the TOE 54

6.3 Security Requirements Rationale 54
6.3.1 Security Functional Requirements Rationale 54
6.3.2 Rationale for SFR's Dependencies 55
6.3.3 Security Assurance Requirements Rationale 57
7 TOE Summary Specification 59
7.1 Digital Signature Generation 59
7.2 Digital Signature Verification 59
7.3 Key Agreement for TLS 60
7.4 Key Agreement for Content Data Encryption 60
7.5 Key Pair Generation 60
7.6 Random Number Generation 61
7.7 Component Authentication via the PACE-Protocol with Negotiation of Session Keys 61
7.8 Secure Messaging 61
7.9 Secure Storage of Key Material and further data relevant for the AS or the Mini-HSM User respectively 61
7.10 TOE SFR Statements 62
7.11 Statement of Compatibility 65
7.11.1 Relevance of Hardware TSFs 65
7.11.2 Security Requirements 65
7.11.3 Security Objectives 68
7.11.4 Compatibility: TOE Security Environment 69
7.11.5 Organizational Security Policies 70
7.11.6 Conclusion 71
7.12 Assurance Measures 71
Appendix Glossary and Acronyms 73
References 76

1 ST Introduction

1 This section provides document management and overview information that are required a potential user of the TOE to determine, whether the TOE fulfils her requirements.

1.1 ST Reference

2

Title:	Specification of the Security Target TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE
TOE:	TCOS Secure Crypto Module Version 1.0 Release 1/ P60C144PVE
Sponsor:	T-Systems International GmbH
Editor(s):	Ernst-G. Giessmann, Markus Bick, T-Systems
CC Version:	3.1 (Revision 4)
Assurance Level:	EAL4 augmented.
General Status:	Final Document
Version Number:	1.0.1
Date:	2017-09-29
Certification ID:	BSI-DSZ-CC-1035
Keywords:	Smart Meter, Secure Crypto Module

3 TCOS is the operating system of smart cards developed at T-Systems International GmbH. They are used in different security environments and infrastructures and are therefore subject of Common Criteria evaluations.

1.2 TOE Reference

4 The Security Target refers to the Product “TCOS Secure Crypto Module Version 1.0 Release 1/P60C144PVE” (TOE) of T-Systems for CC evaluation.

5 In some context the hardware base may be relevant, and, if so, the TOE will be identified in more detail as the “TCOS Secure Crypto Module Version 1.0 Release 1/ P60C144PVE", otherwise the notion "TCOS Secure Crypto Module Version 1.0 Release 1" will be used, indicating that this context applies to any realization regardless which hardware base is used.

1.3 TOE Overview

6 The Target of Evaluation (TOE) addressed by the current Security Target is an composite product comprising hardware and software used by e.g. a so called Hardware Security Module (HSM). It is conform to the Protection Profile [PP0095-SecMod] for the Security Module of a so called Smart Meter Mini-HSM. This modules are used as secure crypto storage mediums with integrated cryptographic service functions like signature creation or key agreement.

7 The device which integrates the SeCMod (in the later called Smart Meter Mini-HSM) provides the functionality of the TOE as a cryptographic service provider for different cryptographic functionalities based on elliptic curve cryptography as the generation and verification of digital signatures and key agreement in the TLS framework, for content data signature and content data encryption to an external instance, in the later called the Application Server (AS).

8 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.

9 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.

10 The reader should be familiar with the requirements given in the Technical Guidelines for Smart Energy ([TR03109]). This TOE implements option 2 of the described access rule policies specified in [TR03109-2 B] .

11 During operational use phase the AS, which comunicates with the SeCMod via the Mini-HSM, is the default user. Additional users are the Mini-HSM - User and the SeCMod Product Manufacturer.

12 The TOE serves as a cryptographic service provider for

- generation and verification of digital signatures,
- key agreement used for TLS,
- content data signature and content data encryption,
- secure storage for cryptographic keys and certificates, and
- random number generation.

13 To protect the user data the communication between AS's software and the TOE is encrypted and protected by means of secure messaging. This secure channel is established by the well known and proven as secure PACE protocol executed between the AS's software and the TOE. It requires the knowledge of a secret, that may be even weak, but it establishes strong session keys. The derived key[1] is called PACE key.

14 The PACE protocol provides also component authentication between the AS and the TOE with negotiation of session keys for secure messaging.

15 The cryptographic algorithms and security parameters of these algorithms used by the TOE are defined outside the TOE in the Smart Metering Systems Infrastructure (cf. [TR03109, part 3]). The TOE supports the standardized domain parameters brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 (cf. [RFC5639]) and the NIST curves P-256, P-384 ([FIPS186]) listed in [TR03116-3, section 2.2 Table 3].

16 The Secure Crypto Module is integrated into a package of HVQFN32 (SOT617-3) format.

17 The TOE follows the composite evaluation aspects ([AIS36]). The Security Target of the underlying platform ([HWST]) claims conformance to Smartcard IC Platform Protection Profile ([PP0035-ICC]).

18 This composite ST is based on the ST of the underlying platform ([HWST]). The compatibility of the Life Cycle Model of the Protection Profile [PP0095-SecMod] and the Life Cycle Model required by [PP0035-ICC] will be shown in 1.5.

[1] denoted as K_{π}. in [TR03110-2, section 4.2]

1.4 TOE Description

1.4.1 TOE Definition

19 The TOE comprises of

- the circuitry of the chip including all IC Dedicated Software being active in the Operational Phase of the TOE (the integrated circuit, IC),
- the IC Embedded Software (operating system),
- the *Security Module* application, and
- the associated guidance documentation.

20 The components of the TOE are therefore the hardware (IC), the operating system TCOS (OS) and the dedicated files for the Security Module application in a file system. A detailed description of the parts of TOE will be given in TOE Design Specification covered by ADV_TDS.

21 The corresponding keys and authentication data used in life cycle phase 5 are delivered securely to the Integrator.

1.4.2 TOE security features for operational use

22 The following TOE security features are the most significant for its operational use:

- 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.

1.4.3 TOE Type

23 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.

1.4.4 TOE Boundaries

1.4.4.1 TOE Physical Boundaries

24 The TOE comprises a smart card chip that consists of hardware containing a microprocessor, (CPU), a coprocessor for special (cryptographic) operations, a random number generator, volatile and non-volatile memory, and associated software, packaged and embedded in a carrier.

25 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 [TR03109-2 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.

1.4.4.2 TOE Logical Boundaries

26 The logical boundaries of the TOE can be identified by its security functionalities:

- Digital Signature Generation,
- Digital Signature Verification,
- Key Agreement for Transport Layer Security (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 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.

27 All these security features are used by the AS 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.

28 The TOE and its (security) functionality is specified from a technical point of view in [TR03109-2 B]. A detailed description of the (security) functionality provided by the TOE for use by the AS or the Mini-HSM User repectively 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 [TR03109-2 B].

1.4.5 Non-TOE hardware/software/firmware

29 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.

30 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.

31 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 [TR03109-2 B].

1.5 Life Cycle Phases Mapping

32 Following the protection profile PP-0095 [PP0095-SecMod, 1.5] the life cycle phases of a TCOS Security Module can be divided into the following six phases:

Phase 1: Security Module Embedded Software Development
Phase 2: IC Development
Phase 3: IC Manufacturing, Packaging and Testing
Phase 4: Security Module Product Finishing Process
Phase 5: Security Module Integration
Phase 6: Security Module End-Usage

Life cycle phase 1 “Security Module Embedded Software Development”

33 The TOE is developed in phase 1. The Platform Developer according to [AIS36] develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

34 The SeCMod 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 initialization and pre-personalization requirements.

35 The purpose of the SeCMod 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.

Life cycle phase 2 “IC Development”

36 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.

Life cycle phase 3 “IC Manufacturing, Packaging and Testing”

37 The IC Manufacturer is responsible for producing the IC including IC manufacturing, IC pre-personalization, implementing/installing the Security Module Embedded Software in the IC and IC testing.

38 The Protection Profile [PP0095-SecMod] allows for modifications in the processes performed in the life cycle phases 3 and 4. This applies to the TOE, i.e. the IC packaging will not be assigned to this phase, but will be performed in the next phase 4 after initialization.

39 As the packing is not finished in this phase there is no role of IC Packing Manufacturer foreseen in this phase.

Life cycle phase 4 “Security Module Product Finishing Process”

40 The SeCMod Product Manufacturer is responsible for the initialization of the TOE, i.e. loading of the initialization data into the TOE, and testing of the TOE.

41 The initialization data is delivered securely to the SeCMod Product Manufacturer.

42 After initialization, successful testing of the Operation System and loading a dedicated file system with security attributes the SeCMod Product Manufacturer will act as the IC Packaging Manufacturer. According to the production processes the IC packing will be performed in this phase, which is allowed by the Protection Profile.

43 The SeCMod product finishing process comprises the embedding of the IC modules of the TOE (manufactured in phase 3 and the first part of this phase 4) in a microcontroller embedded in a HVQFN package.

44 **This finishes the TOE.**

45 The form factor of the TOE is the HVQFN package. The TOE is ready made for the import of User Data.

Life cycle phase 5 “Security Module Integration”

46 The Integrator is responsible for the physical and technical integration of the initialized SeCMod (TOE) 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.

47 The keys and authentication data (the FORMAT APDUs) for opening this phase 5 is delivered securely to the Integrator.

48 The integration process and its single steps follow the procedures desfcribed in the Technical Guidelines [TR03109-2 B].

49 Result of this integration phase is the Smart Meter 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).

Life cycle phase 6 “Security Module End-Usage” (Operational Phase of the Smart Meter Mini-HSM)

50 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.

51 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.

52 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.

53 The security environment for the TOE and the ST of the underlying platform match, the Phases up to 5 are covered by a controlled environment as required in [HWCR, p. 41]. In Phase 6 (Operational Use) no restrictions apply.

54 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.

2 Conformance Claim

2.1 CC Conformance Claims

55 This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation [CC],

Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017,

Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017,

Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

56 as follows:

Part 2 extended,

Part 3 conformant.

57 The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017 ([CC]) has to be taken into account. The evaluation follows the Common Evaluation Methodology (CEM) with current final interpretations.

58 This ST is conformant to Common Criteria Part 2 ([CC]) extended due to the use of SFRs FCS_RNG.1, FMT_LIM.1, FMT_LIM.2, and FPT_EMS.1 defined in the Protection Profile [PP0095-SecMod].

2.2 PP Claims

59 This ST claims strict conformance to the ‘Protection Profile for the Security Module of a Smart Meter Mini-HSM (Mini-HSM Security Module PP)’, Version 1.0 – 23 June 2017 [PP0095-SecMod].

2.3 Package Claims

60 The evaluation of the TOE is a composite evaluation and uses the results of the CC evaluation provided by [HWCR]. The IC hardware platform and its primary embedded software are evaluated at level EAL 6+ (augmented by ASE_TSS.2 and ALC_FLR.1).

61 The evaluation assurance level of the TOE is EAL4 augmented with AVA_VAN.5 as defined in [CC].

2.4 Conformance Rationale

62 The **TOE type** as is a service provider for the Application Server and the miniHSM user for cryptographic functionality in type of a hardware security module with appropriate software installed’.

63 This required TOE type is commensurate with the current TOE type as a smart card chip.

64 All sections of this Security Target regarding the **Security Problem Definition**, **Security Objectives Statement** and **Security Requirements Statement** for the TOE are taken over from the [PP0095-SecMod].

65 The operations done for the SFRs taken from the PP [PP0095-SecMod] are clearly indicated.

66 The **Security Assurance Requirements** statement for the TOE in the current ST includes all the requirements for the TOE of the PP [PP0095-SecMod] as stated in chap. 6.2 below.

3 Security Problem Definition

3.1 Subjects and external entities

67 The Smart Meter Mini-HSM consists of the Mini-HSM with its integrated Security Module (TOE) according to the specification in [TR03109-2 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..

68 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 [TR03109-2 B].

69 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 [TR03109-2 B].

70 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.

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

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

External Entity	Subject	Role	Definition
	in the integration phase: HW/SW tool for the Integrator		
3	Mini-HSM User in the operational phase: e.g. Gateway Administrator, Authorized External Entity (EMT), Gateway Developer 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 1: External Entities and Subjects

72 This table defines external entities and subjects in the sense of [CC]. Subjects can be recognized 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 [CC]). From this point of view, the TOE itself perceives only ‘subjects’ and, for them, does not differ between ‘subjects’ and ‘external entities’.

73 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

74 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.

75 The primary assets to be protected by the TOE as long as they are in scope of the TOE are

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
1	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) • AUTH (support of authentication purpose)	Confidentiality Integrity Authenticity
2	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.	Integrity Authenticity
3	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.	Integrity Authenticity

Table 2: Assets User Data

76 The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are:

Object No.	Asset	Definition	Property to be maintained by the current security policy
4	Ephemeral Keys	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.	Confidentiality Integrity Authenticity
5	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.	Confidentiality Integrity Authenticity
6	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 encryp-	Confidentiality Integrity Authenticity

Object No.	Asset	Definition	Property to be maintained by the current security policy
		tion.	
7	Session Keys	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..	Confidentiality Integrity Authenticity
8	Domain Parameters of Elliptic Curves	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.	Integrity Authenticity
9	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.	Confidentiality Integrity Authenticity

Table 3: Assets TSF Data

3.3 Assumptions

77 According to the threat model in the following assumptions about the environment of the TOE are listed, that need to be taken into account in order to ensure a secure operation of the TOE.

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

A.Name **Short title**

The description of the assumption.

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

79 It is assumed that appropriate technical and/or organizational security measures in the phase of the integration of the Mini-HSM and the TOE in the 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 (cf. [PP0095-SecMod, Table 4 and Table 5]).

80 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.

81 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)**

82 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 (cf. [PP0095-SecMod, Table 4 and Table 5]).

83 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.

84 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**

85 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 [TR03109-2 B] and the requirements in the TOE user guidances into account.

86 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 [TR03109-2 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**

87 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.

88 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.

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

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

90 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.

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

3.4 Threats

92 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.

93 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:

94 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.

95 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.

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

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

98 The threats to the TOE will be defined in the following manner:

T.Name Short title

The description of the threats.

T.ForgeInternalData Forgery of User Data or TSF Data

99 An attacker with high attack potential tries to forge internal User Data or TSF Data via the regular communication interface of the TOE.

100 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

101 An attacker with high attack potential tries to compromise confidential User Data or TSF Data via the regular communication interface of the TOE.

102 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

103 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 authorization.

104 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

105 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.

106 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

107 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.

108 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.

109 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

110 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

111 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.

112 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 initialization 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 initialization functions.

T.Malfunction Malfunction of the TOE

113 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.

114 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 Organizational Security Policies

115 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.

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

P.Name Short title

The description of the organizational security policy.

P.Sign Signature generation and verification

117 The TOE shall generate and verify digital signatures according to [TR03109-3] and [TR03109-2 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

118 The TOE and the Application Server shall implement the DH key agreement (ECKA-DH) according to [TR03109-3], [TR03109-2 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

119 The TOE and the Application Server shall implement the ElGamal key agreement (ECKA-EG) according to [TR03109-3], [TR03109-2 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

120 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 AS itself according to [TR03109-3], [TR03109-2 B].

121 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

122 The TOE and the AS shall implement the PACE protocol according to [TR03110-1], [TR03110-2], [TR03110-3], [TR03109-3], [TR03109-2 B] for component authentication between the AS and the TOE. In the framework of the PACE protocol session keys for securing the data exchange between the AS and the TOE (trusted channel) are negotiated.

4 Security Objectives

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

124 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

The description of the objective.

4.1 Security Objectives for the TOE

125 The following TOE security objectives address the protection provided by the TOE *independently* of the TOE environment as well as the organizational security policies to be met by the TOE independently of the operational environment.

O.Integrity Integrity of User Data and TSF Data

126 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

127 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

128 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

129 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

130 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 AS.

O.TrustedChannel Trusted channel

131 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 AS. The TOE shall enforce the use of a trusted channel if defined by the access condition of an object.

O.Leakage Leakage protection

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

133 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

134 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.

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

O.AbuseFunctionality Protection against abuse of functionality

136 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.

137 *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.

138 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 initialization 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 initialization functions.

O.Malfunction Protection against malfunction of the TOE

139 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

140 The TOE shall securely generate and verify digital signatures according to [TR-03109-3], [TR03109-2 B].

141 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

142 The TOE shall securely implement the DH key agreement (ECKA-DH) according to [TR03109-3], [TR03109-2 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

143 The TOE shall securely implement the ElGamal key agreement (ECKA-EG) according to [TR03109-3], [TR03109-2 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

144 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 [TR03109-3] and [TR03109-2 B].

145 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

146 The TOE shall securely implement the PACE protocol according to [TR03110-1], [TR03110-2], [TR03110-3], [TR03109-3] and [TR03109-2 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

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

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

148 Appropriate technical and/or organizational security measures in the phase of the integration of the Mini-HSM and the TOE in the 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 tables of User and TSF Data in chapter 3.2).

149 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.

150 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)

151 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 tables of User and TSF Data in [PP0095-SecMod, chap. 3.2]).

152 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.

153 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

154 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 [TR03109-2 B] and the requirements in the TOE user guidances into account.

155 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 [TR03109-2 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

156 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.

157 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.

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

OE.TrustedUser Trustworthiness of the Mini-HSM User

159 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.

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

OE.Sign Signature generation and verification

161 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

162 The Application Server shall securely implement the DH key agreement (ECKA-DH) according to [TR03109-2 B],[TR03109-3].

163 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

164 The AS shall securely implement the ElGamal key agreement (ECKA-EG) according to [TR03109-2 B], [TR03109-3].

165 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

166 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

167 The AS shall securely implement the PACE protocol according to [TR03110-1], [TR03110-2], [TR03110-3], [TR03109-2 B], [TR03109-3] 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

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

4.3 Security Objective Rationale

169 The following table is taken over from the Protection Profile [PP0095-SecMod]. It gives an overview how the assumptions, threats and organizational security policies are addressed by the security objectives for the TOE and its environment.

170 The table provides an overview for the security objectives coverage (TOE and its environment), also giving evidence for sufficiency and necessity of the security objectives defined for the TOE and its environment. It shows that all threats are addressed by the security objectives for the TOE and its environment, that all organizational security policies are addressed by the security objectives for the TOE and its environment, and that all assumptions are addressed by the security objectives for the TOE 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	
P.PACE															x

Table 4: Security Objectives Rationale 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											

	OE.Integration	OE.OperationalPhase	OE.Implementation	OE.Protection	OE.TrustedUser	OE.Sign	OE.KeyAgreementDH	OE.KeyAgreementEG	OE.Random	OE.PACE	OE.TrustedChannel
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						

171 Table 5: Security Objectives Rationale for the Operational Environment

172 A detailed justification required for suitability of the security objectives to coup with the security problem definition is given in the chapters 4.3.2 “Countering the Threats”, 4.3.3 “Coverage of Organizational Security Policies” and 4.3.4 “Coverage of Assumptions” in the Protection Profile [PP0095-SecMod] and will be therefore not repeated here.

173 The following Security Objectives for the Hardware Platform are based on [PP0035-ICC]:

O.Leak-Inherent	(Protection against Inherent Information Leakage)
O.Phys-Probing	(Protection against Physical Probing)
O.Malfunction	(Protection against Malfunctions)
O.Phys-Manipulation	(Protection against Physical Manipulation)
O.Leak-Forced	(Protection against Forced Information Leakage)
O.Abuse-Func	(Protection against Abuse of Functionality)
O.RND	(Random Numbers)

174 They are all relevant and do not contradict Security Objectives of the TOE. All they can be mapped to corresponding similar named objectives of the TOE.

175 The remaining objective O.Identification is related to the manufacturing phase. Its support by the TOE is considered in more detail in the Guidance Documentation and is subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1.

176 The detailed analysis of Security Objectives derived from the hardware platform ST [HWST] and the environment of the Hardware Platform is made separately in chapter 7.11 (Statement of Compatibility).

5 Extended Components Definition

177 This protection profile uses components defined as extensions to CC part 2. All these extended components are drawn from Definitions of chapter 5 of [PP0095-SecMod]. The components FCS_RNG, FMT_LIM and FPT_EMS are common in Protection Profiles for smart cards and similar devices.

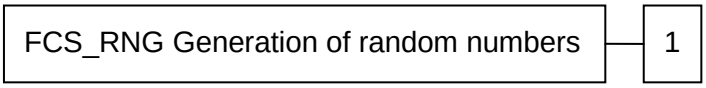
5.1 FCS_RNG Generation of random numbers

The family “Generation of random numbers (FCS_RNG)” is specified as follows.

Family behavior

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

Component leveling:



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

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*].

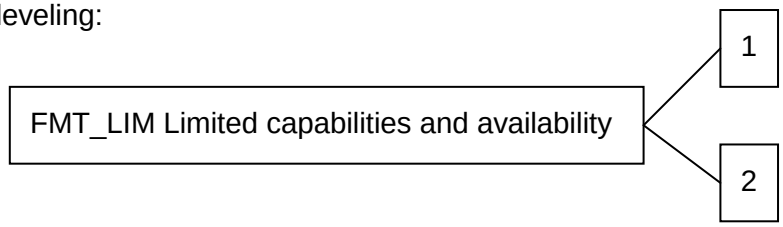
5.2 FMT_LIM Limited capabilities and availability

178 The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

Family behavior:

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 leveling:



FMT_LIM.1 Limited capabilities require 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 restrict 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 lifecycle.

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.

179 **FMT_LIM.1 Limited capabilities**

Hierarchical to: No other components.

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*].

Dependencies: FMT_LIM.2 Limited availability.

180 **FMT_LIM.2 Limited availability**

Hierarchical to: No other components.

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*].

Dependencies: FMT_LIM.1 Limited capabilities.

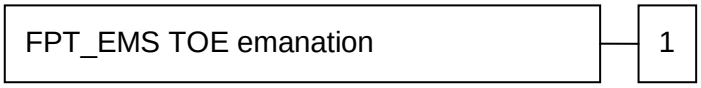
5.3 FPT_EMS TOE Emanation

181 The family “TOE Emanation (FPT_EMS)” is specified as follows.

Family behavior:

This family defines requirements to mitigate intelligible emanations.

Component leveling:



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.

182 **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*].

6 Security Requirements

183 This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of **TOE security requirements** shall define the *functional* and *assurance* security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

184 The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in section 8.1 of Part 1 of the Common Criteria [CC]. Each of these operations is used in this ST.

185 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 are ~~crossed out~~. In some cases an interpretation refinement is given. In such a case an extra paragraph starting with “Refinement” is given. Refinements made by the ST author appear ***slanted, bold and underlined***.

186 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 made by the ST author appear *slanted and underlined*.

187 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 made by the ST author appear *slanted and underlined*.

188 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.

189 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.

6.1 Security Functional Requirements for the TOE

6.1.1 Overview

190 This part defines the detailed security requirements that are satisfied by the TOE. These requirements comprise functional components from CC Part 2 [CC], extended components as defined in Chapter 5, and the assurance components as defined for the Evaluation Assurance Level EAL 4 from CC Part 3 [CC], augmented by AVA_VAN.5.

191 The following table summarizes all TOE security functional requirements of this ST:

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	Specification of Secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.4	Single-use authentication mechanisms
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 6: SFR Overview

6.1.2 Class FCS Cryptographic Support

192 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.

193 The cryptographic algorithms that shall be supported by the Security Module are the same as those that are defined in [TR03109-3] or in [TR03116-3] respectively for the Smart Meter Gateway and its Security Module.

194 [TR03109-3] or [TR03116-3] 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 [TR03109-3] or in [TR03116-3] respectively.**

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

195 The following iterations are caused by different cryptographic key generation algorithms to be implemented and keys to be generated by the TOE.

196 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]: fulfilled by FCS_COP.1/SIG-ECDSA FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_CKM.1.1/ ECC	The TSF shall generate cryptographic **ECC** keys in accordance with a specified cryptographic key generation algorithm *ECKeyPair*[2] and specified cryptographic key sizes *256, 384 and 512 bit length group order*[3] that meet the following: [TR03109-3] or [TR03116-3] respectively, [TR03109-2 B] or [TR03109-2] respectively [4].

197 *Refinement:* The cryptographic key generation algorithm ECKeyPair is defined in the Technical Guideline TR-03111 [TR03111-ECC, 4.1.3].

2 [assignment: *cryptographic key generation algorithm*]

3 [assignment: *cryptographic key sizes*]

4 [assignment: *list of standards*]

198 *Application Note 2*, [TR03109-2 B] or [TR03109-2] 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, for content data encryption and signature as well as in case of the Gateway Administrator for user authentication against the Security Module that is integrated in the Smart Meter Gateway.

199 *Application Note 3:* The TOE supports the following standardized elliptic curve domain parameters (cf. [TR03116-3, 2.2 Table 3]) for the cryptographic SFR FCS_CKM.1 and the SFRs of the family FCS_COP:

Name	Size	Reference
brainpoolP256r1	256	[RFC5639, 3.4]
brainpoolP384r1	384	[RFC5639, 3.6]
brainpoolP512r1	512	[RFC5639, 3.7]
NIST P-256 (secp256r1)	256	[FIPS186, D.1.2.3]
NIST P-384 (secp384r1)	384	[FIPS186, D.1.2.4]

200 **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]: not fulfilled but justified (cf. chapter 6.9.1.4 of the PP [PP0095-SecMod]) FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_CKM.1.1/ ECKA-DH	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECKA-DH ***according to* [TR03111-ECC]**[5] and specified cryptographic key sizes *256, 384 and 512 bit*[6] that meet the following: [TR03109-3] or [TR03116-3] respectively, [TR03109-2 B] or [TR03109-2] respectively[7].

201 *Refinement:* The cryptographic key generation algorithm ECKA-DH is implemented according to [TR03111-ECC, 4.3.2.1]. The cryptographic key sizes specified here are those of shared secret which serve as input for the subsequent key derivation outside the TOE.

202 *Application Note 4:* The TOE generates a shared secret value according to [TR03111-ECC]. This is a refinement to the generic reference given in the PP.

203 *Application Note 5:* [TR03109-2 B] or [TR03109-2] 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.

5 [assignment: *cryptographic key generation algorithm*]

6 [assignment: *cryptographic key sizes*]

7 [assignment: *list of standards*]

204 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]: not fulfilled but justified (cf. chapter 6.9.1.4 of the PP [PP0095-SecMod]) FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_CKM.1.1/ ECKA-EG	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECKA-EG ***according to* [TR03111-ECC]**[8] and specified cryptographic key sizes *256, 384 and 512 bit*[9] that meet the following [TR03109-3] or [TR03116-3] respectively, [TR03109-2 B] or [TR03109-2] respectively[10].

205 *Refinement:* The cryptographic key generation algorithm ECKA-EG is implemented according to [TR03111-ECC, 4.3.2.2]. The cryptographic key sizes specified here are those of shared secret which serve as input for the subsequent key derivation outside the TOE.

206 *Application Note 6:* The TOE generates a shared secret value according to [TR03111-ECC]. This is a refinement to the generic reference given in the PP.

207 *Application Note 7:* [TR03109-2 B] or [TR03109-2] 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.

208 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]: not fulfilled but justified (cf. chapter 6.9.1.4 of the PP [PP0095-SecMod]) FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
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 *128, 192 and 256 bit*[11] that meet the following: [TR03110-1], [TR03110-2], [TR03110-3], [TR03109-3] or [TR03116-3] respectively, [TR03109-2 B] or [TR03109-2] respectively[12].

209 *Application Note 8:* The TOE generates a shared secret value according to PACEv2 defined in [TR03110, part 1-3]. This is a refinement to the generic reference given in the PP.

8 [assignment: *cryptographic key generation algorithm*]

9 [assignment: *cryptographic key sizes*]

10 [assignment: *list of standards*]

11 [assignment: *cryptographic key sizes*]

12 [assignment: *list of standards*]

210 *Application Note 9:* [TR03109-2 B] or [TR03109-2] 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.

211 *Application Note 10:* This SFR implicitly contains the requirements for the hashing functions used for the key derivation by demanding compliance to [TR03110-2], [TR03109-3] or [TR03116-3] respectively, [TR03109-2 B] or [TR03109-2] respectively.

212 **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]: fulfilled by FCS_CKM.1/ECC, FCS_CKM.1/ECKA-DH, FCS_CKM.1/ECKA-EG, FCS_CKM.1/PACE, FDP_ITC.1
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physical deletion by overwriting the memory data with zeros, random numbers or the new key*[13] that meets the following: *none*[14].

213 *Application Note 11:* This SFR applies to the Session Keys, i.e. the TOE destroys the PACE session keys (ENC- and MAC-keys) after detection of an MAC error in a received command. The TOE clears the memory area of any session keys before starting the communication with the Application Server and Mini-HSM user in a new after-reset-session as required by FDP_RIP.1. This SFR applies also to signature or decryption keys. The TOE will overwrite the assigned key-memory-data with the new key.

214 *Application Note 12:* The TOE provides the command DELETE KEY which overwrites explicitly the memory area of a key with zeros.

215 *Application Note 13:* The TOE provides shared secret negotiation (Z_{AB}) in FCS_CKM.1/ECKA-DH and FCS_CKM.1/ECKA-EG. The TOE will overwrite the negotiated secret value Z_{AB} with the new Z_{AB} value. After de-allocation of the resource the memory data of the shared secret Z_{AB} is overwritten by zero bytes.

6.1.2.2 Cryptographic operation (FCS_COP.1)

216 The following iterations are caused by different cryptographic algorithms to be implemented by the TOE.

217 **FCS_COP.1/SIG-ECDSA Cryptographic operation – ECDSA Signature generation**

Hierarchical to:	No other components.

13 [assignment: *cryptographic key destruction method*]

14 [assignment: *list of standards*]

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/ECC. FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
FCS_COP.1.1/ SIG-ECDSA	The TSF shall perform signature generation for the commands PSO COMPUTE DIGITAL SIGNATURE and INTERNAL AUTHENTICATE[15] in accordance with a specified cryptographic algorithm ECDSA ***according to* [TR03111-ECC]**[16] and cryptographic key sizes *256, 384 and 512 bit*[17] that meet the following: [TR03109-3] or [TR03116-3] respectively, [TR03109-2 B] or [TR03109-2] respectively[18].

218 *Refinement:* The signature algorithm ECDSA is defined in [TR03111-ECC] in clause 4.2.1. This Technical Guideline is the reference for ECDSA given in [TR03109-3] respective [TR03116-3]. Note that the TOE supports secure standardized domain parameters listed in Application Note 3 as required by [TR03116-3, clause 2.2].

219 *Application Note 14:* The algorithm ECDSA is conformant with the algorithm EC-DSA defined in the ISO/IEC Standard [ISO14888-3].

220 FCS_COP.1/VER-ECDSA Cryptographic operation – 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]: fulfilled by FCS_CKM.1/ECC FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
FCS_COP.1.1/ VER-ECDSA	The TSF shall perform PSO VERIFY DIGITAL SIGNATURE[19] in accordance with a specified cryptographic algorithm ECDSA ***according to* [TR03111-ECC]**[20] and cryptographic key sizes *256, 384 and 512 bit length group order* [21] that meet the following: [TR03109-3] or [TR03116-3] respectively, [TR03109-2 B] or [TR03109-2] respectively [22].

221 *Refinement:* The signature algorithm ECDSA is defined in [TR03111-ECC] in clause 4.2.1. The TOE verifies ECDSA signatures according to [TR03111-ECC, 4.2.1.2]. This Technical Guideline is the reference for ECDSA given in [TR03109-3] and [TR03116-3]. Note that the TOE supports secure standardized domain parameters listed in Application Note 3 as required by [TR03116-3, clause 2.2].

15 [assignment: *list of cryptographic operations*]

16 [assignment: *cryptographic algorithm*]

17 [assignment: *cryptographic key sizes*]

18 [assignment: *list of standards*]

19 [assignment: *list of cryptographic operations*]

20 [assignment: *cryptographic algorithm*]

21 [assignment: *cryptographic key sizes*]

22 [assignment: *list of standards*]

222 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]: fulfilled by FDP_ITC.1 FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_COP.1.1/ IMP	The TSF shall perform signature verification for import of public keys for the command PSO VERIFY CERTIFICATE[23] in accordance with a specified cryptographic algorithm ECDSA[24] and cryptographic key sizes *256, 384, 512 bit*[25] that meet the following: [TR03109-3] or [TR03116-3] respectively, [TR03109-2 B] or [TR03109-2] respectively [26].

223 *Refinement:* The signature verification algorithm ECDSA implemented in the command PSO VERIFY CERTIFICATE is defined in [TR03111-ECC] in clause 4.2.1. This Technical Guideline is the reference for ECDSA given in [TR03116-3]. Note that the TOE supports secure standardized domain parameters listed in Application Note 3 as required by [TR03116-3, clause 2.2].

224 FCS_COP.1/PACE-ENC Cryptographic operation – AES in CBC 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]: fulfilled by FCS_CKM.1/PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
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 *128, 192 and 256 bit*[27] that meet the following: [TR03109-3] or [TR03116-3] respectively, [TR03109-2 B] or [TR03109-2] respectively [28].

225 *Refinement:* The cryptographic algorithm AES is defined in [FIPS197], the corresponding mode of operation CBC is defined in the NIST Special Publication [SP800-38A]. These are the references given in [TR03116-3, clause 2.1].

226 *Application Note 15:* 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

23 [assignment: *list of cryptographic operations*]

24 [assignment: *cryptographic algorithm*]

25 [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256]

26 [assignment: *list of standards*]

27 [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256]

28 [assignment: *list of standards*]

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.

227 **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]; fulfilled by FCS_CKM.1/PACE, FCS_CKM.4 Cryptographic key destruction:]; fulfilled by FCS_CKM.4.
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 *128, 192 and 256 bit*[29] that meet the following [TR03109-3] or [TR03116-3] respectively, [TR03109-2 B] or [TR03109-2] respectively [30].

228 *Refinement:* The cryptographic algorithm AES is defined in [FIPS197], the corresponding mode of operation CMAC is defined in the NIST Special Publication [SP800-38B]. These are the references given in [TR03116-3, clause 2.1].

229 *Application Note 16*: 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 AS as part of the PACE protocol according to the FCS_CKM.1/PACE.

6.1.2.3 Random Number Generation (FCS_RNG.1)

230 **FCS_RNG.1 Quality metric for random numbers**

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

29 [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256] bit

30 [assignment: *list of standards*]

FCS_RNG.1.1 The TSF shall provide a *hybrid deterministic*[31] random number generator that implements *DRG.4 capabilities according to* [AIS20/31][32]:

(DRG.4.1) The internal state of the RNG shall *use PTRNG of class PTG.2 as random source*[33].

(DRG.4.2) The RNG provides forward secrecy.

(DRG.4.3) The RNG provides backward secrecy even if the current internal state is known.

(DRG.4.4) The RNG provides enhanced forward secrecy *on condition "session closed or aborted"*[34].

(DRG.4.5) The internal state of the RNG is seeded by *a PTRNG of class PTG.2*[35].

FCS_RNG.1.2 The TSF shall provide random numbers that meet[36]

(DRG.4.6) The RNG generates output for which $k > 2^{34}$ [37] strings of bit length 128 are mutually different with probability $1-\varepsilon$, with $\varepsilon < 2^{-16}$ [38].

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A, *the NIST and the dieharder*[39] *tests*[40].

231 *Application Note 17:* Random numbers are generated for the AS 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.

232 In particular, [TR03109-2 B] or [TR03109-2] 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 AS). TOE's RNG is a hybrid generator, which implies a regular refresh to guarantee a sufficient entropy of the generated numbers.

---

31 [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]

32 [assignment: *list of security capabilities*]

33 [selection: *use PTRNG of class PTG.2 as random source*, *have* [assignment: *work factor*], *require* [assignment: *guess work*]

34 [selection: *on demand, on condition* [assignment: *condition*], *after* [assignment: *time*]]

35 [selection: *internal entropy source, PTRNG of class PTG.2, PTRNG of class PTG.3,* [other selection]]

36 [assignment: *a defined quality metric*]

37 [assignment: *number of strings*]

38 [assignment: *probability*]

39 The selected test suites http://csrc.nist.gov/groups/ST/toolkit/rng/documents/sts-2.1.1.zip and http://www.phy.duke.edu/~rgb/General/dieharder/dieharder-3.31.0.tgz are available at NIST and Dieharder web sites. Note that the dieharder tests include Marsaglia's "Diehard battery of tests" and NIST tests.

40 [assignment: *additional test suites*]

6.1.3 Class FDP User Data Protection

233 Access Control Smart Meter Mini-HSM SFP

234 The Access Control Smart Meter Mini-HSM SFP for the SeCMod (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 [TR03109-2 B]. The SFP takes the following subjects, objects, security attributes and operations into account:

235 Subjects:
- external world
- AS
- Mini-HSM User

236 Security attributes for subjects:
- “authenticated via PACE protocol”

237 Objects:
- key pair
- public key
- certificate

as presented in Table 2.

238 Security attributes for objects:
- “access rule” (see below)

239 Operations:
- TOE commands as specified in [TR03109-2 B] or [TR03109-2] respectively

240 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.

241 For the Access Control Smart Meter Mini-HSM SFP, the access rules are defined as prescribed in [TR03109-2 B]. Please notice that in [TR03109-2 B] two different options for such Access Control Smart Meter Mini-HSM SFP are specified. This TOE implements only option 2 .

242 **FDP_ACC.2 Complete access control – Access Control Policy**

Hierarchical to:	FDP_ACC.1 Subset Access control
Dependencies:	FDP_ACF.1 Security attribute based access control: fulfilled by FDF_ACF.1
FDP_ACC.2.1	The TSF shall enforce the Access Control Smart Meter Mini-HSM SFP[41] on[42]: 1. Subjects: a. external world b. AS

41 [assignment: *access control SFP*]

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

c. Mini-HSM User
d. *none*[43],

2. Objects:
a. key pair, public key, certificates as presented in Table 2
b. *none*[44]

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.

243 FDP_ACF.1 Security attribute based access control – Access Control Functions

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.2
FMT_MSA.3 Static attribute initialization: not fulfilled, but justified.

FDP_ACF.1.1 The TSF shall enforce the Access Control Smart Meter Mini-HSM SFP[45] to objects based on the following[46]:

1. Subjects:
a. external world
b. AS with security attribute “authenticated via PACE protocol”
c. Mini-HSM User with security attribute “authenticated via PACE protocol”
d. *none*[47],

2. Objects:
a. key pair, public key, certificates as presented in Table 2 each with security attribute “access rule”
b. *none*[48].

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)[49].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[50].

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 pri-

43 [assignment: *list of further subjects, or none*]

44 [assignment: *list of further objects, or none*]

45 [assignment: *access control SFP*]

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

47 [assignment: *list of further subjects, or none*]

48 [assignment: *list of further objects, or none*]

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

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

vate keys from the TOE[51].

244 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[52] on all objects, based on the following attributes: *integrity checked stored data*[53].
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, *enter the hardware security reset state*[54].

245 *Application Note 18*: Stored data in memory may be flagged by the TOE with the integrity check attribute. Any data with this attribute is always checked for integrity errors as soon as it is accessed by the TOE. This data includes the secret and public key objects as well as the HSM-System-PIN.

246 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 *de-allocation of the resource from*[55] the following objects[56]: 1. PIN, 2. session keys (immediately after closing related communication session), 3. private cryptographic keys, 4. shared secret value Z_{AB}, 5. ephemeral keys, 6. *none*[57].

247 *Application Note 19*: Upon de-allocation old key objects will be overwritten with the new key or zeros according to FCS_CKM.4.

248 FDP_ETC.1 Export from the TOE

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC Subset information flow control] fulfilled by FP_ACC.2

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

52 [assignment: *integrity errors*]

53 [assignment: *user data attributes*]

54 [assignment: *other action to be taken, or none*]

55 [selection: *allocation of the resource to, de-allocation of the resource from*]

56 [assignment: *list of objects*]

57 [assignment: *other data objects or none*]

FDP_ETC.1.1	The TSF shall enforce the Access Control Smart Meter Mini-HSM SFP[58] 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.

249 FDP_ITC.1 Import from outside of the TOE

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.2 FMT_MSA.3 Static attribute initialization not fulfilled but justified
FDP_ITC.1.1	The TSF shall enforce the Access Control Smart Meter Mini-HSMSFP[59] when importing user data, controlled under the SFP, 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[60].

250 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] fulfilled by FTP_ITC.1 [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.2
FDP_UCT.1.1	The TSF shall enforce the Access Control Smart Meter Mini-HSM SFP[61] to transmit, receive[62] user data in a manner protected from unauthorized disclosure.

251 FDP_UIT.1 Inter-TSF user data integrity transfer protection

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1 [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.2
FDP_UIT.1.1	The TSF shall enforce the Access Control Smart Meter Mini-HSM SFP[63] to transmit, receive[64] user data in a manner protected from modification, deletion, insertion, replay[65] errors.

58 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

59 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

60 [assignment: *additional importation control rules*]

61 [selection: *transmit, receive*]

62 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, replay[66] has occurred.

6.1.4 Class FIA Identification and Authentication

252 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[67]:

1. for device (AS): authentication state gained via PIN (PACE-PIN or HSM-System-PIN respectively used within the PACE protocol),
2. for human user (Mini-HSM User): authentication state gained via PIN (PACE-PIN or HSM-System-PIN respectively used within the PACE protocol).

253 *Application Note 20:* Mutual authentication between the AS or the Mini-HSM User repsectively is performed via the PACE protocol between the AS and the TOE, refer to the SFR FCS_CKM.1/PACE.

254 FIA_SOS.1 Specification 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 AS for the PACE-PIN or HSM-System-PIN respectively** meet *a minimal length of 10 octets*[68].

255 *Application Note 21:* Mutual authentication between the AS or Mini-HSM User respectively is performed via the PACE protocol between the AS and the TOE, refer to the SFR FCS_CKM.1/PACE.

256 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1.

FIA_UAU.1.1 The TSF shall allow[69]:

1. establishing a communication channel between the TOE and the external world,

---

63 [selection: *transmit, receive*]

64 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

65 [selection: *modification, deletion, insertion, replay*]

66 [selection: *modification, deletion, insertion, replay*]

67 [assignment: *authentication mechanism*]

68 [assignment: *a defined quality metric*]

69 [assignment: *list of TSF-mediated actions*]

2. Reading the ATR/ATS,
3. Reading of data fields containing technical information,
4. 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 control rules defined in [TR03109-2 B],
5. *none*[70]

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.

257 *Application Note 22:* Authentication of the AS or Mini-HSM User is performed via the PACE protocol between the AS and the TOE, refer to the SFR FCS_CKM.1/PACE.

258 *Application Note 23:* 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 6.1.3) 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.

259 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
1. PACE authentication mechanism.

260 FIA_UAU.5 Multiple authentication mechanisms

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

FIA_UAU.5.1 The TSF shall provide
1. authentication via the PACE protocol,
2. 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[71]:
1. PACE/PIN based authentication shall be used for authenticating a device (AS) 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

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

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

the Access Control Smart Meter Mini-HSM SFP.

261 FIA_UID.1 Timing of identification

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

FIA_UID.1.1 The TSF shall allow[72]:
1. Establishing a communication channel between the TOE and the external world,
2. Reading the ATR/ATS,
3. Reading of data fields containing technical information,
4. Carrying out the PACE protocol according to [TR03110-1], [TR03110-2], [TR03110-3], [TR03109-3] or [TR03116-3] respectively, [TR03109-2 B] or [TR03109-2] respectively (by means of command General Authenticate),
5. 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.

262 FIA_USB.1 User-subject binding

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

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user[73]:
1. authentication state for the AS 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”[74].

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[75]:
1. for device (AS): the authentication state is changed to “authenticated AS” when the device has successfully authenticated itself by the PACE protocol,
2. 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.

72 [assignment: *list of additional TSF-mediated actions*]

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

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

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

6.1.5 Class FMT Security Management

263 FMT_LIM.1 Limited capabilities

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability: fulfilled by FMT_LIM.2.
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[76].

264 FMT_LIM.2 Limited availability

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities: fulfilled by FMT_LIM.1.
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[77].

265 *Application Note 24:* 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.

266 The combination of both requirements shall enforce the policy.

267 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies

76 [assignment: *Limited capability and availability policy*]

77 [assignment: *Limited capability and availability policy*]

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. Management of key objects by means of commands CREATE KEY, DELETE KEY, ACTIVATE KEY, DEACTIVATE KEY, GENERATE ASYMMETRIC KEY PAIR, PSO VERIFY CERTIFICATE,
2. 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
3. Management of PIN objects by means of command CHANGE REFERENCE DATA,
4. Life cycle management of the TOE by means of command TERMINATE CARD USAGE,
5. Update of keys by means of commands GENERATE ASYMMETRIC KEY PAIR, PSO VERIFY CERTIFICATE,
6. Update of data by means of command UPDATE BINARY, UPDATE RECORD,
7. *none* [78].

268 *Application Note 25*: A detailed description of the commands that have to be implemented in the TOE is given in [TR03109-2 B] or [TR03109-2] respectively.

269 **FMT_SMR.1 Security roles**

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification: fulfilled

FMT_SMR.1.1 The TSF shall maintain the roles

1. user,
2. authenticated AS
3. authenticated Mini-HSM User
4. *none* [79].

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

6.1.6 Class FPT Protection of the Security Functions

270 **FPT_EMS.1 TOE Emanation**

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

FPT_EMS.1.1 The TOE shall not emit *power variations, timing variations during command execution* [80] in excess of *non-useful information* [81] enabling access to

1. PIN,
2. session keys,
3. shared secret value Z_{AB},
4. ephemeral keys[82]

78 [assignment: *list of further management functions to be provided by the TSF, or none*]

79 [assignment: *additional authorized identified roles, or none*]

80 [assignment: *types of emissions*]

81 [assignment: *specified limits*]

5. *none*[83]

and

6. private asymmetric keys of the user,
7. *none*[84]

FPT_EMS.1.2 The TSF shall ensure any users[85] are unable to use the following interface circuit interface[86] to gain access to

1. PIN,
2. session keys,
3. shared secret value Z_{AB},
4. ephemeral keys[87]
5. *none*[88]

and

6. private asymmetric keys of the user,
7. *none*[89]

271 *Application Note 26*: The TOE prevents 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.

272 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:

1. power loss,
2. exposure to operating conditions where therefore a malfunction could occur,
3. detection of physical manipulation or physical probing,
4. integrity errors according to FDP_SDI.2,
5. insufficient entropy during random number generation,
6. failure detected by the TSF according to FPT_TST.1,
7. errors during processing cryptographic operations,
8. errors during evaluation of access control rules, and
9. *none* [90].

82 [assignment: *list of types of TSF data*]

83 [assignment: *list of types of (further) TSF data*]

84 [assignment: *list of types of (further) user data*]

85 [assignment: *type of users*]

86 [assignment: *type of connection*]

87 [assignment: *list of types of TSF data*]

88 [assignment: *list of types of (further) TSF data*]

89 [assignment: *list of types of (further) user data*]

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

273 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[91] to the TSF[92] by responding automatically such that the SFRs are always enforced.

274 *Application Note 27*: The TOE implements 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.

275 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[93] to demonstrate the correct operation of the TSF[94].
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data[95].
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of TSF[96].

6.1.7 Class FTP Trusted Path/Channels

276 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[97] to initiate communication via the trusted channel.

91 [assignment: *physical tampering scenarios*]

92 [assignment: *list of TSF devices/elements*]

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

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

95 [selection: [assignment: *parts of TSF*], *TSF data*]

96 [selection: [assignment: *parts of TSF*], *TSF*]

FTP_ITC.1.3 The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the AS according to the Access Control Smart Meter Mini-HSM SFP with its access control rules defined in [TR-03109-2 B] [98].

6.2 Security Assurance Requirements for the TOE

277 The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL4 augmented by the following component:

- AVA_VAN.5 (Advanced methodical vulnerability analysis).

278 The Protection Profile [PP0095-SecMod] provides an overview on the assurance requirements for the evaluation of the TOE. Note that the component AVA_VAN.5 has a refinement, which is applied to the evaluation of the TOE.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

279 The following table provides an overview for security functional requirements coverage.

	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											

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

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

	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
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											
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 7: Coverage of Security Objectives for the TOE by SFR

280 A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given in the Protection Profile [PP0095-SecMod] and therefore not repeated here.

6.3.2 Rationale for SFR's Dependencies

281 The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.

282 The table below shows the dependencies between the SFR of the TOE.

No.	SFR-component from the PP	Dependencies assumed	Fulfilled by SFR

No.	SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
1	FCS_CKM.1/ECC	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/SIG-ECDSA FCS_CKM.4 Please refer to [PP0095-SecMod, chapter 6.9.1.4] for missing dependencies
2	FCS_CKM.1/ECKA-DH	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.4 Please refer to [PP0095-SecMod, chapter 6.9.1.4] for missing dependencies
3	FCS_CKM.1/ECKA-EG	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.4 Please refer to [PP0095-SecMod, chapter 6.9.1.4] for missing dependencies
4	FCS_CKM.1/PACE	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/PACE_ENC FCS_COP.1/PACE_MAC FCS_CKM.4
5	FCS_CKM.4	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/ECC FCS_CKM.1/ECKA-DH FCS_CKM.1/ECKA-EG FCS_CKM.1/PACE FDP_ITC.1
6	FCS_COP.1/SIG-ECDSA	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/ECC FCS_CKM.4
7	FCS_COP.1/VER-ECDSA	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 FCS_CKM.4
8	FCS_COP.1/IMP	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 FCS_CKM.4
9	FCS_COP.1/PACE-ENC	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/PACE FCS_CKM.4
10	FCS_COP.1/PACE-MAC	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/PACE FCS_CKM.4
11	FCS_RNG.1	–	–
12	FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
13	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 Please refer to [PP0095-SecMod, chapter 6.9.1.4] for missing dependencies
14	FDP_SDI.2	–	–
15	FDP_RIP.1	–	–
16	FDP_ETC.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2
17	FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.2 Please refer to [PP0095-SecMod, chapter 6.9.1.4] for missing dependencies
18	FDP_UCT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ICT.1 or FTP_TRP.1]	FDP_ACC.2 FTP_ICT.1
19	FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ICT.1 or FTP_TRP.1]	FDP_ACC.2 FTP_ICT.1
20	FIA_ATD.1	–	–
21	FIA_UAU.1	FIA_UID.1	FIA_UID.1
22	FIA_UAU.4	–	–
23	FIA_UAU.5	–	–
24	FIA_UID.1	–	–
25	FIA_USB.1	FIA_ATD.1	FIA_ATD.1
26	FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
27	FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
28	FMT_SMF.1	–	–

No.	SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
29	FMT_SMR.1	FIA_UID.1	FIA_UID.1
30	FPT_EMS.1	–	–
31	FPT_FLS.1	–	–
32	FPT_PHP.3	–	–
33	FPT_TST.1	–	–
34	FTP_ITC.1	–	–

Table 8: Dependencies between the SFRs

283 For the justification of non-satisfied dependencies see the detailed description in the Protection Profile [PP0095-SecMod, chapter 6.9.1.4] for missing dependencies of the corresponding SFRs.

284 The dependency analysis shows that all dependencies being expected by CC part 2 and by extended components definition (chapter 5) are either fulfilled or their non-fulfillment is justified.

285

6.3.3 Security Assurance Requirements Rationale

Reasoning for Choice of Assurance Level

286 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).

287 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.

Dependencies of Assurance Components

288 The dependencies of the assurance requirements taken from EAL 4 are fulfilled automatically.

289 The augmentation by AVA_VAN.5 does not introduce additional functionalities that are not contained in EAL 4.

Security Requirements – Internal Consistency

290 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.

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

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

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

294 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 the Protection Profile [PP0095-SecMod]. Furthermore, as also discussed in the PP, 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 TOE Summary Specification

295 This section presents an overview of the security functionalities implemented by the TOE and the assurance measures applied to ensure their correct implementation.

296 According to the SFRs the TOE provides the following security functionalities

- 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
- Secure Storage of Key Material and further 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.

297 They are already mentioned in section 6.1.1 and represent the functional description of the feature overview in section 1.4.2. The TOE Summary Specification will be given in more detail in the following sections. Further technical information how the security functions actually implement the TOE security functional requirements, which TOE modules realize which functions is contained in the Security architecture Description (ADV_ARC), the Functional Specification (ADV_FSP) and the TOE Design Specification (ADV_TDS).

7.1 Digital Signature Generation

298 The Security Module serves as a cryptographic service provider for the AS Application Server or the Mini-HSM User respectively. It generates digital signatures based on elliptic curve cryptography according to the ECDSA specification in [TR03111-ECC] (FCS_RNG.1, FCS_COP.1/SIG-ECDSA). The TOE uses the strong brainpool curves [RFC5639] with 256, 384 and 512 bits and the NIST curves P-256 and P-384 [FIPS186] with corresponding key lengths.

299 Digital signatures are used in the framework of TLS as well as for content authentication. The Security Module contains the “cryptographic identity” of the AS and generates AS’s signatures (FCS_COP.1/SIG-ECDSA). There is no security gap between different types of digital signatures generated by the Security Module.

300 Furthermore digital signatures are used to sign certificates int the context of the internal Authenticate command and for generation of authentication tokens.

301 In case keys must be destroyed the Security Module deletes the relevant information by overwriting the memory data with zeros or random data of the new key (FCS_CKM.4). Ephemeral keys are made unavailable upon the de-allocation (FDP_RIP.1).

7.2 Digital Signature Verification

302 The Security Module provides signature verification service to the Application Server or the Mini-HSM User respectively for different purposes. It verifies digital signatures based

on elliptic curve cryptography according to the ECDSA specification in [TR03111-ECC] (FCS_RNG.1, FCS_COP.1/SIG-ECDSA). The TOE uses the strong brainpool curves [RFC5639] with 256, 384 and 512 bits and the NIST curves P-256 and P-384 [FIPS186] with corresponding key lengths.

303 This is important for the import of public keys through certificates into the Security Module. Successful digital signature verification of certificates transfers the trust to certificate data, the public key of an external entity. This is supported by FCS_COP.1/IMP.

304 Reliable signature verification provided to the AS allows to check the authenticity and integrity of transmitted data in the TLS framework and the data transfer inside the TLS channel (FCS_COP.1/VER-ECDSA).

305 The reliability of signature verification result is supported by the trusted channel provided by the PACE protocol (FCS_CKM.1/PACE, FCS_COP.1/PACE-MAC, FDP_UIT.1).

7.3 Key Agreement for TLS

306 During the TLS handshake a shared secret is derived. It is generated by the ECKA-DH protocol which is supported by the SFR FCS_CKM.1/ECKA-DH. The corresponding session keys are generated from the shared secret by the AS. The established by PACE protocol (FCS_COP.1/PACE-ENC, FCS_COP.1/PACE-MAC) trusted channel guarantees the confidentiality and the authenticity of the shared secret.

307 The Security Module uses elliptic curve cryptography according to [TR03111-ECC] based the strong brainpool curves [RFC5639] with 256, 384 and 512 bits and the NIST curves P-256 and P-384 [FIPS186] with corresponding key lengths.

7.4 Key Agreement for Content Data Encryption

308 Asymmetric content data encryption uses an ephemeral shared value, from which the symmetric algorithm key is derived. It is generated by the ECKA-EG protocol. The key derivation is performed by the AS. The confidentiality and the authenticity of the shared ephemeral value is guaranteed by the trusted channel provided by the PACE protocol (FCS_COP.1/PACE-ENC, FCS_COP.1/PACE-MAC).

309 The Security Module uses elliptic curve cryptography according to [TR03111-ECC] based the strong brainpool curves [RFC5639] with 256, 384 and 512 bits and the NIST curves P-256 and P-384 [FIPS186] with corresponding key lengths.

7.5 Key Pair Generation

310 Asymmetric key pairs based on elliptic curve cryptography keys can be generated by the Security Module (FCS_CKM.1/ECC, FCS_RNG.1) for different purposes. These keys can be used for signature generation and verification (FCS_COP.1/SIG-ECDSA, FCS_\ COP.1/VER-ECDSA), Diffie-Hellman (FCS_CKM.1/ECKA-DH) and ElGamal (FCS_\ CKM.1/ECKA-EG) key agreement. The quality of random numbers guarantees (see next chapter 7.6 Random Number Generation) the security level of the keys and therefore the security of the signatures and the derived keys for symmetric encryption or MAC.

311 The Security Module uses elliptic curve cryptography according to [TR03111-ECC] based the strong brainpool curves [RFC5639] with 256, 384 and 512 bits and the NIST curves P-256 and P-384 [FIPS186] with corresponding key lengths.

7.6 Random Number Generation

312 Random numbers are used by the Security Module internally and are also provided to the Application Server or the Mini-HSM User respectively. The Random Number Generator implemented in the TOE is a hybrid deterministic of level DRG.4 according to [AIS20/31], supporting enhanced backward and forward secrecy.

313 For the internal ephemeral and static key generation the TOE refreshes the internal Random Number Generator accordingly.

7.7 Component Authentication via the PACE-Protocol with Negotiation of Session Keys

314 The PACE protocol provides component and user authentication. Even if the authentication data has small entropy the negotiated session keys carry high entropy (FCS_CKM.1/PACE, FDP_UCT.1, FDP_UIT.1, FIA_ATD.1). The usage of these session keys in the context of the trusted channel provides re-authentication, confidentiality and integrity (FIA_UAU.5, FIA_UID.1, FIA_USB.1). Only components knowing the authentication data are able to establish the trusted channel and gain access to other TSF-mediated actions (FIA_UAU.1). The Authentication data (the derived Mini-HSM PIN) will be protected by the TOE. The PACE protocol requires fresh data for a new authentication (FIA_UAU.4).

315 The TSF requires a minimal length of 10 octets (usually decimal digits) for the HSM-System-PIN. This provides enough space for passwords with high entropy (FIA_SOS.1).

7.8 Secure Messaging

316 The TOE provides a trusted channel protected against disclosure, deletion, modification or insertion, and the re-usage of old communication data. Secure Messaging is implemented according to [ISO7816] based on the strong symmetric cipher AES (FCS_COP.1/PACE-ENC) and CMAC authentication method (FCS_COP.1/PACE-MAC).

317 The TOE enforces the usage of the trusted communication except reading of public technical information (FTP_ITC.1).

7.9 Secure Storage of Key Material and further data relevant for the AS or the Mini-HSM User respectively

318 The access to User Data is restricted according to the SFRs FDP_ACC.2 and FDP_ACF.1. The access control provided by this security function includes also the integrity check required by FDP_SDI.2. The TOE software is implemented such that test features after TOE delivery cannot be deployed for data access (disclosure and modification of user and TOE data) and other information about the embedded software (TSF implementation (FMT_LIM.1, FMT_LIM.2).

319 The access to key material and management of user data is restricted to the conformant to [ISO7816] command set (FMT_SMF.1), which can be executed only after authentication (FDP_ACC.2) by the defined roles (FMT_SMR.1) using the PACE (FIA_ATD.1).

320 The TOE enforces the Access Control Smart Meter Mini-HSM SFP (FDP_ACC.2) on export and import of user data (FDP_ETC.1, FDP_ITC.1).

321 The TOE provides a high level of resistance to physical attack (FPT_PHP.3) and prevents emitting of usable information on key material and user data over side-channels like power or timing variations (FPT_EMS.1).

322 In case of power loss, detection of physical manipulation, integrity check failures or TSF functional errors the TOE enters and preserves a secure state (FPT_FLS.1). During initial start-up and continuously during normal operation self tests are run to guarantee the claimed security level and to demonstrate the correctness of the TSF output (FPT_TST.1).

7.10 TOE SFR Statements

323 For the sake of completeness the TOE Summary Specification of the previous sections is re-ordered once again. All the TOE SFR statements are listed and it is described how they are fulfilled by the TOE. If appropriate requirements are handled together to avoid non-necessary text duplication.

324 FCS_CKM.1/ECC: The key pair generation algorithm is compliant to the Technical Specification [TR03111-ECC]. The available parameters can be chosen such that they are suitable for the near and the long future. The standardized prime curves of 256, 384 and 512 bit key lengths are supported by the TOE. The private key is generatated using the strong Random Number Generator implemented by the TOE.

325 FCS_CKM.1/ECKA-DH, FCS_CKM.1/ECKA-EG: The TOE implements operations on points of elliptic curves with prime characteristic. Addition and doubling of points is the base for Diffie-Hellman key agreement and the ElGamal operation. The TOE uses the strong brainpool curves [RFC5639] with 256, 384 and 512 bits and the NIST curves P-256 and P-384 [FIPS186] with corresponding key lengths. The COS ensures the correctness of the generated shared secret Z_{AB} using different checks during the computation.

326 FCS_CKM.1/PACE: The PACE (Password Authenticated Connection Establishment) protocol is based on asymmetric cryptography and provides session keys which strength is independent of the entropy of the input. It is proven to be secure, provides a secure communication channel based on explicit password-based authentication. Ephemeral keys are generated using the strong Random Number Generator implemented by he TOE.

327 FCS_CKM.4: Each session key is used only by the authenticated user and is destroyed if the authentication fails or is restarted again. Additionally in case of loss of power the keys are also erased, because they are not stored permanently.

328 FCS_COP.1/SIG-ECDSA, FCS_COP.1/VER-ECDSA: The TOE implements the standard signature algorithm EC-DSA for the strong elliptic curves mentioned in paragraph 325. The signature creation function uses strong keys provided by the internal Random Number Generator. The COS ensures the correctness of the operation using different checks during the computation.

329 FCS_COP.1/IMP: The signature verification is the base for a certificate based PKI. The TOE will import public keys by verification of certificates. Only keys with the domain parameters of implemented curves (cf. paragraph 330) can be imported.

330 FCS_COP.1/PACE-ENC, FCS_COP.1/PACE-MAC: The secure channel established in the PACE protocol uses Secure Messaging conformant to ISO7816 in encrypt-then-authenticate mode. The cryptographic operation is based on the strong cipher AES with key lengths of 128, 192 and 256 bits, and the CMAC authentication mode. The COS ensures the correctness of the operation using different checks during the computation.

331 FCS_RNG.1: The randomness of values for challenges or ephemeral or permanent keys bases on the underlying hardware TSF. Its Random Number Generator claims the functionality class PTG.2 according to [AIS20/31]. This includes also the fulfillment of the online test requirements. For generating random nonces in the PACE protocol a cryptographic post-processing in the TOE guarantees that statistical tests practically cannot distinguish between generated values and an ideal random number generator. The random number generator provided by the TOE fulfills the requirements of a DRG.4 according to [AIS20/31].

332 FDP_ACC.2, FDP_ACF.1: These SFRs define the **Access Control Smart Meter Mini-HSM SFP**. It provides complete access control of the subjects External World, AS, Mini-HSM User to key pairs, public keys and certificates. Enforcing these access rules defined in the Protection Profile is essential for the security functionality of the TOE. The access rule enforcement is implemented in the COS and cannot be changed.

333 FDP_ETC.1, FDP_ITC.1: The TOE enforces the **Access Control Smart Meter Mini-HSM SFP** when exporting or importing user data. Note that this implies a protection against unauthorized disclosure, insertion, modification and replay of the data (cf. FDP_UCT.1, FDP_\ UIT.1). The access rule enforcement is implemented in the COS and cannot be changed.

334 FDP_SDI.2: The TOE controls user and TOE data for integrity errors, if an error occurs the corresponding data is no more accessible and a warning will be issued on any access. The data attribute “integrity checked” is defined in the operating system and cannot be changed.

335 FDP_RIP.1: This SFR protects sensitive user and TOE data after de-allocation. Ephemeral key material is overwritten by zero bytes after finishing the cryptographic operation and de-allocation of the resources or after closing the session. Persistently stored objects are deleted with a roll-forward procedure, i.e. the TOE will finish first the de-allocation and overwriting with zero bytes before any other operation is allowed.

336 FDP_UCT.1, FDP_UIT.1: The TOE enforces the protection of transmitted user data according to the **Access Control Smart Meter Mini-HSM SFP** against unauthorized disclosure and modification, deletion, insertion and replay. This is supported by the Secure Messaging according to ISO7816 and cannot be avoided.

337 FIA_ATD.1, FIA_SOS.1: This SFR defines the data to be used for authentication and the data needed for storing the authentication state gained via HSM-System-PIN. The AS or the Mini-HSM User respectively will be authenticated by using the HSM System PIN during the PACE protocol. The TOE enforces a minimal length of 10 octets of the HSM-System-PIN (PACE-PIN), which ensures that a password with high entropy can be chosen for authentication.

338 FIA_UAU.1: This SFR defines the rules for using TOE’s cryptographic functions or access to user data. The AS and the Mini-HSM User is authenticated via PACE. The access rules are implemented by the COS and cannot be changed by a user.

339 FIA_UAU.4: Any authentication data shall be unusable in a later authentication protocol. This is supported by the TOE using fresh generated random numbers. The authentication state achieved by PACE is maintained by secure messaging channel. If an authentication

error occurs the authentication state will be reset. This is implemented in the COS and cannot be changed.

340 FIA_UAU.5: The authentication of the AS or the Mini-HSM User respectively is controlled by the Access Rules laid down in the Operating System in a very early stage of the life cycle. This SFR restricts the authentication mechanisms to PACE. The authentication state is maintained by secure messaging channel. If an authentication error occurs the authentication state will be reset. This is implemented in the COS and cannot be changed.

341 FIA_UID.1: Similar to FIA_UAU.1 this SFR defines the access rules before the user is identified. Only the access to public data, as ATR/ATS bytes or data fields containing purely technical information is allowed. Additonally the authentication process itself (PACE) is allowed, too. All other actions require usally the authentication over an established communication channel. The access rules are implemented by the COS and cannot be changed by a user.

342 FIA_USB.1: The actual authentication state of user is bound to the user, and must be achieved by the corresponding protocol. All users are required to execute the authentication protocol successfully, since the initial state is always “not authenticated”. This is implemented by the COS and cannot be changed by a user.

343 FMT_LIM.1, FMT_LIM.2: Limitations of capabilities or availability are enforced by the Operating System of the TOE controlling the integrity of the stored access rules and the used functions. After Initialization all data testing-specific commands and actions are disabled. It is not possible to override these controls and restore them for use.

344 FMT_SMF.1, FMT_SMR.1: Maintaining the different roles and TSFs of the TOE using dedicated access rules cannot be changed or disabled in the Operating System. The assignment of a specific role is supported by a successful authentication and the following-up Secure Messaging. The embedded software (i.e. the operating system) enforces the application of the access rules before any function is allowed to proceed.

345 FPT_EMS.1: The Operating System of the TOE monitors the regular execution of commands, and if variations occur with test failures or integrity mismatch the communication is closed. The strict care of uniformity and non-overloading single components is implemented in the Operating System and will be described detailed in ADV and AVA documentation. This implies the leakage of any information about the private keys. This is supported by the Security Feature “Control of Operating Conditions” of the Hardware (cf. [HWST, SF.OPC).

346 FPT_FLS.1: The Operating System of the TOE guarantees that the TOE preserves a secure state if a test failure or integrity check mismatch occur. If the TOE is exposed to the external operating conditions out of range or if a failure, e.g. entropy loss of the random number generator, the TOE enters and preserves a secure state. This is supported by chip's hardware too.

347 FPT_PHP.3: The Operating System of the TOE monitors the regular execution of commands, and if variations, test failures or integrity mismatch occur the communication will be closed immediately. This is supported on the lower level by chip's hardware too.

348 FPT_TST.1: The self tests of the underlying hardware and additional test maintained by the TOE provide the means for demonstrating that the TSF operation is correct and that the data is not manipulated. In addition, the TOE’s hardware provides an automated continuous user transparent testing of certain functions. This includes, e.g. the entropy check of the hardware based random number generation.

349 FTP_ITC.1: The TOE enforces the communication via the trusted channel by access rules for the commands, which cannot be changed. Only data fields with purely technical information can be accessed outside the trusted channel. The channel will be closed if an error occurred; the session keys are invalidated immediately and cannot be used furthermore.

7.11 Statement of Compatibility

350 This is the statement of compatibility between this Composite Security Target and the Security Target Chip of the underlying hardware [HWST].

7.11.1 Relevance of Hardware TSFs

351 In the following lists the relevance of the hardware security services (SS) and functions (SF) for the composite security target is considered.

Relevant:

- SS.RNG: Random Number Generator
- SS.HW_DES: Triple-DES Co-processor
- SS.HW_AES: AES Co-processor
- SF.OPC: Control of Operating Conditions
- SF.PHY: Protection against Physical Manipulation
- SF.LOG: Logical Protection
- SF.SFR_ACC: Special Function Register Access Control
- SF.MEM_ACC: Memory Access Control

352 Note that the DES algorithm of the Security Service SS.HW_DES is used by the TOE in the algorithmic post-processing of the Random Number Generator. Nevertheless the Triple DES TDES is not used which implies that the reletated Security Objectives are not relevant (cf. p. 67).

Not relevant:

- SS.RECONFIG: Customer Reconfiguration
- SF.COMP: Protection of Mode Control
- SF.FFW: Firmware Firewall
- SF.FIRMWARE: Firmware Support

7.11.2 Security Requirements

353 The relevant Security Requirements of the TOE and the hardware can be mapped or are not relevant. They show no conflict between each other.

Security Requirements of the TOE related to the Composite ST:

354 The following Security Requirements of the TOE are specific for the Applications of the Security Module and have no conflicts with the underlying hardware.

- FCS_CKM.1/ECC
- FCS_CKM.1/ECKA-DH
- FCS_CKM.1/ECKA-EG
- FCS_CKM.1/PACE
- FCS_CKM.4
- FCS_COP.1/SIG-ECDSA
- FCS_COP.1/VER-ECDSA
- FCS_COP.1/IMP
- FCS_COP.1/PACE-ENC
- FCS_COP.1/PACE-MAC
- FCS_RNG.1
- FDP_ACC.2
- FDP_ACF.1
- FDP_SDI.2
- FDP_RIP.1
- FDP_ETC.1
- FDP_ITC.1
- FDP_UCT.1
- FDP_UIT.1
- FIA_ATD.1
- FIA_UAU.1
- FIA_UAU.4
- FIA_UAU.5
- FIA_UID.1
- FIA_USB.1
- FMT_LIM.1
- FMT_LIM.2
- FMT_SMF.1
- FMT_SMR.1
- FPT_EMS.1
- FPT_FLS.1
- FPT_PHP.3
- FPT_TST.1
- FTP_ITC.1

355 Note that some of these requirements, e.g., FCS_CKM.1/DH_PACE rely also on requirements of the hardware as FCS_RNG.1(HW). Nevertheless it is considered as not relevant, because the latter is already covered by FCS_RNG.1 of the TOE.

356 The remaining Security Requirements of the TOE can be mapped to Security Requirements of the hardware. They show no conflict between each other.

- FCS_COP.1/PACE-ENC and FCS_COP.1/PACE-MAC are AES-based and matches FCS_COP.1[AES](HW) of [HWST]
- FCS_RNG.1 matches FCS_RNG.1(HW) of [HWST]
- FMT_LIM.1 matches FMT_LIM.1(HW) of [HWST]

- FMT_LIM.2 matches FMT_LIM.2(HW) of [HWST]
- FPT_EMS.1 is supported by the Security Feature SF.OPC of the hardware ([HWST]) and the AVA_VAN.5 evaluation
- FPT_FLS.1 matches FPT_FLS.1(HW) of [HWST]
- FPT_PHP.3 matches FPT_PHP.3(HW) of [HWST]

Security Requirements of the hardware

- FAU_SAS.1(HW) is related to the manufacturing phase and therefore not relevant for the TOE
- FCS_COP.1[AES](HW) is covered by FCS_COP.1/PACE-ENC and FCS_COP.1/PACE-MAC of the Composite ST both using the AES co-processor
- FCS_COP.1[DES](HW) is not relevant, TDES is not used in the OS
- FCS_RNG.1(HW) matches FCS_RNG.1 of the Composite ST
- FDP_ACC.1[MEM](HW) and FDP_ACC.1[SFR](HW) (Subset access control) is not relevant for the TOE, but for the implementation of the OS, therefore it is covered by ADV_IMP.1 (Implementation representation of the TSF)
- FDP_ACF.1[MEM](HW) and FDP_ACF.1[SFR](HW) (Security attribute based access control) is not relevant for the TOE, but for the implementation of the OS, therefore it is covered by ADV_IMP.1 (Implementation representation of the TSF
- FDP_ITT.1(HW) (Basic internal transfer protection) is covered by FPT_EMS.1 of the Composite ST
- FDP_IFC.1(HW) (Subset information flow control) is covered by FPT_EMS.1 of the Composite ST
- FMT_SMF.1(HW) (Specification of Management Functions) is covered by FMT_SMF.1 of the Composite ST
- FMT_LIM.1(HW) (Limited capabilities) is covered by FMT_LIM.1 of Composite ST
- FMT_LIM.2(HW) (Limited availability) is covered by FMT_LIM.2 of Composite ST
- FMT_MSA.1[MEM](HW) and FMT_MSA.1[SFR](HW) (Management of security attributes) no conflicts
- FMT_MSA.3[MEM](HW) and FMT_MSA.3[SFR](HW) (Static attribute initialization) no conflicts
- FPT_FLS.1(HW) (Failure with preservation of secure state) matches FPT_FLS.1 of the Composite ST
- FPT_ITT.1(HW) (Basic internal TSF data transfer protection) is covered by FPT_EMS.1 of the Composite ST
- FPT_PHP.3(HW) (Resistance to physical attack) is covered by FPT_FLS.1 and FPT_PHP.3 of the Composite STFDP_SDI.2(HW) (Stored data integrity monitoring and action) concerns the hardware operation, does not conflict with SFRs of the TOE

FRU_FLT.2(HW) (Limited fault tolerance) concerns the hardware operation, does not conflict with SFRs of the TOESecurity Assurance Requirements

357 The chosen level of assurance of the hardware is EAL 6 augmented with ALC_FLR.1 and ASE_TSS.2. This includes AVA_VAN.5.

358 This shows that the Assurance Requirements of the TOE matches the Assurance Requirements of the hardware.

7.11.3 Security Objectives

359 The Security Objectives of the TOE and the hardware can be mapped or are not relevant. They show no conflict between each other.

Security Objectives of the TOE related to the Composite ST:

- O.Integrity covers O.HW_AES of the [HWST]
- O.Confidentiality covers O.HW_AES of the [HWST]
- O.Authentication covers O.HW_AES of the [HWST]
- O.AccessControl no conflict
- O.KeyManagement no conflict
- O.TrustedChannel no conflict
- O.Leakage covers O.Leak-Inherent and O.Leak-Forced from [HWST]
- O.PhysicalTampering covers O.Phys-Probing and O.Phys-Manipulation from [HWST]
- O.AbuseFunctionality covers O.Prot_Abuse-Func from [HWST]
- O.Malfunction matches O.Prot_Malfunction from [HWST]
- O.Sign no conflict
- O.KeyAgreementDH, O.KeyAgreementEG no conflict
- O.Random covers O.RND from [HWST]
- O.PACE no conflict

Security Objectives for the hardware ([HWST]):

- O.Leak-Inherent (Protection against Inherent Information Leakage) is covered by O.Leakage
- O.Phys-Probing (Protection against Physical Probing) is mapped to O.Physical-Tampering
- O.Malfunction (Protection against Malfunctions) is covered by the corresponding objective O.Malfunction of the TOE
- O.Phys-Manipulation (Protection against Physical Manipulation) is mapped to O.PhysicalTampering
- O.Leak-Forced (Protection against Forced Information Leakage) is covered by O.Leakage
- O.Abuse-Func (Protection against Abuse of Functionality) is covered by O.AbuseFunctionality

- O.Identification (Hardware Identification) is an objective related to the manufacturing phase. Its support by the TOE is considered in more detail in the Guidance Documentation and is subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1.
- O.RND (Random Numbers) is covered by Security Objective O.Random of the TOE
- O.HW_DES3 (Triple DES Functionality) is not relevant

  The TDES functionality is not used in TOE's OS, therefore related objectives must not be considered.
- O.HW_AES (AES Functionality) is mapped to O.Integrity, O.Authentication and O.Confidentiality.

  The AES Functionality is used to ensure the integrity, the confidentiality and the authenticity of user data during transmission
- O.CUST_RECONFIG: Customer Option Reconfiguration (not relevant)

  This functionality is not used in TOE's OS.
- O.EEPROM_INTEGRITY: Integrity support of data stored in EEPROM

  The hardware shall provide a mechanism to support the integrity of the data stored in the EEPROM. This objective is mapped due to the used in hardware security features to O.AbuseFunctionality, O.PhysicalTampering and O.Malfunction of the TOE.
- O.FM_FW: Firmware Mode Firewall (not relevant)

  This functionality is not used in TOE's OS.
- O.MEM_ACCESS is mapped to O.AbuseFunctionality

  This objective for the hardware supports the correct operation of the TOE providing memory area access control.
- O.SFR_ACCESS is mapped to O.AbuseFunctionality

  The objectives O.MEM_ACCESS and O.SFR_ACCESS support the correct operation of the TOE providing memory area access and Special Function Registers access control. Therefore these objectives are mapped to O.AbuseFunctionality.

7.11.4 Compatibility: TOE Security Environment

Assumptions

360 The following list shows that assumptions neither of the TOE nor of the hardware have any conflicts between each other. They are either not relevant for this Security Target or are covered by appropriate Security Objectives.

Assumptions for the TOE related to the Composite ST:

361 There are no additional assumptions besides the following ones.

Assumptions of the specific hardware platform ([HWST]):

- A.Check-Init (Check of Initialization Data by the Security IC Embedded Software)

  The Check of Initialization Data of the hardware is related to the Life Cycle Phase 2 "Manufacturing of the TOE" and should not be confused with the check

of Initialization Data during Personalization. The Assumption A.Check-Init is no more relevant after TOE Initialization, because Hardware Initialization Data is overridden by TOE's Initialization and Pre-Personalization Data.

- A.Key-Function (Usage of Key-dependent Functions)

  This assumption requires that key-dependent functions are implemented in the OS such that they are not susceptible to leakage attacks. It is covered by the Hardware's objective OE.Resp-Appl for the environment and applies to Life Cycle Phase 1 "Development".

Threats

362 The Threats of the TOE and the hardware can be mapped or are not relevant. They show no conflict between each other.

Threats for the TOE related to the Composite ST:

- T.Skimming no conflict
- T.Eavesdropping no conflict
- T.ID_Card_Tracing no conflict
- T.ForgeryInternalData covers T.RND of the Hardware ST [HWST]
- T.Counterfeit no conflict
- T.Abuse-Func matches the corresponding threat of the of the Hardware ST [HWST]
- T.Leakage matches T.Leak-Inherent and T.Leak-Forced of the Hardware ST [HWST]
- T.PhysicalTampering matches T.Phys-Probing and T.Phys-Manipulation of the Hardware ST [HWST]
- T.Malfunction matches corresponding threat of the Hardware ST [HWST]

Threats of the hardware ST ([HWST]):

- T.Unauthorised_Access Unauthorized Memory or Hardware Access

  This threat is related to the partitioning of memory areas in Boot Mode, Firmware Mode, System Mode and segmentation of memory areas in User Mode. This threat is covered by the objectives O.FW_HW, O.MEM_ACCESS, and O.SFR_ACCESS of the Hardware ([HWST]] and may be considered as part of the threat T.AbuseFunctionality of the Protection Profile [PP0095-SecMod].

7.11.5 Organizational Security Policies

363 The Organizational Security Policies of the TOE and the hardware have no conflicts between each other. They are shown in the following list.

Organizational Security Policies of the Composite ST of the TOE:

- P.Pre-Operational covers P.Process-TOE of the hardware ST
- P.Terminal no conflict
- P.ID_Card_PKI no conflict
- P.Terminal_PKI no conflict

- P.Trustworthy_PKI no conflict

Organizational Security Policies of the Hardware ST:

- P.Add-Components (Additional Specific Security Components) no conflict
  The TOE's hardware provides AES encryption/decryption and Area based Memory Access Control, Memory separation for different software parts and Special Function Register Access Control as security functionalities to the Security IC Embedded Software.
  They are used in security functionalities of the TOE and are considered in the implementation of the OS. The TOE's hardware provides also Triple-DES encryption and decryption, which is not used in the OS.
- P.Process-TOE ([HWST]) is covered by P.Pre-Operational of the Composite ST

7.11.6 Conclusion

364 No contradictions between the Security Targets of the TOE and the underlying hardware can be found.

7.12 Assurance Measures

365 The documentation is produced compliant to the Common Criteria Version 3.1. The following documents provide the necessary information to fulfill the assurance requirements listed in section 6.1.7.

Development

ADV_ARC.1	Security Architecture Description TCOS Secure Crypto Module
ADV_FSP.4	Functional Specification TCOS Secure Crypto Module
ADV_IMP.1	Implementation of the TSF TCOS Secure Crypto Module
ADV_TDS.3	Modular Design of TCOS Secure Crypto Module

Guidance documents

AGD_OPE.1	User Guidance TCOS Secure Crypto Module
AGD_PRE.1	Administrator Guidance TCOS Secure Crypto Module

Life-cycle support

ALC_CMC.4, ALC_CMS.4	Documentation for Configuration Management
ALC_DEL.1	Documentation for Delivery and Operation
ALC_LCD.1	Life Cycle Model Documentation TCOS Secure Crypto Module
ALC_TAT.1, ALC_DVS.1	Development Tools and Development Security for TCOS Secure Crypto Module

Tests

ATE_COV.2, ATE_DPT.1	Test Documentation for TCOS Secure Crypto Module
ATE_FUN.1	Test Documentation of the Functional Testing

Vulnerability assessment

AVA_VAN.5	Independent Vulnerability Analysis TCOS Secure Crypto Module

366 The developer team uses a configuration management system that supports the generation of the TOE. The configuration management system is well documented and identifies all different configuration items. The configuration management tracks the implementation representation, design documentation, test documentation, user documentation, administrator documentation, and security flaws. The security of the configuration management is described in detail in a separate document.

367 The delivery process of the TOE is well defined and follows strict procedures. Several measures prevent the modification of the TOE based on the developer's master copy and the user's version. The User is provided with necessary documentation for initialization and start-up of the TOE.

368 The implementation is based on an informal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements.

369 The tools used in the development environment are appropriate to protect the confidentiality and integrity of the TOE design and implementation. The development is controlled by a life-cycle model of the TOE. The development tools are well-defined and use semi-formal methods, i.e. a security model.

370 The development department is equipped with organizational and personnel means that are necessary to develop the TOE. The testing and the vulnerability analysis require technical and theoretical know-how available at T-Systems International GmbH.

371 As the evaluation is identified as a composite evaluation based on the CC evaluation of the hardware, the assurance measures related to the hardware (IC) will be provided by documents of the IC manufacturer.

Appendix Glossary and Acronyms

372 These are the unchanged tables from [PP0095-SecMod], more detailed information can be found there, too.

Acronyms

Term	Definition
ATR	Answer To Reset
ATS	Answer To Select
AUTH	External Authentication
AS	Application Server
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
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
EF	Elementary File
Enc	Encryption
ECDSA	Elliptic Curve Digital Signature Algorithm
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
EMT	Autorisierter Externer Marktteilnehmer
ENC	Content Data Encryption
GW	Gateway
GWA	Smart Meter Administrator, Mini-HSM Administrator
HAN	Home Area Network
HSM	High Security Module
HW	Hardware
ID	Identifier
Mini-HSM	Integrating Device
IT	Information Technology
KDF	Key Derivation Function
LMN	Local Metrological Network
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PKI	Zertifizierungsinfrastruktur / Public Key Infrastructure

Term	Definition
PP	Protection Profile
SAR	Security Assurance Requirement
SeCMod	Secure Crypto Module
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 Infrastructure (SM-PKI)
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

Glossary

Term	Description
Authenticity	Property that an entity is what it claims to be.
Authorized External Entity	So-called Autorisierter Externer Marktteilnehmer. External entity unlocked for communication with the Smart Meter Gateway.
CLS, Controllable Local Systems	CLS are systems containing IT-components in the Home Area Network (HAN) of the consumer that do not belong to the Smart Metering System but may use the Gateway for dedicated communication purposes. CLS may range from local power generation plants, controllable loads such as air condition and intelligent household appliances (“white goods”) to applications in home automation.
Commodity	Electricity, gas, water or heat.
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Consumer	End user of electricity, gas, water or heat (according to [CEN]).
External Entity	See chapter 3.1
Gateway Administrator	See chapter 3.1
Home Area Network (HAN)	In-house LAN which interconnects domestic equipment and can be used for energy management purposes (according to [CEN]).
Initialization	Completion of the OS by patch code and object system, see chapter 1.5.
Integrator	See chapter 1.5 and 3.1.
Integration	Installation of the TOE in the assigned Mini-HSM, see chapter 1.5 and 3.1. This finishes the IC Personalization.

Term	Description
Integrity	Property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
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 hyponym 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.

References

[AIS20/31]
Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS20/AIS 31, A proposal for Functionality classes for random number generators Version 2.0 vom 18.09.2011, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[AIS36]
Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Version 5 vom 15.03.2017, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[CC]
Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and General Model; Version 3.1, April 2017, CCMB-2017-04-001,
Part 2: Security Functional Requirements; Version 3.1, April 2017, CCMB-2017-04-002,
Part 3: Security Assurance Requirements; Version 3.1, April 2017, CCMB-2017-04-003

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, April 2017, CCMB-2017-04-004

[FIPS186]
Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013

[FIPS197]
Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), U.S. Department of Commerce/National Institute of Standards and Technology, 2001-11-26

[HWCR] Certification Report of the underlying hardware platform
BSI- DSZ-CC-0978-V2-2017 for NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE with IC Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[HWST] Security Target of the underlying hardware platform
NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE, Security Target Lite, BSI-DSZ-CC-0978-V2-2017

[ISO7816]
ISO 7816-4:2013, Identification cards – Integrated circuit cards with contacts, Part 4: Organization, security and commands for interchange, ISO, 2013-04

[ISO7810]
ISO/IEC 7810:2003, Identification cards -- Physical characteristics, ISO, 2010-05-03

[ISO14888-3]
ISO/IEC 14888-3:2006, Information technology – Security techniques – Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms, ISO, 2006

[PP0035-ICC]
Security IC Platform Protection Profile, Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0035-2007, 2007-06-15

[PP0073-SMGW]
CC Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Version 1.3, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0073-2014, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-03-31

[PP0095-SecMod]
Protection Profile for the Security Module of a Smart Meter Mini-HSM (Mini-HSM Security Module PP), Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0095-2017, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017-06-23

[RFC5639]
M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03

[SP800-38A]
Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST Special Publication 800-38A, National Institute of Standards and Technology, December 2001

[SP800-38B]
Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, May 2005

[TCOSADM]
Operational Guidance for users and administrators, Guidance Documentation of TCOS Secure Crypto Module Version 1.0 Release 1, T-Systems International GmbH, 2017-10

[TR03109]
Technische Richtlinie BSI TR-03109 Smart Energy, Version 1.0.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2015-11

[TR03109-1]
Technische Richtlinie BSI TR-03109-1: Smart Meter Gateway - Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2013-03

[TR03109-2]
Technische Richtlinie BSI TR-03109-2: Smart Meter Gateway - Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, Version 1.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-12

[TR03109-2 B]
BSI TR-03109-2 Anhang B: Smart Meter Mini-HSM - Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, BSI, Version 1.0, 2017-06

[TR03109-3]
Technische Richtlinie BSI TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, Version 1.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-04

[TR03109-4]
Technische Richtlinie BSI TR-03109-4: Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways, Version 1.2.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017-08

[TR03109-6]
Technische Richtlinie BSI TR-03109-6: Smart Meter Gateway Administration
Version 1.0, 26.11.2015

[SM-CP]
Certificate Policy der Smart Metering PKI, BSI, Version 1.1.1, 2017-08

[TR03110-1]
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

[TR03110-2]
Technical Guideline 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 2.21, 2016-12

[TR03110-3]
BSI TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, BSI, Version 2.21, 2016-12

[TR03111-ECC]
Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-06

[TR03116-3]
Technische Richtlinie TR-03116-3: eCard-Projekte der Bundesregierung, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3: Intelligente Messsysteme, BSI, Stand 2017,