STMicroelectronics

STSAFE-J100-BS Security Target Public Version

Common Criteria for IT security evaluation

STSAFE-J100-BS_Security_Target_Lite Rev. A
April 2018

life.augmented

BLANK

STSAFE-J100-BS
Security Target Public Version

Common Criteria for IT Evaluation

1. INTRODUCTION

1.1 Document Reference

Document identification: **STSAFE-J100-BS Security Target - Public Version**
Revision: **A**
Registration: STSAFE-J100-BS_Security_Target _Lite

1.2 Security Target Reference

Document identification: STSAFE-J100-BS Security Target
Revision: **I**
Registration: STSAFE-J100-BS_Security_Target

1.3 TOE Reference

TOE Name and Version: STSAFE-J100-BS V.2.1.6

INDEX

List of tables

List of figures

2. PURPOSE

This document presents the Security Target of STSAFE-J100-BS a smartcard application implementing the security module of a smart meter gateway designed as a Java card 3.0.4 applet integrated on STMicroelectronics STSAFE-J Java Card Platform designed on the ST31H320 HW platform (ST31H320 Security Integrated Circuit with dedicated software and embedded cryptographic library).

3. SCOPE

Due to the confidential nature of the contents, this document is intended for the sole use of Software Design Center of STMicroelectronics - srl Marcianise Italy the third-party laboratory and the certification body selected for the Common Criteria evaluation of the product.

4. REFERENCE DOCUMENTS

CC documents	
[CC_P1]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 1: Introduction and General Model; Version 3.1, September 2012, CCMB-2012-09-001,
[CC_P2]	Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002
[CC_P3]	Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004
[AIS31/20]	Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), 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 2 vom 12.11.2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)
Protection Profiles and Technical Guidelines	
[PP-0084]	BSI-CC-PP-0084-2014 – Eurosmart – Security IC Platform Protection Profile with Augmentation Packages
[PP-0073]	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
[PP-0077]	CC Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), Version 1.03, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0077-V2, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-12-11
[TR-03109]	Technische Richtlinie BSI TR-03109 Smart Energy, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2013-03
[TR-03109-1]	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
[TR-03109-2]	Technische Richtlinie BSI TR-03109-2: Smart Meter Gateway - Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.1, 15.12.2014 Technische Richtlinie BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.1, 17.12.2014
[TR-03109-3]	Technische Richtlinie BSI TR-03109-3: Kryptographische Vorgaben, Version 1.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-04
[TR-03109-4]	Technische Richtlinie BSI TR-03109-4: Public Key Infrastruktur für Smart Meter Gateway, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2013-03
[TR-03110-1]	Technical Guideline TR-03110-1: Advanced Security Mechanisms forMachine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20. March 2012
[TR-03110-2]	Technical Guideline TR-03110-2: Advanced Security Mechanisms for Machine Readable Travel Documents Part 2, Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-03-20
[TR-03110-3]	Technical Guideline TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specifications, Version 2.11, 12. July 2013
[TR-03111]	Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 1.11, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-04-17
[TR-03116-3]	Technische Richtlinie BSI TR-03116-3 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3: Intelligente Messsysteme Stand 2017 Datum: 23. Januar 2017
Specifications	
[ANSI_X9.62]	ANSI X9.62-2005: The Elliptic Curve Digital Signature Algorithm (ECDSA), approved November 16, 2005
[FIPS186]	Federal Information Processing Standards Publication FIPS PUB 186-3, Digital Signature Standard (DSS), 2009-06
[FIPS_180-2]	FIPS Publication 180-2: SECURE HASH STANDARD, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1
[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
[SP800-38B]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for

	Authentication, Special Publication 800-38B, May 2005.
[SP800-38A]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Special Publication 800-38A 2001 Edition
[SP800-90A]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators Special Publication 800-90A Rev.1 April 2014
[SP800-22]	National Institute of Standards and Technology, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications Special Publication 800-22 Rev.1a April 2010
[ISO7816]	ISO 7816-4, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, ISO/IEC, IS 2013
[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
[ISO 10116]	ISO/IEC 10116, Information technology - Security Techniques -- Modes of operation of an n-bit block cipher, ISO, 2006.
[RFC4493]	JH. Song, R. Poovendran The AES-CMAC Algorithm, June 2006
[RFC5639]	M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03
Platform documents	
[PP_JC_Closed]	Java Card System – Closed Configuration Protection Profile, Version 3.0, December 2012 [ANSSI-CC-PP-2010/07-M01]
[STSAFE-ST]	STSAFE-J on ST31H320 Security Target – Version Rev E January 2017
[STLite_ST31H320]	ST31H320 A03 including optional cryptographic library NESLIB - Security Target for Composition – Rev A03.0, June 2016.
[MntRep_ST31H320]	ST31H320 A02 including optional cryptographic library NESLIB – Rapport de maintenance ANSSI-CC-2015/59-M01, April 20, 2016.
[SrvRep_ST31H320]	ST31H320 including optional cryptographic library NESLIB – Rapport de surveillance ANSSI-CC-2015/59-S01, August 25, 2016.

5. DEFINITIONS

The following tables are taken over from [PP-0077] .

Acronyms

Term	Definition
ATR	Answer To Reset
ATS	Answer To Select
AUTH	External Authentication
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DEMA	Differential Electromagnetic Analysis
DF	Dedicated File
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
ENC	Content Data Encryption
GW	Gateway
GWA	Gateway Administrator
HAN	Home Area Network
HW	Hardware
ID	Identifier
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
PP	Protection Profile
PTRNG	Physical True Random Number Generator
RNG	Random Number Generator
SAR	Security Assurance Requirement
SecMod	Security Module / Sicherheitsmodul
SEMA	Simple Electromagnetic Analysis
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SIG	Content Data Signature
Sign	Signature
SM	Smart Meter
SMGW	Smart Meter Gateway
SM-PKI	Smart Metering - Public Key Infrastructure (SM-PKI)
SPA	Simple Power Analysis
ST	Security Target
TLS	Transport Layer Security
TOE	Target Of Evaluation
TR	Technische Richtlinie
TRNG	True Random Number Generator
TSF	TOE Security Functionality
WAN	Wide Area Network

Glossary

Term	Description
Authenticity	Property that an entity is what it claims to be. Property that concerns the truthfulness of origins of attributes, data and assets
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 8.1
Gateway Administrator	See chapter 8.1
Home Area Network (HAN)	In-house LAN which interconnects domestic equipment and can be used for energy management purposes (according to [CEN]).
Integrator	See chapter 8.1
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.

6. ST INTRODUCTION

1 This section provides information about the TOE, which enables a potential user of the TOE to determine, whether the TOE implements the functionality required by the user.

6.1 ST Reference

2 Title:	STSAFE-J100-BS Security Target
TOE name:	STSAFE-J100-BS Smart Meter Security Module V.2.1.6
Developer:	STMicroelectronics Z.I. Marcianise SUD I-81025 Marcianise (CE) ITALY
Status:	final
Version:	Rev.A
Date:	9.April.2018

6.2 TOE Reference

3 The Security Target refers to the TOE STSAFE-J100-BS Smartmeter Security Module V.2.1.6. This security module comprises three elements: the IC ST31H320 Security Integrated Circuit with dedicated software and embedded cryptographic library, the Java Card ™ Operating System STSAFE-J developed by STMicroelectronics and the applet STSAFE-J100-BS.

6.3 TOE Overview

4 The Target of Evaluation (TOE) a composite product comprising hardware and software implementing the security functionality according to [PP-0077] for the use by the Smart Meter Gateway of a Smart Metering System. The usage of the Security Module is described in the Protection Profile [PP-0073]

5 The Smart meter Gateway interconnects the LAN of the consumer with the external world via WAN. For this purpose, the Smart meter Gateway utilizes the TOE as a cryptographic service provider. The TOE provides cryptographic functionality based on elliptic curve cryptography such as the generation and verification of digital signatures and key agreement in the TLS framework, for content data signature and content data encryption.

6 The TOE supports the authentication of the Gateway implementing cryptographic authentication protocols and providing a high quality random number generator which must be used in these protocols.

7 Finally, the TOE provides functionality for secure storage of data on behalf of the Smart meter Gateway.

8 The TOE and its security functionality are specified from a technical point of view in [TR-03109-2]. The interaction with the Gateway is described in [TR-03109] and [PP-0073]. Therefore, the reader should be familiar with the requirements given in this Technical Guideline and the Protection Profile for the Gateway.

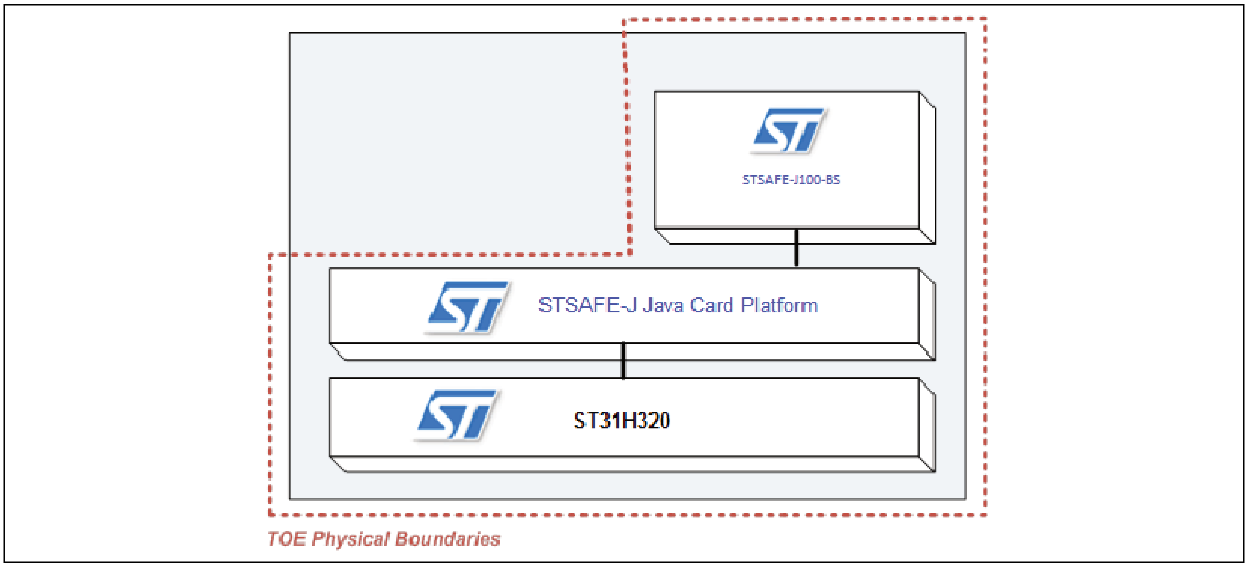


Figure 1 - TOE Overview

9 The Figure 1 shows the composition of the TOE parts. The TOE is a Java Card Flash memory based product.

10 During the Manufacturing phase the Java Card Package, including the STSAFE-J100-BS applet version V.2.1.6 are installed on the TOE.

11 During operational use phase the Security Module is integrated into the Gateway. The TOE primarily interacts with the Gateway itself, but also with the Gateway Administrator and possibly with other external entities.

12 The TOE provides the following cryptographic algorithms and protocols as services to the Gateway:

- Support of the authentication of the external entities with the TOE and with other external entities (TLS, PACE)
- Digital signature creation and verification (ECDSA)
- Secure storage of any private key
- Random Number Generation
- Secure communication channel with external entities (PACE)

13 The cryptographic algorithms and security parameters of these algorithms used by the TOE are defined in the Smart Metering Systems Infrastructure ([TR-03109-3]).

14 The TOE supports the standardized domain parameters brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 (refer to [RFC5639]) and the NIST curves P-256, P-384 ([FIPS186]) as listed in [TR-03116-3] .

15 The Security Module is integrated into an IC with VQFN32 5x5 mm package

The logical communication is implemented according to ISO-7816 on I2C interface for direct serial connection with a Gateway controller IC.

16 The TOE follows the composite evaluation aspects ([AIS36]). It is implemented as a composition of a Java applet upon a certified Java Platform on a certified IC. The consisting parts of the TOE are listed in the sec. 6.4.1

17 The Security Target of the underlying Operating System STSAFE-J Java Card Platform claims conformance to Java Card System – Closed Configuration Protection Profile, Version 3.0, December 2012 ([PP_JC_Closed])

18 This composite ST is based on the ST of the underlying Operating System STSAFE-J Java Card Platform ([STSAFE-ST])

6.3.1 Non-TOE hardware/software/firmware

19 The TOE is the Security Module intended to be used by a Smart Meter Gateway in a Smart Metering System. There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features.

20 In order to be powered up and to be able to communicate the TOE needs an appropriate device for power supply. For the regular communication, the TOE requires a device whose implementation matches the TOE's interface specification (see [TR-03109-2]).

6.4 TOE Description

6.4.1 TOE Definition

21 The TOE is a composition and comprises of the following parts:

- The circuitry of the chip including all IC Dedicated Software being active in the Operational Phase of the TOE (the integrated circuit, IC), ST31H320 including optional cryptographic library NESLIB.
- The Embedded Software:
  - Operating System STSAFE-J Java Card Platform Common Criteria Certified Version by STMicroelectronics
  - The Applet STSAFE-J100-BS version V.2.1.6 by STMicroelectronics
- The associated guidance documentation.

22 Important note: The TOE is closed Java Card implementation with a single applet, the STSAFE-J100-BS applet as a single instance. No post-issuance of further applets is possible to the TOE.

6.4.2 TOE usage and security features for operational use

23 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 data relevant for the Gateway.

6.4.3 Life Cycle Phases Mapping

24 A detailed description of the overall life cycle of a Gateway and its Security Module can be found in [TR-03109-1] and [TR-03109-2]. The Secure Module PP [PP-0077], uses the following life cycle for the TOE.

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

In the beneath discussion the following entities and roles are identified:

Security Module Embedded Software Developer: STMicroelectronics srl, Marcianise (CE) Italy

IC Designer, Developer and Manufacturer: STMicroelectronics SAS, Rousset France

IC Package and Test: STMicroelectronics

Security Module (TOE) manufacturer: STMicroelectronics srl, Marcianise (CE) Italy and STMicroelectronics SAS, Rousset France

Security Module (TOE) integrator: Gateway manufacturer/administrator

Life cycle phase 1 “Security Module Embedded Software Development”.

25 This phase addresses the development of the Embedded Software of the TOE

- IC Designer and embedded library, Operating System and Java Card Platform Common, javacard applet implmenetng the security module functionalities

Life cycle phase 2 “IC Development”

26 The IC Designer designs the IC, develops the IC Dedicated Software, provides information, user manual, guidance documentation, software and tools to the Operating System Developer.

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

27 The IC Manufacturer and IC Packaging Manufacturer are responsible for producing the IC including IC manufacturing, IC pre-personalization, implementing/installing IC Dedicated Software, IC testing, and IC packaging (production of IC modules).

Life cycle phase 4 “Security Module Product Finishing Process”

28 The Security Module 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.

29 The TOE is finished after initialization of the Embedded Software, i.e. installation and successful validation of the STSAFE-J100-BS Applet (testing of the integration of the applet on the Operating System and IC), which includes creation of a dedicated file system with security attributes. The TOE is ready for the import of User Data and delivery to the user.

30 At the end of this phase the TOE is delivered to the secure module integrator for the next phase. The deliverables are listed below:

- TOE (the secure module)
- Operational user guidance
- Preparation procedures guidance

Life cycle phase 5 “Security Module Integration”

31 The Integrator is responsible for the integration of the initialized Security Module and the Gateway, and the pre-personalization of the Security Module, i.e. the generation, installation and import of initial and preliminary key material and certificates on/to the Security Module.

32 The Integrator is responsible for preparing the initial key and certificate material as relevant for the integration phase.

33 A detailed description of the integration process and its single steps can be found in [TR-03109-1] and [TR-03109-2]).

34 Result of this integration phase is the integrated Gateway, consisting of the Gateway and its assigned Security Module. The Gateway and the Security Module are physically and

logically connected, the pairing between the Gateway and its Security Module has been carried out, and the Security Module is equipped with initial and preliminary key and certificate material.

Life cycle phase 6 “Security Module End-Usage”

35 At first operational key and certificate material is generated, installed and imported into the Security Module. This is task of the Gateway Administrator and is secured by using the initial and preliminary key and certificate material that was set-up in the preceding integration phase (phase 5). In spite of the fact that this task is usually called “personalization of the Security Module” this phase is not mapped to Phase 6 of [PP-0084], because it can be repeated at any time again.

36 Afterwards, the Security Module is used by the Gateway in the Smart Metering System as cryptographic service provider.

37 Administration of the integrated Gateway with its Security Module is performed by the Gateway Administrator. A detailed description of the TOE's end-usage and the TOE's collaboration and interaction with the Gateway in the operational phase (including personalization, administration and normal operation) can be found in [TR-03109-1], [TR-03109-2]) and [PP-0073].

6.4.4 TOE Boundaries

6.4.5 TOE Physical Boundaries

38 The TOE comprises module 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 VQFN32 5x5 mm. package. The IC in use is ST31H320 by STMicroelectronics.

39 The Security Module is physically embedded into the Gateway and protected by the same level of physical protection as assumed for and provided by the environment of the Gateway.

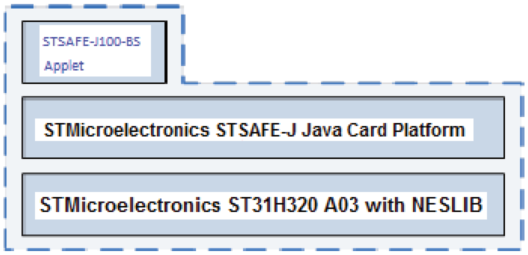

STSAFE-J100-BS Applet
STMicroelectronics STSAFE-J Java Card Platform
STMicroelectronics ST31H320 A03 with NESLIB

Figure 2 - TOE boundaries

6.4.6 TOE Logical Boundaries

40 The logical boundaries of the TOE can be identified by its security functionalities according to the Secure Module PP [PP-0077]:

- 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,
- Secure Storage of Key Material and further data relevant for the Gateway.

41 All these security functionalities are used by the Gateway to uphold the overall security of the Smart Metering System.

42 TOE's security functionalities are specified from a technical point of view in [TR-03109-2]. A detailed description of the security functionality provided by the TOE for use by the Gateway and in particular a detailed description of the TOE's collaboration and interaction with the Gateway can be found in [TR-03109-1], [TR-03109-2] and [PP-0073].

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

7. CONFORMANCE CLAIM

7.1 CC Conformance Claims

44 This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation [CC_P1]

- Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012,
- Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012,
- Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

45 as follows:

- Part 2 extended,
- Part 3 conformant.

46 The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012 [CC_P1]

47 has to be taken into account. The evaluation follows the Common Evaluation Methodology [CEM] with current final interpretations.

48 This ST is conformant to Common Criteria Part 2 [CC_P1]

49 and extended due to the use of additional SFRs FCS_RNG.1, FMT_LIM.1, FMT_LIM.2, and FPT_EMS.1 defined in the Protection Profile [PP-0077]

7.2 PP Claims

50 This ST claims strict conformance to the ‘CC Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)’, Version 1.03, BSI-CC-PP-0077-V2, 25.12.2014, [PP-0077].

7.3 Package Claims

51 The evaluation of the TOE is a composite evaluation and uses the results of the CC evaluation provided by [STSAFE-ST], [STLite_ST31H320] and [MntRep_ST31H320]. The TOE uses a certified STSAFE-J Java Card Platform and IC ST31H320 by STMicroelectronics. STSAFE-J Java Card Platform has been certified by ANSSI (cert. report ANSSI-CC-2017/23) with assurance level EAL5+ its associated Security Target is [STSAFE-ST]. The IC ST31H320 Secure Microcontroller with Cryptographic Library has been certified by ANSSI (cert. report ANSSI-CC-2015/59) with assurance level EAL5+: its associated Security Target Lite is [STLite_ST31H320] and the applicable Maintenance Report is [MntRep_ST31H320], [SrvRep_ST31H320].

52 The evaluation assurance level of the TOE is EAL4 augmented with AVA_VAN.5 as defined in [CC_P3].

7.4 Conformance Rationale

53 The ST claims strict conformance to the protection profile [PP-0077] as required there in sec. 2.5.

54 The TOE type as stated in [PP-0077], sec. 1.4.4 is a service provider for the Gateway for cryptographic functionality in type of a hardware security module with appropriate software installed’.

55 The current TOE type is a smartcard similar device, consisting of hardware and software installed. Thus, the required TOE type corresponds with the current TOE type in the PP [PP-0077], refer to sec. 6.3.

56 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 [PP-0077] .

57 The operations done for the SFRs taken from the PP [PP-0077]are clearly indicated.

58 The **Security Assurance Requirements** statement for the TOE in the current ST includes all the requirements for the TOE of the PP [PP-0077] as stated in chap. 11 below.

8. SECURITY PROBLEM DEFINITION

8.1 Subjects and external entities

59 The only external entity that directly interacts with the TOE in its operational phase is the corresponding Smart Meter Gateway of the Smart Metering System (called Gateway for short, in the following) as defined in [PP-0073] . In view of the TOE, the Gateway is responsible for sending and receiving TOE commands including the necessary data preparation and post-processing.

60 In addition, the Gateway Administrator who is in charge of the administration of the Gateway and its integrated Security Module (TOE), in particular the management of keys and certificates is indirectly interacting with the TOE via the Gateway.

61 In the operational phase, there are further external entities communicating with the Gateway, as e.g.:

- Consumer: The individual or organization that “owns” the Meter Data. In most cases this will be tenants or house owners consuming electricity, water, gas or further commodities. However, it is also possible that the consumer produces or stores energy (e.g. with their own solar plant).
- Gateway Operator: Responsible for installing and maintaining the Gateway. Responsible for gathering Meter Data from the Gateway and for providing these data to the corresponding external entities.

62 As these external entities only indirectly interact with the TOE, these entities are out of scope for this ST.

63 During its pre-operational phases the TOE interacts with the Integrator and the Gateway Administrator. The Integrator is responsible for the integration of the Gateway and the TOE as well as for generating, installing and importing initial respective preliminary key and certificate material. The Gateway Administrator is in charge of preparing the initial key material as relevant for the integration phase. In addition, in the following personalization phase (part of the operational phase), the Gateway Administrator is responsible for the exchange of the preliminary key and certificate material by operational key and certificate material. Refer for details to the description of the TOE life cycle model in chapter 6.4.3 and [TR-03109-1] and [TR-03109-2].

64 For the operational phase, this ST considers the following external entities and subjects:

Subject	Role	Definition
External World	User	Human or IT entity, possibly unauthenticated. The Integrator performing the integration of the TOE in to the Smart meter Gateway is also considered to be part of this role.
Gateway	Authenticated Gateway	Successful authentication via PACE protocol between Gateway and TOE
Gateway Administrator	Authenticated Gateway Administrator	Successful external authentication of the Gateway Administrator against the TOE

Table 1: Subjects

8.2 Assets

65 The Security Module (TOE) of a Smart Metering System can be seen as a cryptographic service provider for the Smart Meter Gateway. It provides different cryptographic functionalities based on elliptic curve cryptography, implements the cryptographic identities of the Gateway, and serves as a secure storage for cryptographic keys and certificates. More detailed, the main cryptographic services provided by the TOE 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 data relevant for the Gateway.

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

Asset	Protection			Definition
	Conf.	Int.	Auth.	
Key Pair Object	X	X	X	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)
Public Key Object		X	X	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) • AUTH (external authentication)
Certificate of SM-PKI-Root		X	X	X.509 Certificate of the SM-PKI-Root. The Certificate and its contained Public Key is to be considered as a trust anchor.
Public Key of SM-PKI-Root		X	X	In addition to the Certificate of the SM-PKI-Root, the Public Key of the SM-PKI-Root is stored in a dedicated Public Key Object of the TOE. The Public Key is to be considered as a trust anchor.
Quality of Seal Certificates of the Gateway		X	X	X.509 Certificates of the Gateway for preliminary Key Pair Objects used for TLS, SIG and ENC.
GW-Key	X	X	X	Symmetric key used by the Gateway to secure its memory.

Table 2: Assets User Data

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

Asset	Protection			Definition
	Conf.	Int.	Auth.	
Ephemeral Keys	X	X	X	Negotiated during the PACE protocol between the Gateway and the TOE, during the DH key agreement protocol (ECKA-DH) respective during the ElGamal key agreement protocol (ECKA-EG).
Shared Secret Value / ECKA-DH	X	X	X	Value Z_{AB} negotiated in the framework of the DH key agreement protocol (ECKA-DH). Used by the Gateway for the TLS handshake.
Shared Secret Value /	X	X	X	Value Z_{AB} negotiated in the framework of the ElGamal key agreement protocol (ECKA-EG). Used by the Gateway for content data encryption.

Asset	Protection			Definition
	Conf.	Int.	Auth.	
ECKA-EG				
Session Keys	X	X	X	Negotiated during the PACE protocol between the Gateway and the TOE and used afterwards for a trusted channel (secure messaging) between the Gateway and the TOE.
Domain Parameters of Elliptic Curves		X	X	Domain Parameters of the elliptic curves that are used by the key objects (key pair objects, public key objects) respective by the cryptographic functionality provided by the TOE.
GW-PIN	X	X	X	Reference value of the system PACE-PIN of the Gateway for use in the PACE protocol between the Gateway and the TOE.

Table 3: Assets TSF Data

8.3 Threats

68 This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the assets protected by the TOE and the method of TOE's use in the operational environment.

69 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 focused on the threats against the TOE.

70 The overall threat model for the Smart Metering System considers two different kinds of attackers to the Gateway and its integrated TOE, distinguishing between their different attack paths:

- Local attacker having physical access to the Gateway and its integrated TOE or a connection to these components.
- Attacker located in the WAN (WAN attacker) who uses the WAN connection for his attack.

71 Please note that the threat model assumes that the local attacker has less motivation than the WAN attacker (see below) as a successful attack of a local attacker will always only impact one Gateway respective its integrated TOE. Please further note that the local attacker includes the consumer.

72 Goal of the attack on the Gateway and its integrated TOE is to try to disclose or alter data while stored in the Gateway or TOE, while processed in the Gateway or TOE, while generated by the Gateway or TOE or while transmitted between the Gateway and the TOE. In particular, as the TOE serves as central cryptographic service provider and secure storage for key and certificate material for the Gateway, the assets stored, processed, generated and transmitted by the TOE are in focus of the attacker.

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

T.Name **Short title**

Description of the threats.

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

T.ForgeInternalData **Forgery of User Data or TSF Data**

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

76 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 (GW-PIN) to a known value.

T.CompromiseInternalData Compromise of confidential User Data or TSF Data

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

78 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 (GW-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

79 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.

80 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

81 An attacker with high attack potential tries to intercept the communication between the TOE and the Gateway to disclose, to forge or to delete transmitted (sensitive) data or to insert data in the data exchange.

82 This threat comprises several attack scenarios. An attacker may read data during data transmission in order to gain access to user authentication data (GW-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

83 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.

84 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 GW-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.

85 In addition, timing attacks have to be taken into account. The sources for this leakage information can be the measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines (side channels).

T.PhysicalTampering Physical tampering

86 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

87 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.

88 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 Gateway 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**

89 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.

90 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.

8.4 Organizational Security Policies

91 This section specifies the organizational security policies (OSP) that the TOE and its environment shall comply with in order to support the Gateway. These OSPs incorporate in particular the organizational security policy OSP.SM defined in the Gateway Protection Profile [PP-0073].

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

P.Name **Short title**

Description of the organizational security policy.

P.Sign **Signature generation and verification**

93 The TOE shall generate and verify digital signatures according to [TR-03109-3] and [TR-03109-2]. The explicit generation and verification of digital signatures is used by the Gateway 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**

94 The TOE and the Gateway shall implement the DH key agreement (ECKA-DH) according to [TR-03109-3] and [TR-03109-2]. The DH key agreement is used by the Gateway in the framework of the TLS handshake. The Gateway uses the generated shared secret value Z_{AB} 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**

95 The TOE and the Gateway shall implement the ElGamal key agreement (ECKA-EG) according to [TR-03109-3] and [TR-03109-2]. The ElGamal key agreement is used by the Gateway in the framework of the content data encryption. The Gateway uses the generated shared secret value Z_{AB} for the generation of the symmetric encryption keys (hybrid encryption/decryption scheme).

P.Random **Random number generation**

96 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 Gateway itself according to [TR-03109-3] and [TR-03109-2].

P.PACE **PACE**

97 The TOE and the Gateway shall implement the PACE protocol according to [TR-03110-2], [TR-03109-3], [TR-03109-2] for component authentication between the Gateway and the TOE. In the framework of the PACE protocol session keys for securing the data exchange between the Gateway and the TOE (trusted channel) are negotiated. The TOE and/or its environment shall comply with the following Organizational Security Policies (OSP) as

security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

8.5 Assumptions

98 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.

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

A.Name **Short title**

Description of the assumption.

A.Integration **Integration phase of the Gateway and TOE**

100 It is assumed that appropriate technical and/or organizational security measures in the phase of the integration of the Gateway and the TOE in the TOE life cycle model guarantee for the confidentiality, integrity and authenticity of the assets of the TOE to be protected with respect to their protection need (refer to [PP-0077], Table 4 and Table 5).

101 In particular, this holds for the generation, installation and import of initial key, certificate and PIN material.

102 The Integrator in particular takes care for consistency of key material in key objects and associated certificates as far as handled in the framework of the integration of the Gateway and the TOE.

A.OperationalPhase **Operational phase of the integrated Gateway**

103 It is assumed that appropriate technical and/or organizational measures in the operational phase of the integrated Gateway guarantee for the confidentiality, integrity and authenticity of the assets of the TOE to be protected with respect to their protection need (cf. [PP-0077]), Table 4 and Table 5]). In particular, this holds for key and PIN objects stored, generated and processed in the operational phase of the integrated Gateway.

A.Administration **Administration of the TOE**

104 The administration of the integrated TOE, in particular related to the administration of the TOE's file and object system consisting of folders, data files and key objects, takes place under the control of the Gateway Administrator.

105 The Gateway Administrator is responsible for the key management on the integrated TOE and takes in particular care for consistency of key material in key objects and associated certificates.

A.TrustedAdmin **Trustworthiness of the Gateway Administrator**

106 It is assumed that the Gateway Administrator is trustworthy and well-trained in particular in view of the correct and secure usage of the TOE.

A.PhysicalProtection **Physical protection of the TOE**

107 It is assumed that the TOE is physically and logically embedded into a Gateway that is certified according to [PP-0073] (whereby the integration is performed during the integration phase of the life cycle model).

108 It is further assumed that the Gateway is installed in a non-public environment within the premises of the consumer that provides a basic level of physical protection. This protection covers the Gateway, the TOE, the Meters that the Gateway communicates with and the communication channel between the Gateway and the TOE.

9. SECURITY OBJECTIVES

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

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

O/OE.Name **Short title**

Description of the objective.

9.1 Security Objectives for the TOE

111 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 or TSF Data**

112 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 or TSF Data**

113 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 GW-PIN) under the TSF scope of control.

O.Authentication **Authentication of external entities**

114 The TOE shall support the authentication of human users (Gateway Administrator) and the Gateway. The TOE shall be able to authenticate itself to the Gateway.

O.AccessControl **Access control for functionality and objects**

115 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**

116 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 Gateway.

O.TrustedChannel **Trusted channel**

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

O.Leakage **Leakage protection**

118 The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits. The TOE shall provide side channel resistance, i.e. shall be able to prevent appropriately leakage of information, e.g. electrical characteristics like power consumption or electromagnetic emanations that would allow an attacker to learn about private key material, confidential results or intermediate results of cryptographic computations, the GW-PIN.

O.PhysicalTampering Protection against physical tampering

119 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.

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

O.AbuseFunctionality Protection against abuse of functionality

121 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.

122 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 Gateway 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

123 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

124 The TOE shall securely generate and verify digital signatures according to [TR-03109-3], [TR-03109-2]. The explicit generation and verification of digital signatures is used by the Gateway 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

125 The TOE shall securely implement the DH key agreement (ECKA-DH) according to [TR-03109-3] and [TR-03109-2]. The DH key agreement is used by the Gateway in the framework of the TLS handshake. The Gateway uses the generated shared secret value Z_{AB} 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

126 The TOE shall securely implement the ElGamal key agreement (ECKA-EG) according to [TR-03109-3] and [TR-03109-2]. The ElGamal key agreement is used by the Gateway in the framework of the content data encryption. The Gateway uses the generated shared secret value Z_{AB} for the generation of the symmetric encryption keys (hybrid encryption/ decryption scheme).

O.Random Random number generation

127 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 Gateway itself according to [TR-03109-3] and [TR-03109-2].

O.PACE PACE

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

9.2 Security Objectives for the Operational Environment

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

OE.Integration Integration phase of the Gateway and TOE

130 Appropriate technical and/or organizational security measures in the phase of the integration of the Gateway 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

131 In particular, for the TOE, this shall hold for the generation, installation and import of initial key, certificate and PIN material.

132 The Integrator shall in particular take care for consistency of key material in key objects and associated certificates as far as handled in the framework of the integration of the Gateway and the TOE.

OE.OperationalPhase Operational phase of the integrated Gateway

133 Appropriate technical and/or organizational measures in the operational phase of the integrated Gateway 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 [PP-0077] , chap. 3.2).

134 In particular, this shall hold for key and PIN objects stored, generated and processed in the operational phase of the integrated Gateway.

OE.Administration Administration of the TOE

135 The administration of the integrated TOE, in particular related to the administration of the TOE's file and object system consisting of folders, data files and key objects, shall take place under the control of the Gateway Administrator.

136 The Gateway Administrator shall be responsible for the key management on the integrated TOE and shall in particular take care for consistency of key material in key objects and associated certificates.

OE.TrustedAdmin Trustworthiness of the Gateway Administrator

137 The Gateway Administrator shall be trustworthy and well-trained, in particular in view of the correct and secure usage of the TOE.

OE.PhysicalProtection Physical protection of the TOE

138 The TOE shall be physically and logically embedded into a Gateway that is certified according to [PP-0073] (whereby the integration is performed during the integration phase of the life cycle model).

139 The Gateway shall be installed in a non-public environment within the premises of the consumer that provides a basic level of physical protection. This protection shall cover the Gateway, the TOE, the Meters that the Gateway communicates with and the communication channel between the Gateway and the TOE.

OE.KeyAgreementDH DH key agreement

140 The Gateway shall securely implement the Diffie-Hellman key agreement (ECKA-DH) according to [TR-03109-2] and [TR-03109-3].

141 The DH key agreement is used by the Gateway in the framework of the TLS handshake. The Gateway uses the generated shared secret value Z_{AB} 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

142 The Gateway shall securely implement the ElGamal key agreement (ECKA-EG) according to [TR-03109-2] and [TR-03109-3].

143 The ElGamal key agreement is used by the Gateway in the framework of the content data encryption. The Gateway uses the generated shared secret value Z_{AB} for the generation of the symmetric encryption keys (hybrid encryption/decryption scheme).

OE. PACE PACE

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

OE.TrustedChannel Trusted channel

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

9.3 Security Objective Rationale

146 The following table is taken over from the Protection Profile [PP-0077]. It gives give an overview how the assumptions, threats and organizational security policies are addressed by the security objectives for the TOE and its environment.

147 The table combines/repeats the Tables 6 and 7 from [PP-0077], sec. 4.3 and 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	OE.Integration	OE.OperationalPhase	OE.Administration	OE.TrustedAdmin	OE.PhysicalProtection	OE.KeyAgreementDH	OE.KeyAgreementEG	OE.PACE	OE.TrustedChannel
T.ForgeInternalData	x																							
T.CompromiseInternalData		x																						
T.Misuse	x	x	x	x																				
T.Intercept				x		x									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									x			
P.KeyAgreementEG						x							x									x		
P.Random														x										
P.PACE															x								x	
A.Integration																x								
A.OperationalPhase																	x							
A.Administration																		x						
A.TrustedAdmin																			x					
A.PhysicalProtection																				x				

Table 4: Security Objectives Rationale

9.3.1 Countering the threats

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

T.ForgeInternalData

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

T.CompromiseInternalData

150 The threat **T.CompromiseInternalData** is countered by the security objective **O.Confidentiality**.The security objective **O.Confidentiality** directly cares for the confidentiality of the User Data and the TSF Data under the TSF scope of control.

T.Misuse

151 The threat **T.Misuse** is countered by a combination of the security objectives **O.AccessControl**, **O.Authentication**, **O.Integrity** and **O.Confidentiality**.The security objective **O.AccessControl** prescribes the access control policy defined for the TOE and ensures for its enforcement. Authentication as needed for regulating the access to the TOE's functionality and the assets stored in and processed by the TOE is addressed by the security objective **O.Authentication**. The security objectives **O.Integrity** and **O.Confidentiality** ensure the protection of the assets independent of the TOE functionality used by the attack.

T.Intercept

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

T.Leakage

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

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

T.PhysicalTampering

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

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

157 Both objectives together ensure for the TOE's physical security and therefore contribute to the security of the internal User Data and TSF Data stored in and processed by the TOE

as well as contribute to the security and correct functioning of the (cryptographic) services provided by the TOE.

T.AbuseFunctionality

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

T.Malfunction

159 The threat **T.Malfunction** is countered by the security objective **O.Malfunction**.The security objective **O.Malfunction** directly averts the threat by ensuring the TOE's correct operation and preservation of a secure state to prevent errors and deactivation of security features of functions even under abnormal environmental conditions.

9.3.2 Coverage of Organisational security policies

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

P.Sign

161 The organisational security policy **P.Sign** that mandates that the TOE implements digital signature generation and verification according to [TR-03109-3], [TR-03109-2] is directly addressed by the security objective **O.Sign**. The security objective **O.KeyManagement** serves for the availability of the keys as necessary for the cryptographic operation.

P.KeyAgreementDH

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

P.KeyAgreementEG

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

P.Random

164 The organisational security policy **P.Random** that mandates that the TOE implements random number generation for its own use and for use by the Gateway according to [TR-03109-3], [TR-03109-2] is directly addressed by the security objective **O.Random**.

P.PACE

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

9.3.3 Coverage of Assumptions

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

A.Integration

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

A.OperationalPhase

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

A.Administration

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

A.TrustedAdmin

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

A.PhysicalProtection

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

10. EXTENDED COMPONENTS DEFINITION

This Security Target uses components defined as extensions to CC part 2. All these extended components are drawn from Definitions of chapter 5 of [PP-0077]. The components FCS_RNG, FMT_LIM and FPT_EMS are common in Protection Profiles for smart cards and similar devices.

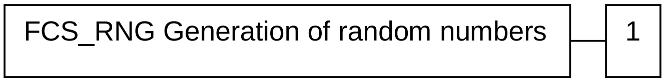
10.1 FCS_RNG Generation of random numbers

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

Family behaviour:

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*].

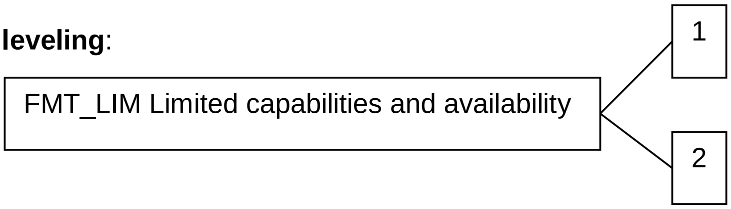
10.2 FMT_LIM Limited capabilities and availability

The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

Family behaviour:

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

Component leveling:



FMT_LIM.1 Limited capabilities require that the TSF is built to provide only the capabilities (perform action, gather information) which are 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.

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.

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.

Application Note:

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

The combination of both requirements shall enforce the policy.

10.3 FPT_EMS TOE Emanation

The family "TOE Emanation (FPT_EMS)" is specified as follows.

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMS TOE emanation
1

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

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*].

11. SECURITY REQUIREMENTS

11.1 Overview

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

173 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_P1]

174 Each of these operations is used in this ST.

175 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~~.

176 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*.

177 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*.

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

179 This part defines the detailed security requirements that are satisfied by the TOE. These requirements comprise functional components from CC Part 2 [CC_P1]

180 Extended components as defined in Chapter 10, and the assurance components as defined for the Evaluation Assurance Level EAL4 from CC Part 3 [CC_P1]

181 Augmented by AVA_VAN.5.

182 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/AUTH	Cryptographic operation/External authentication
FCS_COP.1/IMP	Cryptographic operation/Import of Public Keys
FCS_COP.1/PACE-ENC	Cryptographic operation/AES in CBC mode for secure messaging
FCS_COP.1/PACE-MAC	Cryptographic operation/AES-CMAC for secure messaging
FCS_RNG.1	Random number generation
Class FDP: User Data Protection	
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_SDI.2	Stored data integrity monitoring and action
FDP_RIP.1	Subset residual information protection
FDP_ETC.1	Export of user data without security attributes
FDP_ITC.1	Import of user data without security attributes
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
Class FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1/GW	Timing of authentication (for Gateway)
FIA_UAU.1/GWA	Timing of authentication (for Gateway Administrator)
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 5: SFR Overview

11.2 Class FCS Cryptographic Support

183 The Security Module serves as a cryptographic service provider for the Smart Meter Gateway and provides services in the following cryptographic area:

- 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 (AES), and
- Secure Storage of Key Material and further data relevant for the Gateway.

184 The cryptographic algorithms that shall be supported by the Gateway and its Security Module are defined in [TR-03109-3] respective in [TR-03116-3].

185 [TR-03109-3] respective [TR-03116-3] 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. The Security Module supports ECC key generation, ECDSA signature generation and verification, ECKA-DH, ECKA-EG and PACE all the key sizes and domain parameters for elliptic curves that are defined in [TR-03109-3] respective in [TR-03116-3].

186 The TOE supports the following elliptic curve domain parameters according to [TR-03116-3], sec 2.2:

Elliptic curve	Key size, bits	Specification
brainpoolP256r1	256	[RFC5639], sec 3.4
brainpoolP384r1	384	[RFC5639], sec. 3.6
brainpoolP512r1	512	[RFC5639], sec. 3.7
NIST P-256 (secp256r1)	256	[FIPS186], sec. D.1.2.3
NIST P-384 (secp384r1)	384	[FIPS186], sec. D.1.2.4

Table 6: Supported ECC curves

The TOE supports the following algorithms according to [TR-03109-3], sec. 1:

Algorithm	Key size, bits	Specification
ECDSA	See Table: 6	[TR-03111]
ECKA-DH	See Table: 6	[TR-03111]
ECKA-EG	See Table: 6	[TR-03111]
AES in CBC mode	128, 192, 256	[FIPS197],[ISO 10116]
AES in CMAC mode	128, 192, 256	[FIPS197], [RFC4493], [SP800-38B]

Table 7: Supported cryptographic algorithms

11.2.1 Cryptographic key generation (FCS_CKM.1)

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

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 *ECDSA key generation compliant to Chapter 4.1.3* [TR-03111][1] and specified cryptographic key sizes *256, 384 and 512 bit length group order*[2] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2][3].

188 *Application Note 1:* [TR-03109-2] requires the TOE to implement the command Generate Asymmetric Key Pair. The generated key pairs are used by the Gateway for TLS as well as for content data encryption and signature. The refinement for ECC keys is made by the Protection Profile [PP-0077].

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 [PP-0077])
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*[4] and specified cryptographic key sizes *128, 192 and 256 bit*[5] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2][6].

189 *Application Note 2:* The TOE generates a shared secret value according to [TR-03111].

190 *Application Note 3:* [TR-03109-2] requires the TOE to implement the command General Authenticate / variant ECKA-DH. Please note that the TOE is used by the Gateway for parts of the TLS key negotiation between the Gateway and the external world as outlined in [PP-0073]. The TOE creates on behalf of the Gateway the so-called shared secret value Z_{AB} for the pre-master secret. The key derivation function is not part of the TOE.

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 [PP-0077]) 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*[7] and

[1] [assignment: *cryptographic key generation algorithm*]
[2] [assignment: *cryptographic key sizes*]
[3] [assignment: *list of standards*]
[4] [assignment: *cryptographic key generation algorithm*]
[5] [assignment: *cryptographic key sizes*]
[6] [assignment: *list of standards*]
[7] [assignment: *cryptographic key generation algorithm*]

specified cryptographic key sizes *128, 192 and 256 bit*[8] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2][9].

191 *Application Note 4:* The TOE generates a shared secret value according to [TR-03111].

192 *Application Note 5:* [TR-03109-2] requires the TOE to implement the command GENERAL AUTHENTICATE/variant ECKA-EG. Please note that the TOE is used by the Gateway for parts of the TLS key negotiation between the Gateway and the external world as outlined in [PP-0073]. The TOE creates on behalf of the Gateway the so-called shared secret value Z_{AB} for the pre-master secret. The key derivation function is not part of the TOE.

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 [PP-0077])
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*[10] and specified cryptographic key sizes *128, 192 and 256 bit*[11] that meet the following:[TR-03110-2], [TR-03109-3] respective [TR-03116-3], [TR-03109-2][12].

193 *Application Note 6:* The TOE generates a shared secret value according to PACEv2 defined in [TR-03110-2], sec. 3.2.

194 Application Note 7: [TR-03109-2] requires the TOE to implement the command General Authenticate/variant PACE. The TOE exchanges a shared secret with the Gateway during the PACE protocol. The shared secret is used for deriving the AES session key of key size 128,192 and 256 bit for message encryption as required by FCS_\ COP.1/PACE-ENC and for deriving the AES session key of key size 128,192 and 256 bit for message authentication as required by FCS_COP.1/PACE-MAC. Secure messaging is carried out for the main data exchange between the Gateway and the TOE.

195 *Application Note 8:* This SFR implicitly contains the requirements for the hashing functions used for the key derivation by demanding compliance to [TR-03110-2], [TR-03109-3] respective [TR-03116-3], [TR-03109-2].

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*[13] that meets the following: *none*[14].

[8] [assignment: *cryptographic key sizes*]
[9] [assignment: *list of standards*]
[10] [assignment: *cryptographic key generation algorithm*]
[11] [assignment: *cryptographic key sizes*]
[12] [assignment: *list of standards*]
[13] [assignment: *cryptographic key destruction method*]
[14] [assignment: *list of standards*]

196 ***Application Note** 9:* The TOE destroys the shared secret Z_{AB}, the encryption session keys and the message authentication keys negotiated via the PACE protocol after reset, termination the session or reaching the fail secure state according to FPT_FLS.1 The TOE clears the memory area of any session keys before starting the communication with the external entities in a new after-reset-session as required by FDP_RIP.1.

197 ***Application Note** 10:* The TOE provides the command DELETE KEY which overwrites the memory area of a key with zeros with the use of the Key.clearKey() Java Card API.

198 ***Application Note 11:*** The TOE destroys the negotiated shared secret value Z_{AB} after it has been transmitted to the Gateway as required by FCS_CKM.1/ECKA-DH and by FCS_CKM.1/ECKA-EG

11.2.2 Cryptographic operation (FCS_COP.1)

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

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: 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[16] and cryptographic key sizes *256, 384 and 512 bit*[17] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2][18].

200 ***Application Note** 12:* The signature algorithm EC-DSA (ECDSA in [PP-0077]) is defined in the ISO/IEC Standard [ISO14888-3]. Note that the algorithm ECDSA in NIST Standard [FIPS186] is restricted to the NIST curves only. Furthermore the ECDSA signature generation algorithm is described in [TR-03111] chapter 4.2.1.1.

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 [20] and cryptographic key sizes *256, 384 and 512 bit length group order* [21] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2][22].

[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*]

201 ***Application Note** 13:* The signature algorithm EC-DSA (ECDSA in [PP-0077]) is defined in the ISO/IEC Standard [ISO14888-3]. Note that the algorithm ECDSA in NIST Standard [FIPS186] is restricted to the NIST curves only. Furthermore the ECDSA signature verification algorithm is described in [TR-03111] chapter 4.2.1.2.

FCS_COP.1/AUTH Cryptographic operation – External Authentication

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/AUTH The TSF shall perform signature verification for external authentication for the command EXTERNAL AUTHENTICATE[23] in accordance with a specified cryptographic algorithm ECDSA[24] and cryptographic key sizes *256, 384, 512 bit*[25] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2][26].

202 ***Application Note* 14*:*** As refinement operation for the generic references given in the PP, the specification of ECDSA signature verification algorithm is described in [TR-03111] chapter 4.2.1.2.

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[27] in accordance with a specified cryptographic algorithm ECDSA[28] and cryptographic key sizes *256, 384, 512 bit*[29] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2][30].

203 ***Application Note 15:*** As refinement operation for the generic references given in the PP, the specification of ECDSA signature verification algorithm is described in [TR-03111] chapter 4.2.1.2.

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

Hierarchical to: No other components.

[20] [assignment: *cryptographic algorithm*]
[21] [assignment: *cryptographic key sizes*]
[22] [assignment: *list of standards*]
[23] [assignment: *list of cryptographic operations*]
[24] [assignment: *cryptographic algorithm*]
[25] [assignment: *cryptographic key sizes*]
[26] [assignment: *list of standards*]
[27] [assignment: *list of cryptographic operations*]
[28] [assignment: *cryptographic algorithm*]
[29] [assignment: *cryptographic key sizes*]
[30] [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/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 PACE encryption[31] in accordance with a specified cryptographic algorithm AES in CBC mode[32] and cryptographic key sizes *128, 192 and 256 bit*[33] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2][34].

204 ***Application Note 16:*** This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data and for encrypting the nonce in the first step of PACE. The related session keys (for secure messaging) and key for encryption of the PACE nonce are agreed between the TOE and the Gateway as part of the PACE protocol according to the FCS_CKM.1/PACE.

205 ***Application Note 17:*** As refinement operation for the generic references given in the PP, the specification of AES algorithm is described in [FIPS197] chapter 5 and the CBC mode algorithms is described in [ISO 10116] chapter 7

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[35] in accordance with a specified cryptographic algorithm AES-CMAC[36] and cryptographic key sizes *128, 192 and 256 bit*[37] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2][38].

206 ***Application Note 18*:** This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys (for secure messaging) are agreed between the TOE and the Gateway as part of the PACE protocol according to the FCS_CKM.1/PACE.

207 ***Application Note 19:*** As refinement operation for the generic references given in the PP, the specification of AES algorithm is described in [FIPS197] chapter 5 and the CMAC mode algorithms is described in [RFC4493] chapter 2.

11.2.3 Random Number Generation (FCS_RNG.1)

[31] [assignment: *list of cryptographic operations*]
[32] [assignment: *cryptographic algorithm*]
[33] [assignment: *cryptographic key sizes*]
[34] [assignment: *list of standards*]
[35] [assignment: list of cryptographic operations]
[36] [assignment: cryptographic algorithm]
[37] [assignment: cryptographic key sizes]
[38] [assignment: list of standards]

FCS_RNG.1 Quality metric for random numbers

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

FCS_RNG.1.1

The TSF shall provide a *deterministic*[39] random number generator that implements: *DRG.3 capabilities defined in [AIS31/20] standard*[40]:

(DRG.3.1) *if initialized with a random seed using a PTRNG of class PTG.2 as random source, the internal state of the RNG shall have at least 100 bits of min-entropy.*

(DRG.3.2) *The RNG provides forward secrecy*

(DRG.3.3) *The RNG provides backward secrecy even if the current internal state is known.*

FCS_RNG.1.2 The TSF shall provide random numbers that meet *Class DRG.3 deterministic random defined in [AIS31/20] standard*[41]*based on Hash_DRBG of* [SP800-90A] *where the hash function is the SHA-256*

(DRG.3.4) *The RNG initialized with a random seed during every startup and after 2^{32} requests, generates output for more than 2^{34} strings of bit length 128 that are mutually different with probability of $w>1-2^{-16}$.*

(DRG.3.5) *Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A and the NIST statistical test suite* [SP800-22]

208 ***Application Note 20****:* Random numbers are generated for the Gateway and for TOE internal use, in particular for

- support of the TLS handshake (prevention of replay attacks),
- enabling the external authentication of the Gateway,
- PACE protocol,
- DH key agreement,
- ElGamal key agreement,
- generation of ECC key pairs.
- ECDSA algorithm

209 In particular, [TR-03109-2] requires the TOE to implement the command GET CHALLENGE for the generation of random numbers that are exported to the external world (here the GW) and if desired are in addition available in the TOE for further use. In the case that the GW implements a deterministic RNG and tears the seed for this RNG (as random number) from the TOE sufficient quality respective entropy of the seed has to be taken into account.

11.3 Class FDP User Data Protection

210 Access Control Smart Meter SFP

[39] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

[40] [assignment: list of security capabilities]

[41] [assignment: a defined quality metric]

211 The Access Control Smart Meter SFP for the Smart Meter Security Module (TOE) in its operational phase is based on the specification of access rules in [TR-03109-2]. The SFP takes the following subjects, objects, security attributes and operations into account:

212 Subjects:

- external world
- Gateway
- Gateway Administrator

213 Security attributes for subjects:

- “authenticated via PACE protocol”
- “authenticated via key-based external authentication”

214 Objects:

- key pair objects
- public key objects
- certificates
- symmetric keys (GW-keys)

as presented in Table 2.

215 Security attributes for objects:

- “access rule” (see below)

216 Operations:

- TOE commands as specified in [TR-03109-2]

217 The Access Control Smart Meter 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.

218 For the Access Control Smart Meter SFP, the access rules are defined as prescribed in [TR-03109-2].

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 SFP*[42] on[43]:

1. Subjects:
   a. external world
   b. Gateway
   c. Gateway Administrator
   d. *none*[44],
2. Objects:
   a. key pair objects, public key objects, certificates, and symmetric keys (GW-keys) as presented in Table 2
   b. *none* [45]

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

[42] [assignment: *access control SFP*]

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

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

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

covered by an access control SFP.

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 SFP[46] to objects based on the following[47]:

1. Subjects:
   a. external world
   b. Gateway with security attribute "authenticated via PACE protocol"
   c. Gateway Administrator with security attribute "authenticated via key-based external authentication"
   d. *none* [48],
2. Objects:
   a. key pair objects, public key objects, certificates, and symmetric keys (GW-keys) as presented in Table 2 each with security attribute "access rule"
   b. *none* [49].

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 SFP (refer to the definition of the SFP above)[50].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[51].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: No entity shall be able to read out private keys from the TOE[52].

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[53] on all objects, based on the following attributes: *integrity checked stored data*[54].

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[55], *none*[56].

[46] [assignment: *access control SFP*]

[47] [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*]

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

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

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

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

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

[53] [assignment: *integrity errors*]

[54] [assignment: *user data attributes*]

219 ***Application Note** 21**: The requirements in FDP_SDI.2.1 specifically apply to the assets as defined in Table 2: Assets User Data.***

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*[57] the following objects[58]: PIN, session keys (immediately after closing related communication session),private cryptographic keys, shared secret value Z_{AB}, ephemeral keys, *none*[59].

220 ***Application Note*** *22***: Upon de-allocation old key objects will be overwritten with the new key or zeros according to FCS_CKM.4.**

221 ***Application Note*** *23***:** The TOE allows the creation and deletion of key objects during operational use, even if a newly created key object uses memory areas which belonged to another key object before the TOE ensures that the contents of the old key object are not more accessible by using the new key object.

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
FDP_ETC.1.1 The TSF shall enforce the Access Control Smart Meter SFP[60] 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.

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 SFP[61] 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[62]*.*

[55] [assignment: *action to be taken*]
[56] [assignment: *other action to be taken, or none*]
[57] [selection: *allocation of the resource to, de-allocation of the resource from*]
[58] [assignment: *list of objects*]
[59] [assignment: *other data objects or none*]
[60] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[61] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[62] [assignment: *additional importation control rules*]

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 SFP[63] to transmit, receive[64] user data in a manner protected from unauthorized disclosure.

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 SFP[65] to transmit, receive[66] user data in a manner protected from modification, deletion, insertion, replay[67] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, replay[68] has occurred.

11.4 Class FIA Identification and Authentication

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[69]:

- for device (Gateway): authentication state gained via PIN (PACE-PIN respective GW-PIN used within the PACE protocol),
- for human user (Gateway Administrator): authentication state gained via asymmetric authentication key (used within the external authentication).

222 ***Application Note 24:*** **Authentication of the Gateway is performed via the PACE protocol between the Gateway and the TOE; refer to the SFR FCS_CKM.1/PACE. Authentication of the Gateway Administrator is performed via a key-based external authentication of the Gateway Administrator against the TOE, refer to the SFR FCS_COP.1/AUTH.**

[63] [selection: *transmit, receive*]
[64] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[65] [selection: *transmit, receive*]
[66] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[67] [selection: *modification, deletion, insertion, replay*]
[68] [selection: *modification, deletion, insertion, replay*]
[69] [assignment: *authentication mechanism*]

FIA_SOS.1 Verification of secrets

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

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets **provided by the Gateway for the PACE-PIN respective GW-PIN** meet *minimum length of 10 and maximum length of 64 digits*[70].

223 ***Application Note 25:*** Mutual authentication of the Gateway and the GW is performed via the PACE protocol between the Gateway and the TOE, refer to the SFR FCS_CKM.1/PACE. For the PACE-PIN (respective GW-PIN). The minimum length for the PACE-PIN as defined in FIA_SOS.1.1.

FIA_UAU.1/GW Timing of authentication (for Gateway)

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

FIA_UAU.1.1/ GW The TSF shall allow[71]

- establishing a communication channel between the TOE and the external world,
- Reading the ATR/ATS,
- Reading of data fields containing technical information,
- *none*[72]

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

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

224 ***Application Note** 26:* **Authentication of the Gateway is performed via the PACE protocol between the Gateway and the TOE, refer to the SFR FCS_CKM.1/PACE.**

225 ***Application Note** 27:* **Please note that the requirement in FIA_UAU.1/GW defines that the user (here: the Gateway) 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. The Access Control Smart Meter SFP (see chapter 11.3) 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 Gateway is required by the TOE.**

FIA_UAU.1/GWA Timing of authentication (for Gateway Administrator)

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

FIA_UAU.1.1/ GWA The TSF shall allow[73]:

- establishing a communication channel between the TOE and the external world,
- Reading the ATR/ATS,
- Reading of data fields containing technical information,
- Carrying out the PACE protocol according to [TR-03110-2], [TR-03109-3], [TR-03109-2] (by means of command GENERAL

[70] [assignment: *a defined quality metric*]

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

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

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

AUTHENTICATE),
- *none*[74]

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

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

226 ***Application Note** 28:* **Authentication of the Gateway Administrator is performed via a key-based external authentication of the Gateway Administrator against the TOE, refer to the SFR FCS_COP.1/AUTH.**

227 ***Application Note** 29:* **Please note that the requirement in FIA_UAU.1/GWA defines that the Gateway is successfully authenticated and that the user (here: the Gateway Administrator) has to be successfully authenticated before allowing administrative tasks as related e.g. to key management or update of certificates. Refer in addition to the SFR FMT_SMF.1. The Access Control Smart Meter SFP (see chapter 11.3) 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 Gateway Administrator is required by the TOE.**

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

- PACE authentication mechanism,
- key-based external authentication mechanism [75].

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

- authentication via the PACE protocol,
- secure messaging in encrypt-then-authenticate mode using PACE session keys,
- key-based external authentication[76]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules[77]:

- PACE/PIN based authentication shall be used for authenticating a device (Gateway) and secure messaging in encrypt-then-authenticate mode using PACE session keys shall be used to authenticate its commands if required by the Access Control Smart Meter SFP,
- key-based authentication shall be used for authenticating a human user (Gateway Administrator).

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

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

[75] [assignment: *identified authentication mechanism(s)*]

[76] [assignment: *list of multiple authentication mechanisms*]

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

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow[78]:

- Establishing a communication channel between the TOE and the external world,
- Reading the ATR/ATS,
- Reading of data fields containing technical information,
- Carrying out the PACE protocol according to [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3], [TR-03109-2] (by means of command GENERAL AUTHENTICATE),
- *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.

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[79]:

- authentication state for the Gateway,
- authentication state for the Gateway Administrator.

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 “not authenticated”[80].

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[81]:

- for device (Gateway): the authentication state is changed to “authenticated Gateway” when the device has successfully authenticated himself by the PACE protocol,
- for human user (Gateway Administrator): the authentication state is changed to “authenticated Gateway Administrator” when the user has successfully authenticated himself by the key-based authentication mechanism.

11.5 Class FMT Security Management

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. Embedded software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks[82].

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

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

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

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

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

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 Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated. Embedded software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks[83].

228 ***Application Note** 30:* The SFRs FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF Data to prevent misuse of test features of the TOE over the life cycle phases. The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

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

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

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies

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

- Management of key objects by means of CREATE KEY, DELETE KEY, ACTIVATE KEY, DEACTIVATE KEY, GENERATE ASYMMETRIC KEY PAIR, PSO VERIFY CERTIFICATE,
- Management of DFs and EFs by means of the commands CREATE DF/EF, ACTIVATE DF/EF, DEACTIVATE DF/EF, DELETE DF/EF, TERMINATE DF/EF,
- Management of PIN objects by means of command CHANGE REFERENCE DATA,
- TOE Lifecycle management by means of command TERMINATE CARD USAGE,
- Update of keys by means of commands GENERATE ASYMMETRIC KEY PAIR, PSO VERIFY CERTIFICATE,
- Update of certificates by means of command UPDATE BINARY,
- Update of symmetric keys (GW-keys) by means of command UPDATE BINARY,
- *none* [84].

229 ***Application Note*** *31*: A detailed description of the commands that have to be implemented in the TOE is given in [TR-03109-2].

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

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

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

- user,
- authenticated Gateway
- authenticated Gateway Administrator
- *none* [85].

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

11.6 Class FPT Protection of the Security Functions

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* [86] in excess of *non-useful information* [87] enabling access to PIN, session keys, shared secret value Z_{AB}, ephemeral keys[88]*none*[89]and private asymmetric keys of the user, symmetric keys of the user (GW-keys)[90]*none*[91]

FPT_EMS.1.2 The TSF shall ensure any users[92] are unable to use the following interface circuit interface[93] to gain access to PIN, session keys, shared secret value Z_{AB}, ephemeral keys[94]*none*[95] and *private asymmetric keys of the user, symmetric keys of* the user (GW-keys)[96] *none*[97]

230 ***Application Note** 32*: 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.

[85] [assignment: *additional authorized identified roles, or none*]
[86] [assignment: *types of emissions*]
[87] [assignment: *specified limits*]
[88] [assignment: *list of types of TSF data*]
[89] [assignment: *list of types of (further) TSF data*]
[90] [assignment: *list of types of user data*]
[91] [assignment: *list of types of (further) user data*]
[92] [assignment: *type of users*]
[93] [assignment: *type of connection*]
[94] [assignment: *list of types of TSF data*]
[95] [assignment: *list of types of (further) TSF data*]
[96] [assignment: *list of types of user data*]
[97] [assignment: *list of types of (further) user data*]

FPT_FLS.1 Failure with preservation of secure state

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

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

- power loss,
- exposure to operating conditions where therefore a malfunction could occur,
- detection of physical manipulation or physical probing,
- integrity errors according to FDP_SDI.2,
- insufficient entropy during random number generation,
- failure detected by the TSF according to FPT_TST.1,
- errors during processing cryptographic operations,
- errors during evaluation of access control rules, and
- *none* [98].

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[99] to to the all TOE components implementing the TSF[100] by responding automatically such that the SFRs are always enforced.

231 ***Application Note*** *33*: 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.

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[101] to demonstrate the correct operation of the TSF[102].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data[103].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of TSF[104].

11.7 Class FTP Trusted Path/Channels

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

[99] [assignment: *physical tampering scenarios*]

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

[101] [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*]]

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

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

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

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[105] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall **enforce** communication via the trusted channel for any data exchange between the TOE and the Gateway except reading out the data fields with technical information[106].

11.8 Security Assurance Requirements for the TOE

232 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).

The following table lists the assurance components which are applicable

ASSURANCE CLASS	ASSURANCE COMPONENTS
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures These SARs ensure proper installation and configuration: the TOE will be properly configured and the TSFs are configured to process as expected
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification

[105] [selection: *the TSF, another trusted IT product*]
[106] [assignment: *list of functions for which a trusted channel is required*]

	ADV_IMP.1 Implementation representation of the TSF ADV_TDS.3 Basic modular design
ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample. The purpose of these SARs is to ensure whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis EAL4 requires for the vulnerability assessment the assurance component AVA_VAN.3. Its aim is to determine whether the TOE, in its intended environment, has vulnerabilities exploitable by attackers with attack potential of enhanced-basic. In order to provide the necessary level of protection, EAL4 is augmented with the component AVA_VAN.5, which requires that the TOE is resistant against attackers processing high attack potential.

Table 8: Assurance Requirements - EAL 4 extended with AVA_VAN.5

Refinement:

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

234 In addition, for the evaluation and assessment of the TOE's random number generation functionality for the random number generator classes DRG.3 and PTG.2 the scheme documents [AIS31/20] or an evaluation approach agreed under the umbrella of the SOG-IS MRA shall be applied.

11.9 Security Requirements Rationale

11.9.1 Security Functional Requirements Rationale

235 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				

	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_COP.1/VER-ECDSA											x				
FCS_COP.1/AUTH			x	x											
FCS_COP.1/IMP				x	x						x				
FCS_COP.1/PACE-ENC		x				x									x
FCS_COP.1/PACE-MAC	x					x									
FCS_RNG.1												x	x	x	x
FDP_ACC.2		x		x											
FDP_ACF.1		x		x											
FDP_SDI.2	x										x	x	x		x
FDP_RIP.1					x						x	x	x	x	x
FDP_ETC.1					x										
FDP_ITC.1					x										
FDP_UCT.1		x				x									
FDP_UIT.1	x					x									
FIA_ATD.1				x											
FIA_SOS.1			x												
FIA_UAU.1/GW				x											
FIA_UAU.1/GWA				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 9: Coverage of Security Objectives for the TOE by SFR

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

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

O.Integrity

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

O.Confidentiality

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

O.Authentication

239 The security objective **O.Authentication** is addressed by the SFRs **FIA_UAU.4** and **FIA_UAU.5**. Furthermore, in view of the cryptographic functionality of the different authentication mechanisms: For the PACE authentication between the TOE and the Gateway the SFRs **FCS_CKM.1/PACE** and **FIA_SOS.1** are of relevance, for the user authentication of the Gateway Administrator the SFR **FCS_COP.1/AUTH** which realises the external authentication mechanism is involved.

O.AccessControl

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

O.KeyManagement

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

O.TrustedChannel

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

O.Leakage

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

O.PhysicalTampering

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

O.AbuseFunctionality

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

O.Malfunction

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

O.Sign

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

O.KeyAgreementDH

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

O.KeyAgreementEG

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

O.Random

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

O.PACE

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

11.9.3 SFR Dependency Rationale

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

SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
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 [PP-0077] , chapter 6.9.1.4] for missing dependencies
FCS_CKM.1/ECKA-DH	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.4 Please refer to [PP-0077], chapter 6.9.1.4] for missing dependencies

SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
FCS_CKM.1/ECKA-EG	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.4 Please refer to [PP-0077], chapter 6.9.1.4] for missing dependencies
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
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
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
FCS_COP.1/VER-ECDSA	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 FCS_CKM.4
FCS_COP.1/AUTH	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 FCS_CKM.4
FCS_COP.1/IMP	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 FCS_CKM.4
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
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
FCS_RNG.1	–	–
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 Please refer to [PP-0077], chapter 6.9.1.4] for missing dependencies
FDP_SDI.2	–	–
FDP_RIP.1	–	–
FDP_ETC.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.2 Please refer to [PP-0077], chapter 6.9.1.4] for missing dependencies
FDP_UCT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ICT.1 or FTP_TRP.1]	FDP_ACC.2 FTP_ICT.1
FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ICT.1 or FTP_TRP.1]	FDP_ACC.2 FTP_ICT.1

SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
FIA_ATD.1	–	–
FIA_SOS.1	–	–
FIA_UAU.1/GW	FIA_UID.1	FIA_UID.1
FIA_UAU.1/GWA	FIA_UID.1	FIA_UID.1
FIA_UAU.4	–	–
FIA_UAU.5	–	–
FIA_UID.1	–	–
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
FMT_SMF.1	–	–
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_EMS.1	–	–
FPT_FLS.1	–	–
FPT_PHP.3	–	–
FPT_TST.1	–	–
FTP_ITC.1	–	–

Table 10: Dependencies between the SFRs

253 The demonstration that all of the SFR dependencies are fulfilled is presented in sec. 6.9.1.3 of [PP-0077].

254 The justification for missing dependencies presented in sec. 6.9.1.4 of [PP-0077].

255 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-fullfillment is justified

11.9.4 Security Assurance Requirements Rationale

11.9.4.1. Reasoning for Choice of Assurance Level

256 The decision on the assurance level has been mainly driven by the assumed attack potential.

257 As outlined in the Gateway Protection Profile [PP-0073] it is assumed that – at least from the WAN side – a high attack potential is posed against the security functions of the TOE. This leads to the use of AVA_VAN.5 (Resistance against high attack potential).

258 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.

11.9.4.2. Dependencies of Assurance Components

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

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

11.9.5 Security Requirements – Internal Consistency

261 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.

262 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 analysed and non-satisfied dependencies are appropriately explained.

263 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 behaviour of these 'shared' items.

264 The assurance package EAL4 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.

265 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 [PP-0077]. 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.

12. TOE SUMMARY SPECIFICATION

266 The TOE provides the following TOE security functionality, which comply to the [PP-0077]:

- 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
- Access Control
- Cryptographic Functions
- Protection of data relevant for the Gateway

267 These Security Functions are implemented by the realisation of the Security Functional requirements, according to sec. 11.The details of the implementation of this TOE security functionality by the SFRs is provided in the following sections.

12.1 SF_SIG_GEN - Digital Signature Generation

268 The Smartmeter Gateway is utilising the Security Module as a cryptographic service provider. The digital signatures created by the Security Module are used for TLS establishment and authenticity of data. The Security Module creates signatures for the Gateway implementing the SFR, FCS_COP.1/SIG-ECDSA.

269 This Security Function relies on SF_CRY to implement the signature generation, signature keys destruction and the generation of the random numbers

12.2 SF_SIG_VER - Digital Signature Verification

270 The TOE functionality of Signature Verification via FCS_COP.1/VER-ECDSA is essential for authenticity purposes. The signature verification is used for certificate approval, which provides a security anchor for included certificate data, signed public keys being imported into the TOE via FCS_COP.1/IMP and supports authentication of external devices via FCS_COP.1/AUTH.

271 This Security Function relies on SF_CRY to implement the signature verification.

12.3 SF_KA_TLS - Key Agreement for TLS

272 The TOE implements the ECKA-DH protocol via FCS_CKM.1/ECKA-DH to support a TLS handshake, during the establishment of a secure network connection by the Gateway.

12.4 SF_KA_CDE - Key Agreement for Content Data Encryption

273 The TOE implements the ECKA-EG protocol (FCS_CKM.1/ECKA-EG) to support a key derivation for a symmetric algorithm for data encryption.

12.5 SF_KEY_GEN - Key Pair Generation

274 The TOE provides a service for signature key pair generation (FCS_CKM.1/ECC).

275 This Security Function relies on SF_CRY to implement the key pair generation.

12.6 SF_RND_GEN - Random Number Generation

276 The TOE provides a service for challenge generation via the random number generator (FCS_RNG.1) for authentication protocols and for other use cases of the Gateway.

277 This Security Function relies on SF_CRY to implement the random number generator.

12.7 SF_PACE_AUTH - Component Authentication via PACE

278 The TOE implements the PACE protocol with negotiation of session keys (FCS_CKM.1/PACE).

12.8 SF_SM - Secure Messaging

279 The TOE implements a trusted channel providing confidentiality and integrity of transferred data according to the FTP_ITC.1 requirement. The trusted channel is using AES cipher for encryption in AES-CBC mode and message authentication code generation in AES-CMAC mode provided by SF_CRY.

12.9 SF_AC - Access Control

280 This function checks that for each operation initiated by a user, the security attributes for user authorization (FMT_SMR.1) and data communication required are satisfied. The function covers the management, export and import of stored keys and data as defined in FMT_SMF.1.

281 This function operates in accordance to the access policies according to FDP_ACC.2, FDP_ACF.1 and considers the authentication preconditions and user roles defined in FIA_ATD.1 and FMT_SMR.1, respectively.

12.10 SF_CRY - Cryptographic Support

282 This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation and operations on data such as encrypt and sign:

- Secure generation of asymmetric Key Pair.
- Digital Signature generation and verification.
- High quality Random Number Generator.
- AES cipher for encryption in CBC mode
- AES message authentication in AES-CMAC mode
- Secure destruction of cryptographic key secret or private material.

283 This TSF enforces protection of Key material during cryptographic functions processing and Key Generation, against state-of-the-art attacks, including IC power consumption analysis.

12.11 SF_PRO - Protection of data relevant for the Gateway

284 This Security Function is responsible for protection of the TSF data, user data, and TSF functionality. The SF Protection function is composed of software implementations of test and security functions including:

- Performing self-tests of the TOE
- Initializing memory after reset
- Initializing memory of de-allocated data
- Preserving the TOE lifecycle state integrity
- Protecting the integrity of all stored cryptographic keys before use and preventing use of corrupted data by stopping the operation involved and setting an error
- Preventing electromagnetic and power emissions or associated information like timing behaviour, in order to preserve the confidentiality of stored keys or residual key material information
- Preserving secure state after sensitive processing failure or potential physical tampering or intrusion detection

12.12 Statement of Compatibility

285 This is the statement of compatibility between this Composite Security Target and the Security Target of the underlying javacard platform STSAFE-J, [STSAFE-ST].

12.12.1 Relevance of javacard Platform-ST STSAFE-J TSF

286 Relation of TOE security Function of the Composite-TOE and the javacard Platform-ST STSAFE-J:

Javacard Platform STSAFE-J SF Composite TOE SF	SF.CryptoKey	SF.CryptoOp	SF.ObjectDeletion	SF.SecureManagement SF.Transaction SF.SmartCardPlatform SF.Firewall **apply indirectly to all Composite-TOE security functions**
SF_SIG_GEN	X	X		X
SF_SIG_VER	X	X		X
SF_KA_TLS	X	X	X	X
SF_KA_CDE	X	X	X	X
SF_KEY_GEN	X			X
SF_RND_GEN		X		X
SF_PACE_AUTH	X	X	X	X
SF_SM		X		X
SF_AC				X
SF_CRY	X	X	X	X
SF_PRO				X

287 The SF **SF.PIN** is considered not relevant to the composite TOE

288 The SF **SF.Firewall** is considered partially relevant for the composite TOE.

12.12.2 Security Requirements

289 The following section verifies that there is no contradiction between the SFRs of the Composite-TOE and the platform STSAFE-J. The table below shows the mapping between the javacard platform STSAFE-J SFRs and the Composite ST SFRs. Only the relevant platform STSAFE-J SFRs are listed

Relation of Security Requirements of the Composite-TOE to javacard Platform-ST STSAFE-J:

SFR-components of the Composite-TOE	**Platform STSAFE-J SFRs**
FCS_CKM.1/ECC Cryptographic key generation – ECC-Key pair	fcs_ckm.1/EC - Cryptographic key generation fcs_ckm.2/EC - Cryptographic key distribution fcs_ckm.3/EC - Cryptographic key access
FCS_CKM.1/ECKA-DH Cryptographic key generation – DH Key agreement	fcs_cop.1/DHKeyExchange - Cryptographic operation
FCS_CKM.1/ECKA-EG Cryptographic key generation – ElGamal Key agreement	fcs_cop.1/GMap - Cryptographic operation
FCS_CKM.1/PACE Cryptographic key generation – PACE	fcs_rng.1/DRBG - Generation of random numbers fcs_ckm.2/AES - Cryptographic key distribution

SFR-components of the Composite-TOE	Platform STSAFE-J SFRs
	fcs_ckm.3/AES - Cryptographic key access fcs_cop.1/AES_Cipher - Cryptographic operation fcs_cop.1/AES_CMAC - Cryptographic operation fcs_cop.1/DHKeyExchange - Cryptographic operation fcs_cop.1/GMap - Cryptographic operation
FCS_CKM.4 Cryptographic key destruction	fcs_ckm.4 Cryptographic key destruction
FCS_COP.1/SIG-ECDSA Cryptographic operation – ECDSA Signature generation	fcs_cop.1/EC Signature - Cryptographic operation
FCS_COP.1/VER-ECDSA Cryptographic operation – Signature verification	fcs_cop.1/EC Signature - Cryptographic operation
FCS_COP.1/AUTH Cryptographic operation – External Authentication	fcs_cop.1/EC Signature - Cryptographic operation
FCS_COP.1/IMP Cryptographic operation – Import of Public Keys	fcs_cop.1/EC Signature - Cryptographic operation fcs_ckm.2/EC - Cryptographic key distribution fcs_ckm.3/EC - Cryptographic key access
FCS_COP.1/PACE-ENC Cryptographic operation – AES in CBC for secure messaging	fcs_cop.1/AES_Cipher - Cryptographic operation
FCS_COP.1/PACE-MAC Cryptographic operation – AES-CMAC for secure messaging	fcs_cop.1/AES_CMAC - Cryptographic operation
FCS_RNG.1 Quality metric for random numbers	fcs_rng.1/DRBG - Generation of random numbers
FDP_ACC.2 Complete access control – Access Control Policy	-
FDP_ACF.1 Security attribute based access control – Access Control Functions	-
FDP_SDI.2 Stored data integrity monitoring and action	fdp_sdi.2 - Stored data integrity monitoring and action
FDP_RIP.1 Subset residual information protection	fdp_rip.1/OBJECTS - Subset residual information protection fdp_rip.1/ABORT - Subset residual information protection fdp_rip.1/APDU - Subset residual information protection fdp_rip.1/bArray - Subset residual information protection fdp_rip.1/KEYS - Subset residual information protection fdp_rip.1/TRANSIENT - Subset residual information protection fdp_rip.1/ODEL
FDP_ETC.1 Export from the TOE	-
FDP_ITC.1 Import from outside of the TOE	-
FDP_UCT.1 Basic data exchange confidentiality	fcs_cop.1/AES_Cipher - Cryptographic operation
FDP_UIT.1 Inter-TSF user data integrity transfer protection	fcs_cop.1/AES_CMAC - Cryptographic operation
FIA_ATD.1 User attribute definition	-
FIA_SOS.1 Verification of secrets	-
FIA_UAU.1/GW Timing of authentication	fcs_rng.1/DRBG - Generation of random numbers

SFR-components of the Composite-TOE	Platform STSAFE-J SFRs
(for Gateway)	fcs_ckm.2/AES - Cryptographic key distribution fcs_ckm.3/AES - Cryptographic key access fcs_cop.1/AES_Cipher - Cryptographic operation fcs_cop.1/AES_CMAC - Cryptographic operation fcs_cop.1/DHKeyExchange - Cryptographic operation fcs_cop.1/GMap - Cryptographic operation
FIA_UAU.1/GWA Timing of authentication (for Gateway Administrator)	fcs_cop.1/EC Signature - Cryptographic operation
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	-
FMT_LIM.1 Limited capabilities	fmt_lim.1/Test - Limited capabilities
FMT_LIM.2 Limited availability	fmt_lim.2/Test - Limited availability
FMT_SMF.1 Specification of Management Functions	-
FMT_SMR.1 Security roles	-
FPT_EMS.1 TOE Emanation	fpt_emsec.1 TOE Emanation
FPT_FLS.1 Failure with preservation of secure state	fpt_fls.1/Operate - Failure with preservation of secure state
FPT_PHP.3 Resistance to physical attack	fpt_php.3 - Resistance to physical attack
FPT_TST.1 TSF testing	fpt_tst.1 TSF testing
FTP_ITC.1 Inter-TSF trusted channel	fcs_rng.1/DRBG - Generation of random numbers fcs_ckm.2/AES - Cryptographic key distribution fcs_ckm.3/AES - Cryptographic key access fcs_cop.1/AES_Cipher - Cryptographic operation fcs_cop.1/AES_CMAC - Cryptographic operation fcs_cop.1/DHKeyExchange - Cryptographic operation fcs_cop.1/GMap - Cryptographic operation

Security Assurance Requirements

290 The chosen level of assurance of the javacard platform-ST STSAFE-J is EAL5 augmented by ALC_DVS.2 and AVA_VAN.5.

291 The Assurance Requirement levels of Composite-TOE and the underlying platform are compliant to each other.

12.12.3 Security Objectives

292 The following section verifies that there is no contradiction between the Security Objectives of the Composite-TOE and the javacard platform-ST STSAFE-J.

Relation of the Security Objectives of the Composite-ST and the javacard platform-ST STSAFE-J:

Javacard platform-ST STSAFE-J Security Objectives Composite-ST Security Objectives	O.OPERATE	O.REALLOCATION	O.SCP.RECOVERY	O.SCP.IC	O.SCP.SUPPORT	O.CIPHER	O.KEY-MNGT	O.TRANSACTION	O.OBJ-DELETION	O.SIDE_CHANNEL	O.GLOBAL_ARRAY_CONFID	O.PIN-MNGT
O.Integrity			x					x				x
O.Confidentiality				x			x					x
O.Authentication						x	x					x
O.AccessControl						x	x					
O.KeyManagement		x					x		x		x	
O.TrustedChannel						x	x					
O.Leakage		x		x					x	x		
O.PhysicalTampering				x	x							
O.AbuseFunctionality				x	x							
O.Malfuntion	x											
O.Sign						x	x					
O.KeyAgreementDH,						x	x					
O.KeyAgreementEG						x	x					
O.Random						x					x	
O.PACE						x	x					

Security Objectives for the javacard platform STSAFE-J not relevant for the Composite-TOE:

293 O.ALARM, O.SID, O.ROLES, O.GLOBAL_ARRAYS_INTEG, O.NATIVE, O.LIFE_CYCLE, O.RESOURCES , O.FIREWALL

12.12.4 Compatibility: TOE Security Environment

12.12.4.1. Assumptions

294 There are no contradictions between the assumptions of the composite TOE and the assumptions of the underlying javacard platform-ST STSAFE-J.

12.12.4.2. Threats

295 There are no contradictions between the threats of the composite TOE and the threats of the underlying javacard platform-ST STSAFE-J.

12.12.4.3. Organizational Security Policies

296 There are no contradictions between the organizational security policies of the composite TOE and the organizational security policies of the underlying javacard platform-ST STSAFE-J.

12.12.5 Conclusion

297 There are no contradictions between the ST of the composite TOE and the ST of the underlying javacard platform-ST STSAFE-J.

13. ANNEX A – CRYPTO DISCLAIMER

298 The following cryptographic algorithms are used by STSAFE-J100-BS to enforce its security policy:

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1.	Authenticity	ECDSA-signature generation without hashing Id-ecdsa-plain-signatures	[ANSI_X9.62](ECDSA) [FIPS_180-2](SHA) [TR-03111]	Key sizes of used elliptic curve brainpool P{256,384,512}r1 [RFC5639] NIST P{256,384} [FIPS186]	[TR-03109-2]	N.A.
2.		ECDSA-signature verification without hashing Id-ecdsa-plain-signatures ECDSA-signature verification with hash parameter Id-ecdsa-plain-SHA256/SHA384/SHA512	[ANSI_X9.62](ECDSA) [FIPS_180-2](SHA) [TR-03111]	Key sizes corresponding to the used elliptic curve brainpool P{256,384,512}r1 [RFC5639] NIST P{256,384} [FIPS186]	[TR-03109-2]	N.A.
3.	Authentication	ECDSA-signature verification with hash parameter Id-ecdsa-plain-SHA256/SHA384/SHA512	[TR-03109-3], [TR-03109-2] [TR-03116-3]	Key sizes corresponding to the used elliptic curve brainpool P{256,384,512}r1 [RFC5639] NIST P{256,384} [FIPS186]	[TR-03109-2]	N.A.
		ECDSA-signature generation without hashing Id-ecdsa-plain-signatures				N.A.
4.	Authenticated Key Agreement	PACE protocol PACE-ECDH-GM-AES-CBC-CMAC-128/192/256	[TR-03110-2], [TR-03109-3], [TR-03109-2]	PWD size: minimum 10 char. maximum 64 char. Derived AES key size: 128/192/256 bits	[TR-03109-2]	N.A.
5.	Key Agreement	ECKA-DH	[TR-03111]	Key sizes corresponding to the used elliptic curve brainpool P{256,384,512}r1 [RFC5639] NIST P{256,384} [FIPS186]	[TR-03109-2]	N.A.
		ECKA-EG	[TR-03111]	Key sizes corresponding to the used elliptic curve brainpool P{256,384,512}r1 [RFC5639] NIST P{256,384} [FIPS186]	[TR-03109-2]	N.A.
6.	Confidentiality	AES in CBC mode	[FIPS197] (AES), [ISO 10116] (CBC)	Key sizes: 128, 192 and 256 bits	[TR-03109-2]	N.A.
7.	Integrity	AES in CMAC mode	[FIPS197] (AES), [RFC4493] (CMAC)	Key sizes: 128, 192 and 256 bits	[TR-03109-2]	N.A.
8.	Trusted Channel	Secure messaging in ENC_MAC mode and key established with PACE protocol	[ISO7816] [TR-03110-3]		[TR-03109-2]	N.A.
9.	Cryptographic Primitive	True Random Generator (TRNG) class PTG.2 Deterministic Random Generator (DRBG) class RNG DRG.3	[AIS31/20]	n.a.	[TR-03109-2]	N.A.

14. QUALITY REQUIREMENTS

14.1 Revision History

Version	Subject
Rev A	Final Puclic Version – April-2018

Table 11 - Revision History

15. ENVIRONMENTAL/ECOLOGICAL REQUIREMENTS

STMicroelectronics recommends viewing documents on the screen rather than printing to limit paper consumption.