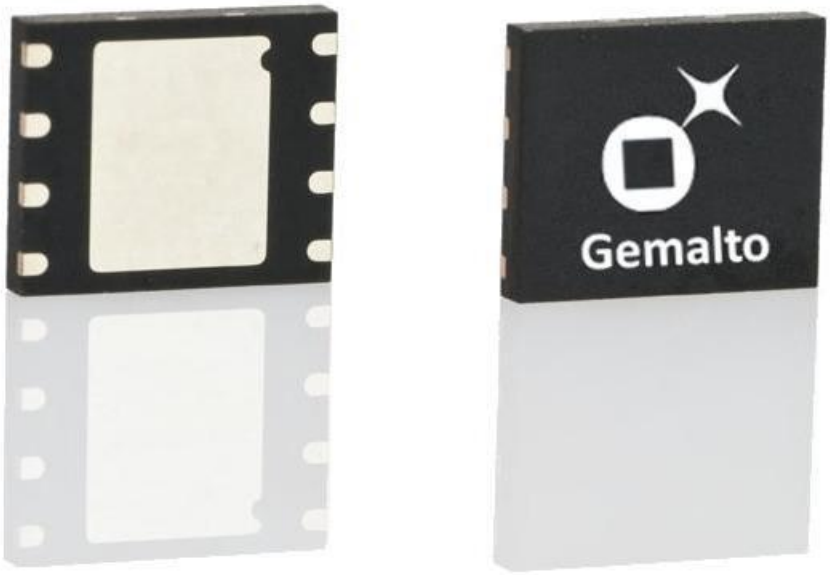
Security Target of Security Module for Smart Meter Gateway (PUBLIC version) BSI-DSZ-CC-1003-2017 TOE NAME: Smart Meter Gateway SM applet on MultiApp V4



Document History

Rel	Date	Author	Modification
2.1p	3 August 2018	Gemalto	ST PUBLIC version is extracted from evaluated Security Target (V2.1)

CONTENT

FIGURES

TABLES

1. ST INTRODUCTION

1.1 SECURITY TARGET REFERENCE

Title :	Security Target of Security Module for Smart Meter Gateway
Version :	2.1p (Public version extracted from evaluated version)
ST Reference :	D1359877
CC Version:	3.1 Revision 4
Assurance Level:	EAL 4 Augmented with AVA_VAN.5
General Status:	EVALUATED
Origin :	Gemalto
Author :	Francois GUERIN
ITSEF:	TUV-IT
Certification Body :	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Certification ID	BSI-DSZ-CC-1003-2018

1.2 TOE REFERENCE

Product Name :	**Smart Meter Gateway Security Module V1.1**
TOE Reference*:	**M1010878A**
TOE Name :	Smart Meter Gateway Security Module Application on MultiApp V4
TOE Version :	Revision A
Applet Reference*:	**T1033684A (included link with platform)**
Platform Reference*:	**T1027933A (included link with IC)**
Security Controllers:	**M7892 G12 (see [CR-PF] and [CR-IC-M7892])**
TOE documentation:	Guidance [GUIDE_SMGW]

* note: PDM reference system includes version in letter revision (A)
The Product and TOE identification details are provided in §TOE description.

1.3 ST OVERVIEW

The Target of Evaluation (TOE) addressed by the current Security Target is a product comprising hardware and software used by the Gateway of a Smart Metering System according to the Protection Profile [PP0077-SecMod] for the Security Module of a Smart Meter Gateway.

The TOE is Smart Meter Gateway Security Module Application on platform named MultiApp V4 also named further in document as “Smart Meter Gateway SM applet on platform”.

As depicted on figure 4, Platform includes the hardware, its dedicated software and the operating system. Evaluation is performed using a composite approach defined in [JIL_CPE].

The IC is evaluated in conformance with [PP-IC-0084] according to [ST-IC] and certified in [CR-IC].
The Platform is evaluated in conformance with [PP-JCS-Open] according to [ST-PLTF] and certified in [CR-PF] and reusing results from IC evaluation in [CR-IC-M7892].

The Smart Meter Gateway SM applet on platform is evaluated in conformance with [PP0077-SecMod] according to current document and reusing results from platform evaluation.

The main objectives of this ST are:

- To introduce TOE and the Smart Meter Gateway SM applet on platform,
- To define the scope of the TOE and its security features,
- To describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.

- To describe the security objectives of the TOE and its environment.
- To specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functions.

1.4 REFERENCES

1.4.1 External References

[AIS20/31]	Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20/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)
[AIS31]	Anwendungshinweise und Interpretationen zum Schema (AIS): AIS 31 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, BSI, 3.0 Stand 15.05.2013
[AIS36]	Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Kompositionsevaluierung,Version 4 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[ANSI X9.62]	ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005.
[ANSI X9.63]	ANSI X9.63 Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Key Transport Schemes, X9.63-2011
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2012-09-001, version 3.1 rev 4, September 2012
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2012-09-002, version 3.1 rev 4, September 2012
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2012-09-003, version 3.1 rev 4, September 2012
[CEM]	Common Methodology for Information Technology Security Evaluation MethodologyCCMB-2009-07-004, version 3.1 rev 4, September 2012
[CEN]	SMART METERS CO-ORDINATION GROUP (SM-CG) Item 5. M/441 first phase deliverable Communication – Annex: Glossary (SMCG/Sec0022/DC)
[CR-IC]	Certification Report, see [CR-IC-M7892]
[CR-IC-M7892]	Certification Report, Infineon smart card IC (Security Controller) M7892 BSI-DSZ-CC-0891-V2-2016
[CR-PF]	Rapport de certification ANSSI-CC-2017/54 Plateforme JavaCard MultiApp V4.0 - PACE en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12)
[FIPS180-4]	Federal Information Processing Standards Publication 180-4, Secure Hash Standard (SHS), March 2012 http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
[FIPS186]	Federal Information Processing Standards Publication FIPS PUB 186-3, Digital Signature Standard (DSS), 2009-06
[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
[FIPS46-3]	*Federal Information Processing Standards Publication FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES),* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, Reaffirmed 1999 October 25
[GP221]	Global Platform Card Specification v 2.2.1 – January 2011
[ISO15946-1]	ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002

[ISO15946-2]	ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures, 2002
[ISO15946-3]	ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment, 2002
[ISO7816]	*ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange*, FDIS2004
[ISO 7816-4]	ISO/IEC 7816-4: Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange, ISO/IEC, IS 2014
[ISO 7816-8]	ISO/IEC 7816-8: Identification cards - Integrated circuit cards - Part 8: Commands for security operations, ISO/IEC, IS 2004
[ISO 7816-9]	ISO/IEC 7816-9: Identification cards - Integrated circuit cards - Part 9: Commands for card management, ISO/IEC, IS 2004
[ISO9796-2]	*ISO/IEC 9797: Information technology – Security techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms,* 2002
[ISO9797-1]	*ISO/IEC 9797: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher,* 1999
[ISO 10116]	ISO/IEC 10116 Information technology – Security techniques – Modes of operation for an n-bit block cipher, 2006
[ISO14888-3]	ISO/IEC 14888-3:2006, Information technology – Security techniques – Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms, ISO, 2006
[JIL_GSE]	Joint Interpretation Library: Guidance for smartcard evaluation Version 2.0 February 2010
[JIL_CPE]	Joint Interpretation Library: Composite product evaluation for Smart Cards and similar devices, Version 1.4 August 2015
[JIL_CDE]	Joint Interpretation Library: Collection of developer evidence Version 1.5 January 2012
[NIST 197]	NIST FIPS 197 - Advanced Encryption Standard (AES), 2001
[NIST SP800-90A]	NIST Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
[PKCS#3]	*PKCS #3: Diffie-Hellman Key-Agreement Standard,* An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[PP-IC-0084]	Security IC Platform Protection Profile with augmentation Packages– BSI-CC-PP-0084-2014
[PP0073-SMGW]	CC Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Version 1.3, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0073-2014, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-03-31
[PP0077-SecMod]	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-V2-2015, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-12
[PP-JCS-Open]	Java Card System Protection Profile – Open Configuration ANSSI-PP-2010-03M01, Version 3.0, May 2012
[PTB_A50.7]	Anforderungen an elektronische und software- gesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme, PTB-A 50.7, April 2002
[RFC 2409]	The Internet Key Exchange (IKE), RFC 2409, IETF, 1998-11
[RFC 4493]	IETF RFC 4993 J. H. Song, J. Lee, T. Iwata: The AES-CMAC Algorithm, 2006
[RFC5639]	M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03

[SP800-38A]	Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST, Special Publication 800-38A, National Institute of Standards and Technology, December 2001
[SP800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, May 2005
[ST-IC]	ST for Infineon smart card IC (Security Controller) M7892 G12 SLE78 – 1.7 as of 2016 -11-16
[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, Version 1.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-12
[TR-03109-3]	Technische Richtlinie BSI TR-03109-3 Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen - Version: 1.1 (BSI), 2014-04
[TR-03109-4]	Technische Richtlinie BSI TR-03109-4: Public Key Infrastruktur für Smart Meter Gateway, Version 1.1.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2015-05-18
[TR-03110-1]	BSI TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents - Part 1 - eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.10, 2012
[TR-03110-2]	BSI TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents - Part 2 - Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), BSI, Version 2.10, 2012
[TR-03110-3]	BSI TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents - Part 3 - Common Specifications, BSI, Version 2.11, 2013
[TR-03111-EC] [TR-03111]	Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012
[TR-03116-3]	BSI TR-03116-3 - Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3 - Intelligente Messsysteme (BSI) 26.03.2015

1.4.2 Internal References

[ST-PLTF]	MultiApp V4 JCS with PACE Security Target D1368111_EXT version 1.0 lite, D1368111_EXT V1.0, August 2017
[AGD_OPE_PLTF]	MultiApp V4 AGD_OPE document – Javacard Platform, D1390321_EXT version 1.2 Rules for applications on MultiApp certified product, D1390963_EXT version 1.1 MultiApp ID Operating System Reference Manual, D1392687A
[GUIDE_PLTF]	[AGD_OPE_PLTF] + [AGD_PRE_PLTF]
[AGD_PRE_PLTF]	AGD_PRE of MultiApp V4, D1390316 version 1.1
[AGD_OPE_SMGW]	Operational Guidance for Smart Meter Gateway Security Module Application on MultiApp V4, D1393788 + Smart Meter Gateway Security Module V1.1 - Personalization and Operational Life Cycle (SEID01) User Guide, D1413164G
[AGD_PRE_SMGW]	Preparation Guidance for Smart Meter Gateway Security Module Application on MultiApp V4, D1393787 SMGW SM V1.1-Integration and Pre-Personalization Guideline D1386918C Smart Meter Gateway Security Module V1.1 - Integration and Pre-Personalization Life Cycle (SEID02) User Guide, D1422373F
[GUIDE_SMGW]	[AGD_OPE_SMGW] + [AGD_PRE_SMGW] + [GUIDE_PLTF]
[ALC_DVS]	ALC_DVS: Sufficiency of security measures, DVS_D1393795

1.5 ACRONYMS AND GLOSSARY

See table next page

Acr.	Term	Definition
	ATR	Answer To Reset
	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
	CLS	CLS are systems containing IT-components in the Home Area Network (HAN) of the consumer that do not belong to the Smart Metering System but may use the Gateway for dedicated communication purposes.
	Consumer	End user of electricity, gas, water or heat. The consumer can also generate energy using a Distributed Energy Resource.
	DEMA	Differential Electro Magnetic 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
GWA	Gateway Administrator	Authority that installs, configures, monitors, and controls the Smart Meter Gateway.
	GW	Gateway
HAN	Home Area Network	In-house data communication network which interconnects domestic equipment and can be used for energy management purposes.
	ID	Identifier
	IT	Information Technology
	JIWG	Joint Interpretation Working Group
	KDF	Key Derivation Function
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.
LMN	Local Metrological Network	In-house data communication network which interconnects metrological equipment.
	Meter	The term Meter refers to a unit for measuring the consumption or production of a certain commodity with additional functionality. It collects consumption or production data and transmits this data to the Gateway.
	Meter Data	Meter readings that allow calculation of the quantity of a commodity, for example electricity, gas, water or heat consumed or produced over a period. Other readings and data may also be included (such as quality data, events and alarms).
	MRA	Mutual Recognition Agreement

Acr.	Term	Definition
	NIST	National Institute of Standards and Technology
	PIN	Personal Identification Number
	PKI	Public Key Infrastructure
IC	Integrated circuit	Electronic component(s) designed to perform processing and/or memory functions. The MultiApp's chip is an integrated circuit.
	Personalization	The process by which the portrait, signature and biographical data are applied to the document. [SS]
	Personalization Agent	The agent acting on the behalf of the issuing State or organization to personalize the TOE for the holder.
	Authenticity	Property that an entity is what it claims to be.
	Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
	Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [SS]
	IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
	Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the TOE Manufacturer (Phase 2) for traceability of non-personalized TOE's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair.
	Pre – personalized TOE's chip	TOE's chip equipped with pre-personalization data.
	IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
	Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification l (IC identification data).
	Security Module	A Security device utilized by the Gateway for cryptographic support–typically realized in form of a smart card or equivalent form factor.
	SAR	Security Assurance Requirement
	SecMod	Security Module
	SHA	Secure Hash Algorithm
	SIG	Content Data Signature
	SM-PKI	Smart Metering - Public Key Infrastructure (SM-PKI)
	Smart Meter Gateway (SMGW)	Device or unit responsible for collecting Meter Data, processing Meter Data, providing communication capabilities for devices in the LMN, protecting devices in the LAN (such as Controllable Local Systems) against attacks from the WAN and providing cryptographic primitives (in cooperation with a Security Module).
	TOE	Target Of Evaluation (CC part 1 [CC-1]).
	TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [CC-1]).
	TLS	Transport Layer Security
	User, external entity	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary.
	User data	Data created by and for the user that does not affect the operation of the [CC-1]).
	Wide Area Network, WAN	Extended data communication network connecting a large number of communication devices over a large geographical area.

1.6 TOE OVERVIEW

1.6.1 Introduction to Smart Metering System

The TOE as defined in this Security Target is the Security Module contained in the Gateway of a Smart Metering System.

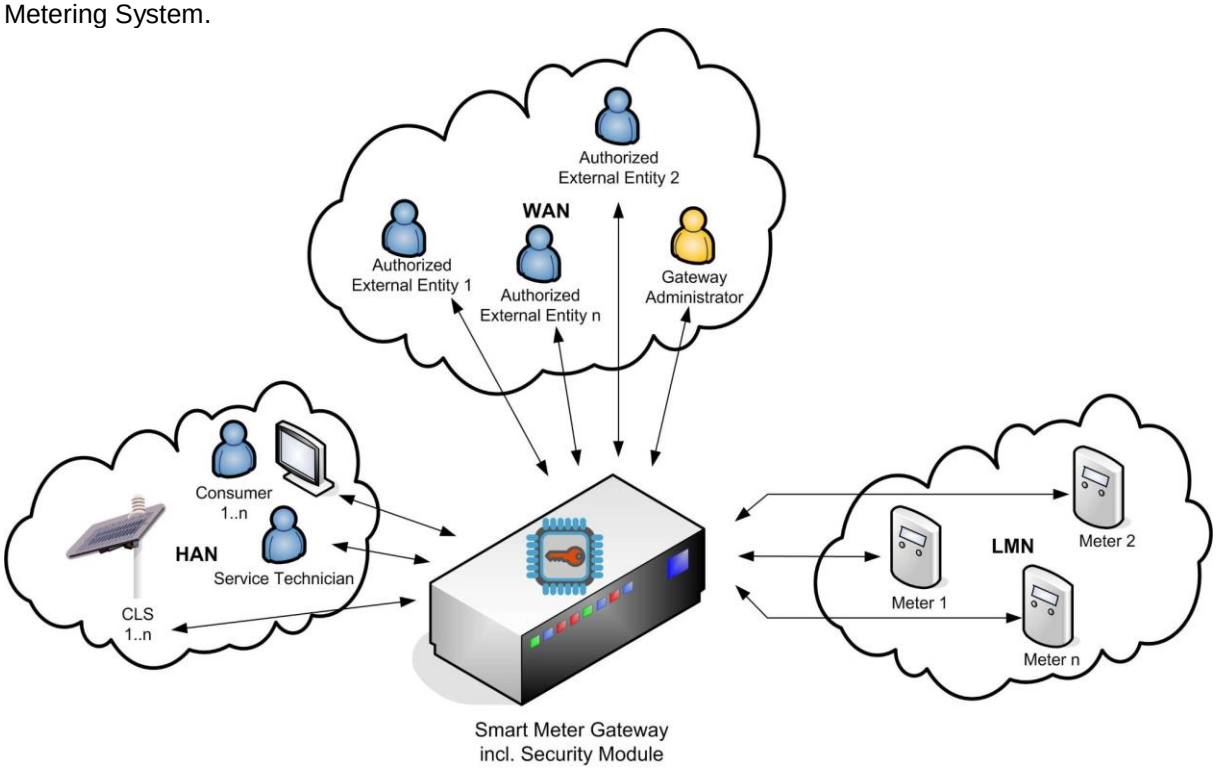


Figure 1: Smart Metering System with Gateway including security module as TOE

As can be seen in Figure 1, a Smart Metering System comprises different functional units in the context of the descriptions in this ST:

- The **Gateway** (as defined in [PP0073-SMGW]) serves as the communication component between the components in the LAN of the consumer and the outside world. It can be seen as a special kind of firewall dedicated to the Smart Metering functionality. It also collects, processes and stores the records from Meter(s) and ensures that only authorized parties have access to them or derivatives thereof. Before sending relevant information the information will be signed and encrypted using the services of the TOE. The Gateway features a mandatory user interface, enabling authorized consumers to access the data relevant to them. The Gateways will be evaluated separately according to the requirements in the corresponding Protection Profile (see [PP0073-SMGW]).

- The **Meter** itself records the consumption or production of one or more commodities (e.g. electricity, gas, water, heat) in defined intervals and submits those records to the Gateway. The Meter Data has to be signed before transfer in order to ensure their authenticity and integrity. The Meter is comparable to a classical meter and has comparable security requirements; it will be sealed as classical meters are today according to the regulations of [PTB_A50.7]. The Meter further supports the encryption of its connection to the Gateway.

- The Gateway utilizes the services of a **Security Module** as a cryptographic service provider for different cryptographic functionalities based on elliptic curve cryptography as the generation and verification of digital signatures and key agreement which is used by the Gateway in the framework of TLS, content data signature and content data encryption. The Security Module contains the cryptographic identity of the Gateway, and it serves as a reliable source for random numbers as well as a secure storage for cryptographic keys and certificates. The Security Module is addressed within this Security Target. It is embedded into the Gateway and directly communicates with the Gateway.

- **Controllable Local Systems** (CLS, as shown in Figure 1) may range from local power generation plants, controllable loads such as air condition and intelligent household appliances ("white goods") to applications in home automation. CLS may utilize the services of the Gateway for communication services.

While the Gateway is the central unit in the Smart Metering System that collects, processes and stores Meter Data and that communicates with external parties, the Security Module (TOE) supports the Gateway for specific cryptographic needs and is responsible for certain cryptographic services that are invoked by the Gateway for its operation in a Smart Metering System.

1.6.2 TOE description

The Security Module (TOE) is a service provider for the Gateway for cryptographic functionality in type of a hardware security module with appropriate software installed. It provides an external communication interface to the Gateway, so that the cryptographic service functionality provided by the TOE can be utilized by the Gateway via this interface. Moreover, the TOE serves as a secure storage for cryptographic keys and certificates and further sensitive data relevant for the Gateway.

The Target of Evaluation (TOE) addressed by the current Security Target is a Security Module used by the Gateway of a Smart Metering System according to the Protection Profile [PP0077-SecMod] for the Security Module of a Smart Meter Gateway.

1.6.2.1 Product and TOE identification

For Product and TOE identification, refer to §1.2

The Product and TOE identification and configuration are provided by executing a dedicated command described in [AGD_OPE_PLTF], §1.5).

The TOE and the product differ, as further explained in §1.7 TOE boundaries:

- The TOE is the Smart Meter Gateway SM applet on MultiApp V4
- The product based on MultiApp V4 platform may also include default optional applications loaded in Non-volatile memory prior issuance (none of them are present in current TOE configuration).

Platform identification can be obtained through ATR value: 3B FF 96 00 00 81 31 FE 43 80 31 80 65 B0 85 04 00 11 12 0F FF 82 90 00 E0.

SM applet identification is given by:

- package AID: A000000030800000000099A00,
- applet AID: A000000030800000000099A01,
- instance AID: A000000030E80704007F00070304.

Using the SELECT APDU (see [AGD_OPE_SMGW], §APDU COMMANDS):

- 00 A4 04 00 0E A0 00 00 00 30 E8 07 04 00 7F 00 07 03 04.
- Expected return from TOE is SW: 9000

SM applet configuration can be determined using following sequence of operations :

- SELECT EF File ID = EF.SecModTRInfo (01 1A) (see [AGD_OPE_SMGW], §APDU COMMANDS)
- READ RECORD Record number = 1
- Expected return from TOE is: (54522D30333130392D322076312E31FF..FF) corresponding to the string "TR-03109-2 v1.1" that identifies the TOE under evaluation.

It can also be identified using information from GET DATA with tag '9F7F'(see [AGD_OPE_PLTF], §1.5):

CPLC field	Length	Value	Meaning
IC Fabricator	2	4090h	IFX
IC Type	2	7897	SLE78CLFX400VPHM, M7892, G12
Operating System Identifier	2	1291h	Unique identifier for Vendor (Gemalto)
Operating System release date	2	6153	(2016/05/19)
Operating System release level	2	0400h	(4.0)

Table 1: Card Production Life Cycle Data

There are also complementary information obtained with GET DATA '0103' (see [AGD_OPE_PLTF], §1.5):

TAG Identity	Length	Value
Gemalto Family Name	1	B0h
Gemalto OS Name	1	85h
Mask Number	1	55h
Product Name	1	FFh
Flow ID Version	1	01h
Filter Set	1	00h
Chip Manufacturer	2	4090h
Chip Identifier	2	7897h (SLE78CLFX400VPHM)
BPU	2	7881h (SLE78CFX4000PH)
PDM Technical Product Identifier	3	033684h
PDM Customer Item Identifier	3	099675h
Feature Flag – Crypto Config	2	BFA5h Crypto supported: ECC RSA
Feature Flag – Feature Config	1	9Dh Features supported: PACE Common PACE ECC Linker for Java loading package ISM
Feature Flag – Following features		00h
Platform Certificates		40h
APPLI CERTIFICATES byte 1		00h
APPLI CERTIFICATES byte 2		00h

Table 2: Tag Identity

1.7 TOE BOUNDARIES

The Target of Evaluation (TOE) is the Secure Module for Smart Meter Gateway. It is integrated in a DFN8 form factor defined by the ETSI standard (TS 102.671 – MFF2 form factor) and delivered associated to a reel. The intended use for the TOE is restricted to this application in the infrastructure for Smart Metering Systems where Gateway that connects the LAN of the consumer and the outside world.

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

TOE and TOE physical boundaries are defined on the following figure. As presented in figure 4, TOE includes:

- The underlying Integrated Circuit,
- The MultiApp V4 platform (JavaCard platform),
- The Smart Meter Gateway SM applet, and
- The associated guidance documentation.

Note: Secrets are exchanged securely with Personalisation agent: GW PIN are generated by Gemalto using a proprietary diversification method and it is introduced in TOE by Gemalto. GW PIN is derived from a master key provided securely by personalisation agent to Gemalto with a dedicated Gemalto tool. Master key is stored securely in Gemalto site and used only for GW PIN derivation.

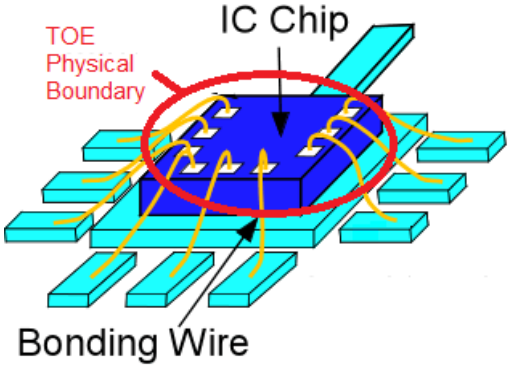


Figure 2: TOE Physical boundaries

It is composed with hardware and software evaluated according to composite evaluation methodology.

Following figure shows product under construction from IC picked on sawn wafer to security module delivered on a reel. The figure also highlights the physical TOE boundary to be considered during evaluation. Figure also illustrates that after delivery to gateway manufacturer, TOE is supposed to be separated from the reel to be integrated in a Gateway.

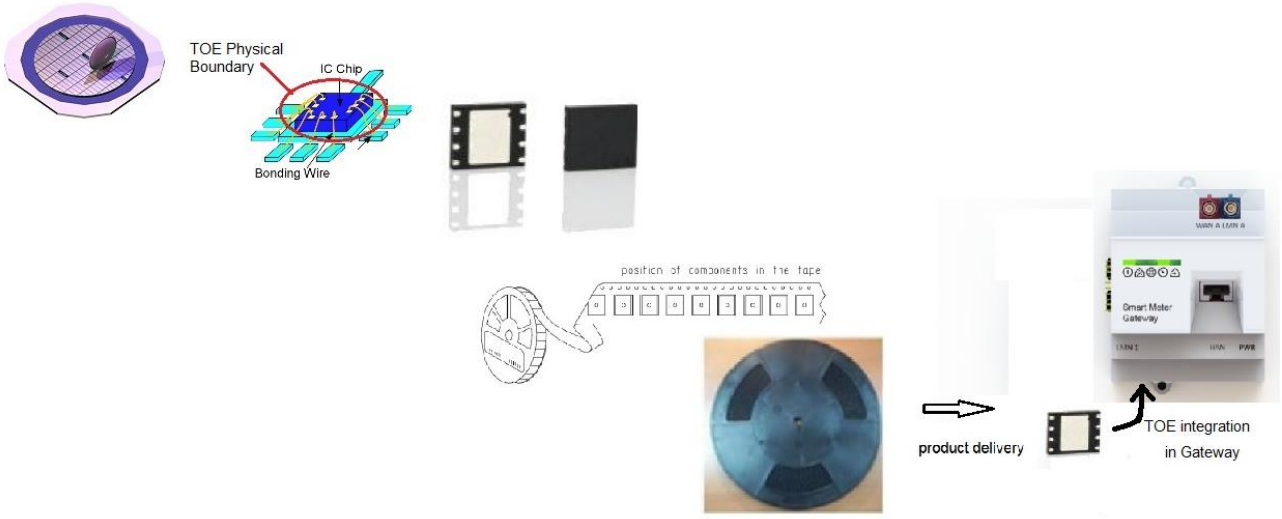


Figure 3: TOE Physical boundaries and Lifecycle

SM applet is a Java Card application running on the platform that provides the cryptographic identity of the Gateway, and it serves as a cryptographic service provider for different cryptographic functionalities, a reliable source for random numbers as well as a secure storage.

The main cryptographic functionalities provided to Gateway by TOE to be compliant to [TR-03109-2] are:

- on Board Key Generation
- secure storage of Key Material and further data relevant for the Gateway as certificates,
- key agreement used by the Gateway for TLS and content data encryption,

- generation and verification of digital signatures on the base of ECDSA,
- secure messaging using PACE V2 protocol,
- content data signature and content data encryption based on Elliptic Curves cryptography,
- RNG according to [AIS20/31] (class DRG.4).

This security target is written on the specification basis [TR-03109-2] for a Smart Meter Security Module.
On a logical level the communication between the TOE and the Gateway follows the requirements outlined in [TR-03109-2] and is therefore oriented on [ISO 7816-4], [ISO 7816-8] and [ISO 7816-9].

The MultiApp V4 Platform is configured in the current evaluation in **Closed** mode:

- **Closed** configuration is default configuration where only SM application (currently evaluated) and default applications (evaluated during platform evaluation) are loaded in TOE in pre-issuance by trusted actor.
- For **Closed** configuration, ability to create GP platform secure channel is no more active after TOE delivery. Therefore there is no ability to perform any platform administration function in post issuance (as add/delete application).
- During platform evaluation, rules for applet verification has been reviewed (on default optional applications) to demonstrate that such verified applet cannot be malicious to platform or any other applet.
- Evaluation of respect of verifications rules for SM application will be evaluated during current evaluation.

This Security Target covers a product in Closed configuration.

This composite Security Target uses the Multiapp Platform security target with the restriction described above. The Platform evaluation (including TOE features, verification process and prior issuance loading process) gives evidences that such verified applets (and the default applets) cannot circumvent the SM applet behavior (see [ST-PLTF] §2.1) and [AGD_PRE_PLTF], §chapter 3).

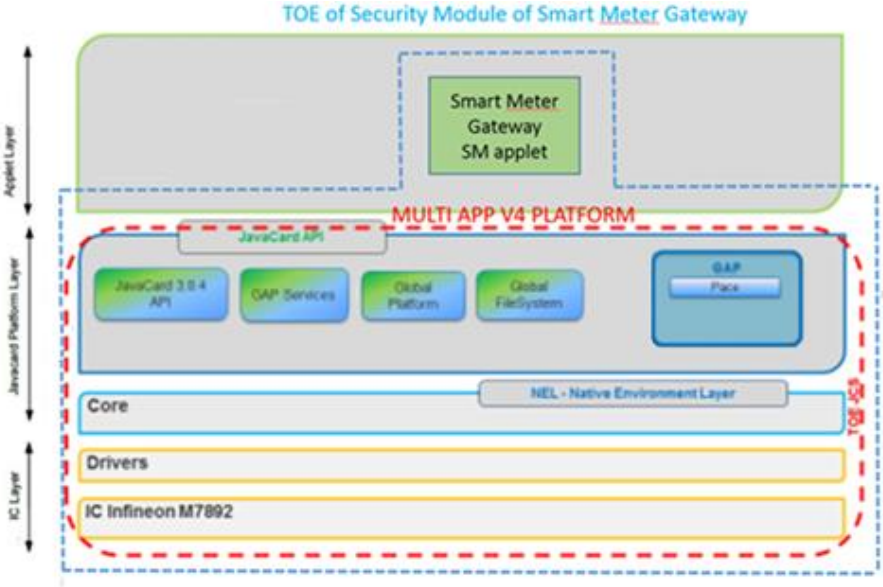


Figure 4: TOE Logical boundary in closed configuration

TOE logical boundary is defined with blue dotted line (- -) on Figure 4.

List of potential default applets seen during platform evaluation are listed in [AGD_OPE_PLTF], §2.2.

Due to BSI limitation, none of default optional applet is included in current TOE configuration.

1.8 NON-TOE HARDWARE/SOFTWARE/FIRMWARE

The TOE is the Security Module intended to be used by a Smart Meter Gateway in a Smart Metering System.

It is an independent product in the sense that it does not require any additional hardware, firmware or software to ensure its security.

However, as the Security Module is physically embedded into the Smart Meter Gateway the Security Module is in addition protected by the same level of physical protection as assumed for and provided by the environment of the Smart Meter Gateway.
In order to be powered up and to be able to communicate the TOE needs an appropriate device for power supply. For regular communication, the TOE requires a device whose implementation matches the TOE's interface specification, refer to [TR-03109-2].

In order to communicate with SM applet, GW includes a software middleware that will be included in the GW evaluation.

1.9 TOE LIFE-CYCLE

The TOE life cycle model is oriented on a life cycle model typically used for smart cards and similar devices and is adapted appropriately for the needs in the framework of Smart Metering Systems. Refer in addition to [TR-03109-1] and [TR-03109-2] where a detailed description of the overall life cycle of a Gateway and its Security Module can be found.

Following the protection profile [PP0077-SecMod, 1.5] the TOE life cycle phases can be divided into the following six phases:

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

In this ST, TOE delivery is performed between phase 4 and phase 5, therefore phase 5 and 6 are considered as operational phases and there are managed through guidances for Integrator and Smart Meter Gateway Administrator.

1.9.1 The phases prior the TOE delivery to Security Module Integrator

The TOE life cycle is described with the following phases:

Phase 1 and 2 “Development”:
The TOE is developed in phase 1 and 2. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these items.
The Embedded Software developer uses the guidance documentation for the integrated circuit and the IC Dedicated Software and develops the Embedded Software platform (MultiApp V4) and associated guidance, the SM application developer uses the platform and associated guidance to develop the SM application and the TOE guidance documentation to be delivered to final user and administrator.
The default application developer uses the platform and associated guidance [AGD_PRE_PLTF] to develop the applications to be loaded in pre-issuance after usage of verification process.

Phase 3 “Manufacturing, Packaging and Testing”:
A first step is under responsibility of IC manufacturer. The IC is manufactured and delivered on sawn wafer form factor. At such step, TOE under construction includes IC and dedicated software including IC flash loader and relevant keys. The IC is securely delivered from the IC manufacturer to the product manufacturer.
The product manufacturer is responsible of the other operations
A packing step is performed without any logical operations.
The IC is extracted from the wafer and packaged using a DNF8 form factor (also named MFF).

The product manufacturer manages the following logical tasks: initial testing and configuration, initialization with product software configuration and pre-personalization of applications**.**

The TOE is then tested and initialized to prepare next operations.
The TOE is initialized with Embedded Software using IC flash loader according to product including platform and pre-issuance application with initial data stored in non-volatile memory.

In this phase, Gemalto must receive a master key for diversification of transport code (PACE-PIN (GW-PIN)). Gemalto recommend the usage of Key export tool [KPT] for exchange of the master key. This tool has not been part of the evaluation.

Phase 4: Security Module Product Finishing Process

Pre-personalizer reuses information of software (platform and SM application) to be loaded to prepare script for TOE configuration.
The TOE pre-personalization is performed at platform level to load software, to import sensitive keys and for initialization of the SM application with dedicated data.
The TOE is finally tested prior delivery to check it is in a secure state before delivery to Security Module Integrator.

1.9.2 Actors

Actors	Identification
Integrated Circuit (IC) Developer	Infineon
Embedded Software Developer	Gemalto
SM Application Developer	Gemalto
Integrated Circuit (IC) Manufacturer	Infineon
Product Manufacturer-Packaging	Gemalto or supplier (optional) covered by platform evaluation
Product-Manufacturer Pre-personalizer	Gemalto
Security Module Integrator	The agent who integrates it in the gateway and pre-personalizes the security module in the gateway.
Security Module Administrator	The agent who personalizes and administrates the security module.*
Smart Meter Gateway Administrator	The agent who administrates the gateway.

Table 3: Identification of the actors

Note: In [TR-03109-2], it is assumed that the administration of the Gateway and the integrated Security Module is performed by same role/entity.

1.9.3 Involved sites

The lifecycle is described in following table.

Life cycle phase	Gemalto Involved sites
Embedded software development (Phase 1)	**Gemalto Meudon** site (Crypto team and R&D team) **Gemalto La Ciotat** site (R&D team) **Gemalto Gémenos** site (Component team and PSE) Covered by platform evaluation mentioned in [CR-PF]
	Gemalto Singapore site (Application R&D team) Covered by site audit included in platform evaluation mentioned in [CR-PF]
IC development (Phase 2)	Infineon development site(s) mentioned in [CR-IC-M7892]
IC Manufacturing, Testing (Phase 3)	Infineon production site(s) mentioned in [CR-IC-M7892]
TOE packaging & testing (Phase 3)	Supplier site for IT or packaging only (no logical operation on TOE) are mentioned in [ALC_DVS]. **Gemalto Pont-Audemer** site Covered by platform evaluation mentioned in [CR-PF]
Security Module Product Finishing Process Prepersonalization & testing (Phase 4)	**Gemalto Pont-Audemer** site Covered by platform evaluation mentioned in [CR-PF]
	Delivery to Security Module Integrator from **Gemalto Pont-Audemer** site Covered by platform evaluation mentioned in [CR-PF]

Table 4: Involved sites

2. CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIM

This security target claims conformance to

- [CC-1]
- [CC-2]
- [CC-3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- [CEM] has to be taken into account.

The evaluation of the TOE uses the result of the CC evaluation of the platform MultiApp V4 claiming conformance to [PP-JCS-Open].

2.2 PP CLAIM

This security target 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-V2-2015, 2014-12 [PP0077-SecMod].

2.3 PACKAGE CLAIM

The evaluation of the TOE is a composite evaluation and uses the results of the CC evaluation of the MultiApp V4 platform. The platform embedded software has been evaluated at level EAL 5 augmented with AVA_VAN.5.The security problem definition, the objectives, and the SFR of the platform are not described in this document but in [ST-PLTF].

The MultiApp V4 JCS security target [ST-PLTF], claims demonstrable conformance to the Protection Profile "JavaCard System – Open configuration", ANSSI-PP-2010- 03, Version 2.6 ([PP-JCS-Open]).

This ST is conforming to assurance package EAL4 augmented with AVA_VAN.5 defined in CC part 3 [CC-3].

2.4 PP CONFORMANCE CLAIM RATIONALE

This security target 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-V2-2015, 2014-12 [PP0077-SecMod].

a) TOE type

The TOE type as stated in the PP [PP0077-SecMod, sec. 1.4.4] is "a service provider for cryptographic functionality in type of a hardware security module with appropriate software installed".

The TOE in this security target is a security module applet running on a smart card platform, the Multiapp V4. This platform includes the hardware, its dedicated software and the operating system. The IC is evaluated in conformance with [PP-IC-0084] according to [ST-IC]. The Platform is evaluated in conformance with [PP-JCS-Open] according to [ST-PLTF] and reusing results from IC evaluation.

This composite TOE as a smart card meets the TOE type of the PP.

b) SPD

The security problem definition, i.e threats, assets, assumptions and OSP are taken from the PP. The compatibility statements between the Security Module TOE and the underlying platform are given in §7.2.2 and demonstrate the consistency.

c) Security objectives and Security Requirements

The security objectives, security requirements are taken from the PP and the operations done for the SFR are clearly indicated. The compatibility between security environment of the security module TOE and the security requirements, security functions and organization policies of the underlying platform is described in §7.2.2.

The operations done for the SFRs taken from the PP [PP0077-SecMod] are clearly indicated.

This demonstrates that this Security Target correctly claims strict conformance to the Protection Profile [PP0077-SecMod].

3. SECURITY PROBLEM DEFINITION

3.1 GENERAL

The assets, threats, OSP, and assumptions of the TOE are those defined in [PP0077-SecMod].

The additional assets, threats and OSP of the platform are described in [ST-PLTF], chapter 5.

For Closed configuration, Platform administration functions are blocked prior TOE delivery. Any impact on the SPD will be indicated by a specific note.

3.2 SUBJECTS AND EXTERNAL ENTITIES

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 [PP0073-SMGW]. In view of the TOE, the Gateway is responsible for sending and receiving TOE commands including the necessary data preparation and post-processing.

In addition, the Smart Meter Gateway Administrator (called Gateway Administrator for short in the following) 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 interacting with the TOE via the Gateway.
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.

As these external entities do not directly interact with the TOE, these entities are out of scope for this ST.

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 1.9 and [TR-03109-1] and [TR-03109-2].

As defined in [PP0077-SecMod], for the operational phase, this ST considers the following external entities and subjects:

External Entity / Subject	Role	Definition
External World	User	Human or IT entity, possibly unauthenticated
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 5: External Entities and Subjects

This table defines external entities and subjects in the sense of [CC1].

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

3.3 ASSETS

The next tables focus on the assets that are relevant for the TOE and does not claim to provide an overview over all assets in the Smart Metering System or for other devices in the LMN. In the tables, for the assets a distinction related to their need for protection in view of confidentiality (Conf.), integrity (Int.) and authenticity (Auth.) is made.

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

Asset / User Data	Description	Need for Protection		
		Conf.	Int.	Auth.
Key Pair Object	Contains for the TOE's asymmetric cryptographic functionality the private key data and optionally the corresponding public key data of a key pair. In addition, the corresponding key attributes (as e.g. information on the related elliptic curve, on the key usage etc.) are stored. A key pair object can be used for the following purposes: • TLS • SIG (content data signature) • ENC (content data encryption)	X	X	X
Public Key Object	Contains for the TOE's asymmetric cryptographic functionality the public key data of a public key. In addition, the corresponding key attributes (as e.g. information on the related elliptic curve, on the key usage etc.) are stored. A public key object can be used for the following purposes: • TLS • SIG (content data signature) • ENC (content data encryption) • AUTH (external authentication)		X	X
Certificate of SM-PKI-Root	X.509 Certificate of the SM-PKI-Root. The Certificate and its contained Public Key is to be considered as a trust anchor.		X	X

Asset / User Data	Description	Need for Protection		
		Conf.	Int.	Auth.
Public Key of SM-PKI-Root	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.		X	X
Quality of Seal Certificates of the Gateway	X.509 Certificates of the Gateway for preliminary Key Pair Objects used for TLS, SIG and ENC.		X	X
GW-Key	Symmetric key used by the Gateway to secure its memory.	X	X	X

Table 6: User Data

In the next table, the TSF Data to be protected by the TOE (as long as in scope of the TOE) are described:

Asset / TSF Data	Description	Need for Protection		
		Conf.	Int.	Auth.
Ephemeral Keys	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).	X	X	X
Shared Secret Value / ECKA-DH	Value ZAB negotiated in the framework of the DH key agreement protocol (ECKA-DH). Used by the Gateway for the TLS handshake.	X	X	X
Shared Secret Value / ECKA-EG	Value ZAB negotiated in the framework of the ElGamal key agreement protocol (ECKA-EG). Used by the Gateway for content data encryption.	X	X	X
Session Keys	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.	X	X	X
Domain Parameters of Elliptic Curves	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.		X	X
GW-PIN	Reference value of the system PACE-PIN of the Gateway for use in the PACE protocol between the Gateway and TOE	X	X	X

Table 7: TSF Data

Assets relevant to platform are described in ([ST-PLTF], § 5.1) and not repeated here.
Note that default applet is a refinement of D_APP_CODE already verified during platform evaluation.
Note that SM applet is a refinement of D_APP_CODE to be verified during TOE evaluation.
Note that applets to be integrated in Closed configuration is also a refinement of D_APP_CODE on which A.VERIFICATION will be applied.

The TSF assets listed in this composite ST, are “user data” or “TSF data” of the platform according to the following table:

Asset	User data of the platform	TSF data of the platform
User data		
Key Pair Object	x	
Public Key Object	x	
Certificate of SM-PKI-Root	x	
Public Key of SM-PKI-Root	x	
Quality of Seal Certificates of the Gateway	x	
GW-Key		x
TSF data		
Ephemeral Keys		x
Shared Secret Value / ECKA-DH		x
Shared Secret Value / ECKA-EG		x
Session Keys		x
Domain Parameters of Elliptic Curves		x
GW-PIN	x	

Table 8: Links between SM Assets and Platform Assets

3.4 ASSUMPTIONS

In the following, according to the threat model as outlined in the following chapter 3.5, assumptions about the environment of the TOE that need to be taken into account in order to ensure a secure operation of the TOE are listed.

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

A.Name **Short title**

Description of the assumption.

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

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

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.

Application note: Recommendations in Administration guidance will help to obtain secure integration of gateway and TOE and to consider such assumption as accurate.

A.OperationalPhase **Operational phase of the integrated Gateway**
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 (see also tables in chapter 3.3).
In particular, this holds for key and PIN objects stored, generated and processed in the operational phase of the integrated Gateway.

Application note: Recommendations in Administration guidance will help to obtain secure management of TOE and to consider such assumption as accurate. Usage of consistent middleware in Gateway for secure communication with security module is required.

A.Administration **Administration of the TOE**

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.

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.

Application note: Recommendations in Administration guidance will help to obtain secure administration of TOE and to consider such assumption as accurate.

A.TrustedAdmin	**Trustworthiness of the Gateway Administrator** 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.
Application note:	Recommendations in Administration guidance will help to obtain well trained administrator of TOE and to consider such assumption as accurate.
A.PhysicalProtection	**Physical protection of the TOE** It is assumed that the TOE is physically and logically embedded into a Gateway that is certified according to [PP0073-SMGW] (whereby the integration is performed during the integration phase of the life cycle model). 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

Other assumptions relevant to platform are described in [ST-PLTF], §5.4 and not repeated here. Those assumptions concern applet management in post issuance (loading and deletion) and are by default valid but not applicable for closed configuration.

3.5 THREATS

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

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

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

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

T.Name	**Short title** Description of the threats.
T.ForgeInternalData	**Forgery of User Data or TSF Data** An attacker with high attack potential tries to forge internal User Data or TSF Data via the regular communication interface of the TOE.

This threat comprises several attack scenarios of forgery of internal User Data or TSF Data. The attacker may try to alter User Data e.g. by deleting and replacing persistently stored key objects or adding data to data already stored in elementary files. The attacker may misuse the TSF management function to change the user authentication data (GW-PIN) to a known value.

T.Compromise InternalData **Compromise of confidential User Data or TSF Data**

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

This threat comprises several attack scenarios of revealing confidential internal User Data or TSF Data. The attacker may try to compromise the user authentication data (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**

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.
This threat comprises several attack scenarios. The attacker may try to circumvent the user authentication mechanism to access assets or functionality of the TOE that underlie the TOE's access control and require user authentication. The attacker may try to alter the TSF data e.g. to extend the user rights after successful authentication.

T.Intercept **Interception of communication**

An attacker with high attack potential tries to intercept the communication between the TOE and the Gateway to disclose, to forge or to delete transmitted (sensitive) data or to insert data in the data exchange.
This threat comprises several attack scenarios. An attacker may read data during data transmission in order to gain access to user authentication data (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**

An attacker with high attack potential tries to launch a cryptographic attack against the implementation of the cryptographic algorithms or tries to guess keys using a brute-force attack on the function inputs.

This threat comprises several attack scenarios. An attacker may try to predict the output of the random number generator in order to get information about a generated session key, shared secret value or ephemeral key. An attacker may try to exploit leakage during a cryptographic operation in order to use SPA, DPA, DFA, SEMA or DEMA techniques with the goal to compromise the processed keys, the 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. 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 **PhysicalTampering**

An attacker with high attack potential tries to manipulate the TOE through physical tampering, probing or modification in order to extract or alter User Data or TSF Data stored in or processed by the TOE. Alternatively, the attacker tries to change TOE functions (as e.g. cryptographic functions provided by the TOE) by physical means (e.g. through fault injection).

T.AbuseFunctionality **Abuse of Functionality**

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

In particular, the TOE shall ensure that functionality that shall not be usable in the operational phase, but which is present during the phases of the TOE's manufacturing and 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.

Note: operational phase includes phase 5 & 6 (see §1.9)

T.Malfunction **Malfunction of the TOE**

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

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

Note: the “IC embedded software” in this ST is made of the platform software and the IC dedicated software.

Threats relevant to platform are described in [ST-PLTF] §5.2 and not repeated here. Nevertheless, the threats described above may overlap with the threats described in [ST-PLTF] for this composite TOE (e.g. T.PhysicalTampering and T.Physical of the platform.

3.6 ORGANIZATIONAL SECURITY POLICIES

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 [PP0073-SMGW].

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**

The TOE shall 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.

P.KeyAgreementDH **DH key agreement**

The TOE and the Gateway shall implement the DH key agreement (ECKA-DH) according to [TR-03109-3], [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**

The TOE and the Gateway shall implement the ElGamal key agreement (ECKA-EG) according to [TR-03109-3], [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**

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], [TR-03109-2].

P.PACE **PACE**
The TOE and the Gateway shall implement the PACE protocol according to [TR-03110-3], [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.

Organizational security policy relevant to platform are described in [ST-PLTF], §5.3, and not repeated here.

3.7 COMPATIBILITY BETWEEN SECURITY ENVIRONMENTS OF [ST-SM] AND [ST-PLTF]

3.7.1 Compatibility between threats of [ST-SM] and [ST-PLTF]

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

SM threats vs platform threats	T.CONFID-JCS-CODE	T.CONFID-APPLI-DATA	T.CONFID-JCS-DATA	T.INTEG-APPLI-CODE	T.INTEG-JCS-CODE	T.INTEG-APPLI-DATA	T.INTEG-JCS-DATA	T.INTEG-APPLI-CODE.LOAD	T.INTEG-APPLI-DATA.LOAD	T.SID.1	T.SID.2	T.EXE-CODE.1	T.EXE-CODE.2	T.NATIVE	T.RESOURCES	T.INSTALL	T.DELETION	T.OBJ-DELETION	T.PHYSICAL
T.ForgeInternalData						X	X								X			X	
T.Compromise InternalData		X	X												X			X	
T.Misuse	X			X	X					X	X	X	X	X	X			X	
T.Intercept																			
T.Leakage																			X
T.PhysicalTampering																			X
T.AbuseFunctionality																			X
T.Malfunction				X	X							X	X	X					X

Table 9: Links between SM and Platform threats

In [ST-PLTF], a dedicated paragraph has been added to threats associated to Platform PACE module. The following table illustrates relationship between SM threats and Platform PACE module threats.

SM threats vs platform Pace Module threats	*T.Skimming*	*T.Eavesdropping*	*T.Abuse-Func*	*T.Information_Leakage*	*T.Phys-Tamper*	*T.Malfunction*	*T.Forgery*
T.ForgeInternalData							X
T.CompromiseInternalData			X				
T.Misuse			X				
T.Intercept	X	X					
T.Leakage				X			
T.PhysicalTampering					X		
T.AbuseFunctionality			X				
T.Malfunction						X	

Table 10: Links between SM and Platform PACE Module Threats

Find here quick explanation of threats mapping.
Note M: Mapping is done using platform in an Open configuration exhibiting threats present in the platform even if most of the threats are not really applicable due to the platform configuration (closed and only SM applet present on platform and loading of extra application is blocked). All code present in the TOE has been developed by Trusted developer and the evaluation process is supposed to check that no malicious code is present in evaluated applet and platform code due respect of platform guidance.
Such explicit mapping also allows to exhibit security features platform even if not fully used in current TOE configuration.

T.ForgeInternalData deals with *"Forgery of User Data or TSF Data*"**,**
therefore there is a link with **T.INTEG-JCS-DATA** where
"The attacker executes an application to alter (part of) Java Card System or API data".
This link is not really applicable with current TOE configuration as explained in note M.

T.ForgeInternalData deals with *"Forgery of User Data or TSF Data*"**,**
therefore there is a link with **T.INTEG-APPLI-DATA** where
"The attacker executes an application to alter (part of) another application's data".
This link is not really applicable with current TOE configuration as explained in note M.

T.ForgeInternalData deals with **"***Forgery of User Data or TSF Data*"**,**
therefore there is a link with **T.RESOURCES** where
"*An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM*".
This link is not really applicable with current TOE configuration as explained in note M.

T.ForgeInternalData deals with *"Forgery of User Data or TSF Data*"**,**
therefore there is a link with **T.OBJ-DELETION** where
"The attacker keeps a reference to a garbage collected object in order (…) to gain access to a memory containing data that is now being used by another application".
This link is not really applicable with current TOE configuration as explained in note M.

T.CompromiseInternalData deals with *"Compromise of confidential User Data or TSF Data*"**,**
therefore there is a link with **T.CONFID-APPLI-DATA** where
"The attacker executes an application to disclose data belonging to another application".
This link is not really applicable with current TOE configuration as explained in note M.

T.CompromiseInternalData deals with *"Compromise of confidential User Data or TSF Data*"**,**
therefore there is a link with **T.CONFID-JCS-DATA** where
"The attacker executes an application to disclose data belonging to the Java Card System".
This link is not really applicable with current TOE configuration as explained in note M.

T.CompromiseInternalData deals with *"Compromise of confidential User Data or TSF Data*"**,**
therefore there is a link with **T.RESOURCES** where
"*An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM*".
This link is not really applicable with current TOE configuration as explained in note M.

T.CompromiseInternalData deals with *"Compromise of confidential User Data or TSF Data*"**,**
therefore there is a link with **T.OBJ-DELETION** where
"The attacker keeps a reference to a garbage collected object in order (…) to gain access to a memory containing data that is now being used by another application".
This link is not really applicable with current TOE configuration as explained in note M.

T.Misuse deals with *"Misuse of TOE functions*"**,**
therefore there is a link with **T.INTEG-APPLI-CODE** where
"*The attacker executes an application to alter (part of) its own code or another application's code*".
This link is only applicable with current TOE configuration for SM applet not for any *another application's code* as explained in note M.

T.Misuse deals with *"Misuse of TOE functions***",**
therefore there is a link with **T.INTEG-JCS-CODE** where
"*The attacker executes an application to alter (part of) the Java Card System code*".
This link is not really applicable with current TOE configuration as explained in note M.

T.Misuse deals with *"Misuse of TOE functions***",**
therefore there is a link with **T.SID.1** where
"An applet impersonates another application, or even the Java Card RE, in order to gain illegal access to some resources of the card or with respect to the end user or the terminal".
This link is not really applicable with current TOE configuration as explained in note M.

T.Misuse deals with *"Misuse of TOE functions***",**
therefore there is a link with **T.SID.2** where
"*The attacker modifies the TOE's attribution of a privileged role (e.g. default applet and currently selected applet), which allows illegal impersonation of this role*".

T.Misuse deals with *"Misuse of TOE functions***",**
therefore there is a link with **T.EXE-CODE.1** where
"*An applet performs an unauthorized execution of a method.*"

T.Misuse deals with *"Misuse of TOE functions***",**
therefore there is a link with **T.EXE-CODE.2** where
"*An applet performs an execution of a method fragment or arbitrary data.*"

T.Misuse deals with *"Misuse of TOE functions***",**
therefore there is a link with **T.NATIVE** where
"*An applet executes a native method to bypass a security function such as the firewall.*"
This link is not really applicable with current TOE configuration as explained in note M.

T.Misuse deals with *"Misuse of TOE functions***",**
therefore there is a link with **T.RESOURCES** where
"*An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM*".
This link is not really applicable with current TOE configuration as explained in note M.

T.Misuse deals with *"Misuse of TOE functions***",**
therefore there is a link with **T.OBJ-DELETION** where
"The attacker keeps a reference to a garbage collected object in order (…) to gain access to a memory containing data that is now being used by another application".
This link is not really applicable with current TOE configuration as explained in note M.

T.Leakage deals with *"leakage of information using observation techniques***",**
therefore there is a link with **T.PHYSICAL** where
"*This threat includes IC failure analysis, electrical probing, unexpected tearing, and DPA*".

T.PhysicalTampering deals with *"Physical Tampering, probing or modification***",**
therefore there is a link with **T.PHYSICAL** where
"*The attacker discloses or modifies the design of the TOE, its sensitive data or application code by physical (opposed to logical) tampering means. This threat includes IC failure analysis, electrical probing, unexpected tearing, and DPA*".

T.AbuseFunctionality deals with *"Abuse of Functionality to disclose or manipulate sensitive User Data or TSF Data***",** therefore there is a link with **T.PHYSICAL** where
"*This threat includes IC failure analysis, electrical probing, unexpected tearing, and DPA*".

T.Malfunction deals with *"applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify TSS***",**

therefore there is a link with **T.INTEG-APPLI-CODE** where
"*The attacker executes an application to alter (part of) its own code or another application's code*".
This link is only applicable with current TOE configuration for SM applet not for any *another application's code* as explained in note M.

T.Malfunction deals with *"applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify TSS***",**
therefore there is a link with **T.INTEG-JCS-CODE** where
"*The attacker executes an application to alter (part of) the Java Card System code*".
This link is not really applicable with current TOE configuration as explained in note M.

T.Malfunction deals with *"applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify TSS***",**
therefore there is a link with **T.EXE-CODE.1** where
"*An applet performs an unauthorized execution of a method.*"

T.Malfunction deals with *"applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify TSS***",**
therefore there is a link with **T.EXE-CODE.2** where
"*An applet performs an execution of a method fragment or arbitrary data.*"

T.Malfunction deals with *"applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify TSS***",**
therefore there is a link with **T.NATIVE** where
"*An applet executes a native method to bypass a security function such as the firewall.*"
This link is not really applicable with current TOE configuration as explained in note M.

T.Malfunction deals with *"applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify TSS***",**
therefore there is a link with **T.PHYSICAL** where
"*This threat includes IC failure analysis, electrical probing, unexpected tearing, and DPA*".

T.ForgeInternalData deals with *"Forgery of User Data or TSF Data***",**
therefore there is a link with **T.Forgery** where
"An attacker fraudulently alters the User Data or/and TSF-data stored on Toe or associated application (e.g. the travel document) or/and exchanged between the TOE and the termina l(..;)".

T.CompromiseInternalData deals with *"Compromise of confidential User Data or TSF Data***",**
therefore there is a link with **T.Abuse-Func** where
"An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE (…)".
This link is not really applicable with current TOE configuration as explained in note M.

T.Misuse deals with *"Misuse of TOE functions***",**
therefore there is a link with **T.Abuse-Func** where
"This threat addresses the misuse of the functions for the initialization and personalization in the operational phase after delivery to the Application user".

T.Intercept deals with *"Misuse of TOE functions***",**
therefore there is a link with **T.Skimming** where
"*An attacker imitates a PACE terminal (e.g. inspection system) in order to get access to the user data stored on or transferred between the TOE and the user(…).*"

T.Intercept deals with *"Misuse of TOE functions***",**
therefore there is a link with **T.Eavesdropping** where
"*Eavesdropping on the communication between the TOE and the PACE terminal.*"

T.Leakage deals with *"leakage of information using observation techniques***",**
therefore there is a link with **T.Information_Leakage** where
"*An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the TOE and associated applications (e.g. travel document) or/and exchanged between the TOE and the terminal connected*."

T.PhysicalTampering deals with *"Physical Tampering, probing or modification***",**
therefore there is a link with **T.Phys-Tamper** where
"*An attacker may perform physical probing of the TOE and associated applications (e.g. travel document) in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software (…).*".

T.AbuseFunctionality deals with *"Abuse of Functionality to disclose or manipulate sensitive User Data or TSF Data***",** therefore there is a link with **T.Abuse-Func** where
"This threat addresses the misuse of the functions for the initialization and personalization in the operational phase after delivery to the Application user".

T.Malfunction deals with *"applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify TSS***",**
therefore there is a link with **T.Malfunction** where
"*An attacker may cause a malfunction the TOE (hardware and software) and associated applications by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software*.".

The threats of the TOE and those of the Platform are mapped in the previous tables without demonstrating any conflict. Some threats of the platform are not linked with TOE without impacting TOE, i.e. T_DELETION and T.INSTALL are specific to the platform and to the post issuance applet management and are not relevant to **closed** configuration.

We can therefore conclude that the threats of [ST-SM] and [ST-PLTF] are consistent.

3.7.2 Compatibility between OSP of [ST-SM] and [ST-PLTF]

The following table demonstrates there are no conflict between Organizational Security Policies associated to TOE and those associated to platform.

SM OSPs vs platform OSPs	OSP.VERIFICATION	OSP.SpecificAPI	OSP.RND
P.Sign			
P.KeyAgreementDH			
P.KeyAgreementEG			
P.Random			X
P.PACE			

Table 11: Links between SM and Platform OSPs

In [ST-PLTF], a dedicated paragraph has been added to OSPs associated to Platform PACE module. The following table illustrates relationship between SM OSPs and Platform PACE module OSPs.

SM OSPs vs platform Pace Module OSPs	P.Terminal	P.Personalisation	P.Manufact	P.Pre-Operational
P.Sign				
P.KeyAgreementDH				X
P.KeyAgreementEG				X
P.Random				
P.PACE				

Table 12: Links between SM and Platform Pace Module OSPs

P.Sign, P.KeyAgreementDH, P.KeyAgreementEG, P.Random, P.PACE are OSP specified in [ST-SM]. The OSP of [ST-PLTF] are valid for the current TOE, in closed configuration (e.g. OSP.Verification is valid for SM applet loaded in pre issuance).

P.Random is linked to **OSP.RND** ensuring that "the entropy of the random numbers provided by the TOE to applet using [JCAPI304] is sufficient".

P.KeyAgreementDH is linked to **P.Pre-Operational** ensuring **"**that only authorized agent performs operations on TOE in pre-operation phase contributing to the correctness of the user data and more especially secret used for key agreement" in pre–issuing phase.

P.KeyAgreementEG is linked to **P.Pre-Operational** ensuring **"**that only authorized agent performs operations on TOE in pre-operation phase contributing to the correctness of the user data and more especially secret used for key agreement" in pre–issuing phase.

There is no contradiction between OSP specified in [ST-SM] vs OSP requested in [ST-PLTF] because there are consistent when they address the same policy and they have no links for different type of policies.

We can therefore conclude that the OSP of [ST-SM] and [ST-PLTF] are consistent.

3.7.3 Compatibility between Threats of [ST-SM] and OSP of [ST-PLTF]

T.ForgeInternalData, T.CompromiseInternalData, T.Misuse, T.Intercept, T.Leakage, T.PhysicalTampering, T.AbuseFunctionality, T.Malfunction are specific to SM TOE and do not contradict the OSP platform described in [ST_PLTF]. Indeed, OSP.VERIFICATION is covered by CC evaluation, OSP.SpecificAPI provides features for secure execution of application and OSP.RND provide random to application.

3.7.4 Compatibility between OSP of [ST-SM] and threats of [ST-PLTF]

The OSP of the TOE (**P.Sign**, **P.KeyAgreementDH, P.KeyAgreementEG, P.Random, P.PACE)** are mainly about cryptography (digital signature generation and verification, DH and ElGamal key agreement,PACE protocol and Random generation) do not contradict the threats on the platform ([ST_PLTF], §5.2; indeed platform objectives (aligned on platform threat coverage) are defined in order to provide security features to be used by application.

3.7.5 Compatibility between Assumptions of [ST-SM] and [ST-PLTF]

A.Integration, A.OperationalPhase, A.Administration, A.TrustedAdmin, A.PhysicalProtection are assumptions specific to [ST-SM] and they do no conflict with the assumptions of [ST-PLTF].

SM assumptions vs platform assumptions	A.APPLET	A.DELETION	A.VERIFICATION
A.Integration			
A.OperationalPhase			
A.Administration			
A.TrustedAdmin			
A.PhysicalProtection			

Table 13: Links between SM and Platform Assumptions

The assumption **A.VERIFICATION** is applicable to the SM applet done prior issuance. The two other assumptions concern applet management in post issuance (loading and deletion) and are by default valid but not applicable for **closed** configuration.

In [ST-PLTF], a dedicated paragraph has been added to assumptions associated to Platform PACE module. The following table illustrates relationship between SM assumptions and Platform PACE module OSPs.

SM assumptions vs platform Pace Module assumptions	A.Insp_Sys
A.Integration	
A.OperationalPhase	X
A.Administration	
A.TrustedAdmin	
A.PhysicalProtection	

Table 14: Links between SM and Platform Pace Module assumptions

A.OperationalPhase assumes 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 is linked to **A.Insp_Sys** as it precises that “PACE secure channel must be established and applicative data (e.g. the logical travel document) must be transferred under PACE” requiring usage of secret protected by environment..

We can therefore conclude that the assumptions of [ST-SM] and [ST-PLTF] are consistent.

3.7.6 Conclusion for Compatibility

As presented in previous chapters, no contradictions or inconsistencies between the security environment of the composite TOE and the underlying Platform (including IC) have been found. Therefore, statement of compatibility is assumed.

4. SECURITY OBJECTIVES

4.1 GENERALS

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

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

O/OE.Name **Short title**

Description of the objective.

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

The security objectives of the TOE are those defined in [PP0077-SecMod].

4.2 SECURITY OBJECTIVES FOR THE TOE

This chapter describes the security objectives for the TOE which address the aspects of the identified threats to be countered by the TOE independently of the operational 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**

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**

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**

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**

The TOE shall provide and enforce the functionality of access right control. The access right control shall cover the functionality provided by the TOE (including its management functionality) and the objects stored in or processed by the TOE. The TOE shall enforce that only authenticated entities with sufficient access control rights can access restricted objects and services. The access control policy of the TOE shall bind the access control right to an object to authenticated entities.

O.KeyManagement	**Key management** The TOE shall enforce the secure generation, import, distribution, access control and destruction of cryptographic keys. The TOE shall support the public key import from and export to the Gateway.
O.TrustedChannel	**Trusted channel** The TOE shall establish a trusted channel for protection of the confidentiality and the integrity of the transmitted data between the TOE and the successfully authenticated Gateway. The TOE shall enforce the use of a trusted channel if defined by the access condition of an object.
O.Leakage	**Leakage protection** The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits. The TOE shall provide side channel resistance, i.e. shall be able to prevent appropriately leakage of information, e.g. electrical characteristics like power consumption or electromagnetic emanations that would allow an attacker to learn about : • private key material, • confidential results or intermediate results of cryptographic computations, • the GW-PIN.
O.PhysicalTampering	**Protection against physical tampering** The TOE shall provide system features that detect physical tampering, probing and manipulation of its components against an attacker with high attack potential, and uses those features to limit security breaches. The TOE shall prevent or resist physical tampering, probing and manipulation with specified system devices and components.
O.AbuseFunctionality	**Protection against abuse of functionality** The TOE shall prevent that functions intended for the testing and production of the TOE and which must not be accessible after TOE delivery can be abused in order (i) to disclose or manipulate sensitive User Data or TSF Data, (ii) to manipulate the TOE's software or (iii) to bypass, deactivate, change or explore security features or functions of the TOE. **Application Note:** Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here. In particular, the TOE shall ensure that functionality that shall not be usable in the operational phase, but which is present during the phases of the TOE's manufacturing and 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** The TOE shall ensure its correct operation. The TOE shall prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. The TOE shall preserve a secure state to prevent errors and deactivation of security features of functions. The environmental conditions include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, and temperature.
O.Sign	**Signature generation and verification** The TOE shall securely generate and verify digital signatures according to [TR-03109-3], [TR-03109-2]. 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** The TOE shall securely implement the DH key agreement (ECKA-DH) according to [TR-03109-3], [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 ZAB for the generation of the pre-master secret and with random numbers as well generated by the TOE afterwards to create the master secret.
O.KeyAgreementEG	**ElGamal key agreement** The TOE shall securely implement the ElGamal key agreement (ECKA-EG) according to [TR-03109-3], [TR-03109-2]. 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 ZAB for the generation of the symmetric encryption keys (hybrid encryption/decryption scheme).
O.Random	**Random number generation** The TOE shall securely generate random numbers for its own use (e.g. for the generation of ECC key pairs and session keys) and for use by the Gateway itself according to [TR-03109-3], [TR-03109-2].
O.PACE	**PACE** The TOE shall securely implement the PACE protocol according to [TR-03110], [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.

4.3 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

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

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 (see also ***Table 6*** and ***Table 7*** in chapter 3.3).

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

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**

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 ***Table 6*** and ***Table 7*** in chapter 3.3).
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**

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.

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**

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**

The TOE shall be physically and logically embedded into a Gateway that is certified according to [PP0073-SMGW] (whereby the integration is performed during the integration phase of the life cycle model).

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** The Gateway shall securely implement the DH key agreement (ECKA-DH) according to [TR-03109-3], [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 ZAB for the generation of the pre-master secret and with random numbers as well generated by the TOE afterwards to create the master secret.
OE.KeyAgreementEG	**ElGamal key agreement** The Gateway shall securely implement the ElGamal key agreement (ECKA-EG) according to [TR-03109-3], [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 ZAB for the generation of the symmetric encryption keys (hybrid encryption/decryption scheme).
OE.PACE	**PACE** The Gateway shall securely implement the PACE protocol according to [TR-03110], [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.
OE.TrustedChannel	**Trusted Channel** 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.

4.4 SECURITY OBJECTIVE RATIONALE

Security objectives rationale is not provided in PUBLIC version.
Refer to complete version for details of this section.

5. EXTENDED COMPONENT DEFINITION

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

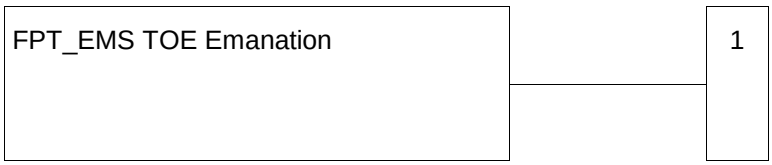
5.1 DEFINITION OF THE FAMILY FPT_EMS

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

Family Behaviour

This family defines requirements to mitigate intelligible emanations.

Component Levelling



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

Management

FPT_EMS.1 There are no management activities foreseen.

Audit

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

FPT_EMS.1 TOE Emanation

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

[assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

5.2 DEFINITION OF THE FAMILY FCS_RNG

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

Family Behaviour

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

Component Levelling

FCS_RNG Generation of random numbers	1

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

Management

FCS_RNG.1 There are no management activities foreseen.

Audit

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

FCS_RNG.1 Random number generation

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

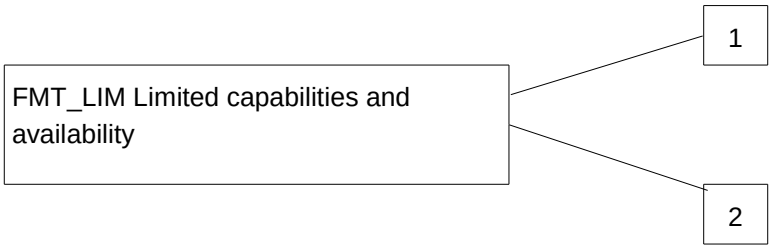
5.3 DEFINITION OF THE FAMILY FMT_LIM

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

Family Behaviour

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

Component Levelling



FMT_LIM.1	Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
FMT_LIM.2	Limited availability requires that the TSF 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 life cycle.

Management

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

Audit

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

FMT_LIM.1 Limited capabilities

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

FMT_LIM.2 Limited availability

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

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

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

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

iii. The combination of both requirements shall enforce the policy

6. SECURITY REQUIREMENTS

6.1 OVERVIEW

This part of the ST defines the detailed security requirements that shall be satisfied by the TOE, as defined by the [PP0077-SecMod] protection profile and for the Evaluation Assurance Level EAL 4 from CC Part 3 [CC3] augmented by AVA_VAN.5.

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

The **refinement** operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed words are ~~crossed out~~. In some cases an interpretation refinement is given. In such a case an extra paragraph starting with "Refinement" is given. In this ST, refinements made by the author will be noted using ***bold italic and underlined text.***

Note: Detailed refinement for references are included in Refinement note rather than in SFR for clarity reason.

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

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

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

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

6.2 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

The following table summarizes all TOE security functional requirements (SFR) of this ST:

SFRs	
Class FCS: Cryptographic Support	
FCS_CKM.1/ECC	Cryptographic key generation / ECC-Key Pairs
FCS_CKM.1/ECKA-DH	Cryptographic key generation / DH key agreement (for TLS)
FCS_CKM.1/ECKA-EG	Cryptographic key generation / ElGamal key agreement (for content data encryption)
FCS_CKM.1/PACE	Cryptographic key generation / PACE
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/SIG-ECDSA	Cryptographic operation / ECDSA Signature generation
FCS_COP.1/VER-ECDSA	Cryptographic operation / ECDSA Signature verification
FCS_COP.1/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

SFRs	
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 15: List of Security Functional Requirements

6.2.1 Class FCS: Cryptographic Support

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

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

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].

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

Application note: [ANSI X9.62] defines Elliptic Curve Digital Signature Algorithm (ECDSA), and [ANSI X9.63] defines Elliptic Curve Key Agreement and Key Transport Schemes.

The TOE supports the following standardized elliptic curve domain parameters (see table 22): (cf. [TR-03116-3, 2.2 Table 3]) for the cryptographic SFR FCS_CKM.1 and the SFRs of the family FCS_COP.1

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

Table 16: List of standardized elliptic curve domain parameters

Cryptographic Key Management (FCS_CKM)

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

FCS_CKM.1/ECC Cryptographic key generation / ECC-Key Pairs

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]: 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 [assignment: *ECKeyPair*] and specified cryptographic key sizes [assignment: *256, 384 and 512 bit length group order*] that meet the following: ~~[TR-03109-3] respective [TR-03116-3], [TR-03109-2],~~ ***[TR-03111-EC, 4.1.3]*[1].**

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

[1] According to the application note for FCS_CKM.1.1/ECC within [PP0077-SecMod], the exact reference is defined by the ST author.

Application Note: [TR-03109-2] requires the TOE to implement the command GENERATE ASYMETRIC 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 [PP0077-SecMod].

Refinement*:** ***The TOE supports the following standardized elliptic curve domain parameters (cf. [TR-03116-3, 2.2 Table 3]) (see table 22).

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

FCS_CKM.1/ECKA-DH	Cryptographic key generation / DH key agreement
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]: not fulfilled but justified (cf. chapter 6.4.1 of the PP [PP0077-SecMod]) FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_CKM.1.1/ECKA-DH	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECKA-DH and specified cryptographic key sizes [assignment: *256, 384 and 512 bits*] that meet the following: ~~[TR-03109-3] respective [TR-03116-3], [TR-03109-2],~~ ***[TR-03111-EC, 4.3.2.1]***[2].

Refinement*:** ***The cryptographic key generation algorithm ECKA-DH is implemented according to [TR-03111-EC, 4.3.2.1]. In [TR-03116-3] a reference to [TR-03111] is given where the specification of ECKA-DH can be found.

Application Note: [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 [PP0073-SMGW]. 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.

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

FCS_CKM.1/ECKA-EG	Cryptographic key generation / ElGamal key agreement
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]: not fulfilled but justified (cf. chapter 6.4.1 of the PP [PP0077-SecMod]), FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

[2] According to the application note for FCS_CKM.1.1/ECKA-DH within [PP0077-SecMod], the exact reference is defined by the ST author.

FCS_CKM.1.1/ ECKA-EG	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECKA-EG and specified cryptographic key sizes [assignment: *256, 384 and 512 bit]* that meet the following**:** ~~[TR-03109-3] respective [TR-03116-3], [TR-03109-2],~~ ***[TR-03111-EC, 4.3.2.2]***[3]***.***
Application Note:	[TR-03109-2] requires the TOE to implement the command GENERAL AUTHENTICATE / variant ECKA-EG. Please note that the TOE is used for parts of the key agreement of keys that are used afterwards in the framework of content data encryption as outlined in [PP0073-SMGW]. The TOE creates on behalf of the Gateway the so-called shared secret value Z_{AB}. The key derivation function is not part of the TOE.

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

FCS_CKM.1/PACE	Cryptographic key generation / PACE
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]: not fulfilled but justified (cf. chapter 6.4.1 of the PP [PP0077-SecMod]) FCS_CKM.4 Cryptographic key destruction : fulfilled by FCS_CKM.4
FCS_CKM.1.1/PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm PACE and specified cryptographic key sizes [assignment: *128, 192 and 256 bits]* that meet the following: ~~[TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3] respective [TR-03116-3], [TR-03109-2]~~ ***[TR-03111-EC, 4.4]***[4].
***Refinement*:**	***The cryptographic key generation algorithm used for PACE keys is implemented according to [TR-03111-EC, 4.4]. The key derivation function KDF is selected according to [TR-03111-EC, 4.3.3], the mapping function is GMap() as defined there in 4.4.1.***
Application Note:	Based on [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3] respective [TR-03116-3], [TR-03109-2], the TOE generates cryptographic keys according to PACEv2 defined in [TR-03110-2, part 2] (as refinement operation for the generic references given in the PP at present). In [TR-03116-3] a reference to [TR-03110-2] and [TR-03110-3] with information on the PACE-algorithm specification as relevant for the TOE can be found.
Application Note:	[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 keys for message encryption and authentication (secure messaging) as required by FCS_COP.1/PACE-ENC and FCS_COP.1/PACE-MAC. Secure messaging is carried out for the main data exchange between the Gateway and the TOE.

[3] According to the application note for FCS_CKM.1.1/ECKA-EG within [PP0077-SecMod], the exact reference is defined by the ST author.

[4] According to the application note for FCS_CKM.1.1/PACE within [PP0077-SecMod], the exact reference is defined by the ST author.

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

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

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]:: 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 [assignment: *physical deletion by overwriting the memory data with logical zeros, or the new key]* that meets the following: [assignment: *none*].

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

Application Note: Explicit deletion of a secret using the DELETE KEY command is covered by the ST.

Refinement: ***The TOE provides the command DELETE KEY which overwrites explicitly the memory area of a key with logical zeros.***

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

Further, the negotiated shared secret value Z_{AB} as required by FCS_CKM.1/ECKA-EG shall be destroyed after it has been transmitted to the Gateway.

Refinement: ***After de-allocation of the resource the memory data of the shared secret is overwritten by logical zeros.***

Cryptographic Operation (FCS_COP)

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

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]: 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 in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes [assignment: *256, 384 and 512 bits*] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2].
***Refinement*:**	***Based on [TR-03109-3] respective [TR-03116-3], [TR-03109-2], the TOE implements algorithm ECDSA according to [TR-03111-EC §4.2.1.1]. In [TR-03116-3] a reference to [TR-03111] is given where the specification of ECDSA (in particular, signature generation) can be found.***

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

FCS_COP.1/VER-ECDSA	Cryptographic operation / ECDSA Signature verification
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: 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 signature verification using the command PSO VERIFY DIGITAL SIGNATURE in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes [assignment: *256, 384 and 512 bits]* that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2].
Refinement:	***The signature algorithm ECDSA is defined in [TR-03111-EC] in clause 4.2.1. The TOE verifies ECDSA signatures according to [TR-03111-EC, 4.2.1.2]. This Technical Guideline is the reference for ECDSA given in [TR-03109-3] and [TR-03116-3].***

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

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 in accordance with a specified cryptographic algorithm *ECDSA* and cryptographic key sizes [assignment:

*256, 384, 512 bits***]** that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2].

Refinement: ***Based on [TR-03109-3] respective [TR-03116-3], [TR-03109-2], the TOE implements the command EXTERNAL AUTHENTICATE defined in [TR-03111-EC] in clause 4.2.1.1. In [TR-03116-3] a reference to [TR-03111] is given where the specification of ECDSA (in particular, signature verification) can be found.***

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

FCS_COP.1/IMP	Cryptographic operation / Import of Public Keys
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: 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 the import of Public Keys for the command PSO VERIFY CERTIFICATE in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes [assignment: *256, 384, 512 bits*] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2].
Refinement:	***The signature verification algorithm ECDSA implemented in the command PSO VERIFY CERTIFICATE is defined within [TR-03111-EC] in clause 4.2.1. This Technical Guideline is the reference for ECDSA given in [TR-03116-3].*** ***Based on [TR-03109-3] respective [TR-03116-3], [TR-03109-2], the TOE implements PSO VERIFY CERTIFICATE as defined within [TR-03111-EC] in clause 4.2.1.2).***

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

FCS_COP.1/PACE-ENC	Cryptographic operation / AES in CBC mode for secure messaging
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: 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 in accordance with a specified cryptographic algorithm AES in CBC mode and cryptographic key sizes [assignment: *128,192,256 bits*] that meet the following**:** [TR-03109-3] respective [TR-03116-3], [TR-03109-2].

***Refinement*:**	***The cryptographic algorithm AES is defined in [FIPS197], the corresponding mode of operation CBC is defined in [SP800-38A] (CBC). These are the references given in [TR-03116-3, clause 2.1].***
Application Note:	Based on [TR-03109-3] respective [TR-03116-3], [TR-03109-2], the TOE implements 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 .
Application Note:	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.

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

FCS_COP.1/PACE-MAC	Cryptographic operation / AES-CMAC for secure messaging
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: 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 in accordance with a specified cryptographic algorithm AES-CMAC and cryptographic key sizes [assignment: *128, 192 and 256 bits*] that meet the following: [TR-03109-3] respective [TR-03116-3], [TR-03109-2].
***Refinement*:**	***Based on [TR-03109-3] respective [TR-03116-3], [TR-03109-2], the TOE implements AES with mode of operation CMAC as defined in [NIST 197] and [RFC 4493] and NIST Special Publication [SP800-38B] referenced in [TR-03116-3, clause 2.1].***
Application Note:	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.

Random Number Generation (FCS_RNG)

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

FCS_RNG.1	Random number generation
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FCS_RNG.1.1	The TSF shall provide a [selection: *hybrid deterministic*] random number generator that implements: [assignment: *DRG.4 capabilities according to [AIS20/31]*]. *(DRG.4.1) The internal state of the RNG shall use PTRNG of class PTG.2 as random source.* *(DRG.4.2) The RNG provides forward secrecy.* *(DRG.4.3) The RNG provides backward secrecy even if the current internal state is known.* *(DRG.4.4) The RNG provides enhanced forward secrecy on demand using call to internal function "cry_rng_reseed".* *(DRG.4.5) The internal state of the RNG is seeded by a PTRNG of class PTG.2.*
FCS_RNG.1.2	The TSF shall provide random numbers that meet [assignment: *(DRG.4.6) The RNG generates output for which $k = 2^{35}$ strings of bit length 128 are mutually different with probability at least 1-ε, with $\varepsilon = 2^{-58}$ ($k > 2^{34}$ and $\varepsilon < 2^{-16}$)* *(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A*].

Application Note: 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.

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 respective the Gateway Administrator) 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.

6.2.2 Class FDP: User Data Protection

Access Control Smart Meter SFP

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:

Subjects:

- external world
- Gateway
- Gateway Administrator

Security attributes for subjects:

- "authenticated via PACE protocol"
- "authenticated via key-based external authentication"

Objects:

- key pair objects, public key objects, certificates, and symmetric keys (GW-keys) as presented in Table 6.

Security attributes for objects:

- "access rule" (see below)

Operations:

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

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

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

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

FDP_ACC.2	Complete access control
Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Security attribute based access control: fulfilled by FDF_ACF.1
FDP_ACC.2.1	The TSF shall enforce the Access Control Smart Meter SFP on Subjects: • external world • Gateway • Gateway Administrator • [assignment: *none*] Objects: • key pair objects, public key objects, certificates, and symmetric keys (GW-keys) as presented in ~~Table 4~~ ***Table 6*** • [assignment: *none*] and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

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

FDP_ACF.1	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control : 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 to objects based on the following: Subjects: • external world • Gateway with security attribute "authenticated via PACE protocol" • Gateway Administrator with security attribute "authenticated via key-based external authentication" • [assignment: *none*] Objects: • key pair objects, public key objects, certificates, and symmetric keys (GW-keys) as presented in ~~Table 4~~ ***Table 6*** each with security attribute "access rule" • [assignment: *none*].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: Access rules defined in the Access Control Smart Meter SFP (refer to the definition of the SFP above).
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: No entity shall be able to read out private keys from the TOE.

Stored data integrity (FDP_SDI)

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

FDP_SDI.2	Stored data integrity monitoring and action
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors on all objects, based on the following attributes: [assignment: *integrity checked stored data*].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall not use the data and stop the corresponding process accessing the data, warn the entity connected, [assignment: *or enter the software security reset state*].

Application Note: The requirements in FDP_SDI.2.1 specifically apply to the assets as defined in Table 6.

Residual Information Protection (FDP_RIP)

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

FDP_RIP.1	Subset residual information protection
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation **[A]** of the resource to, deallocation **[D]** of the resource from]* the following objects: PIN ***[A] (done by platform)***, session keys ***[D]*** (immediately after closing related communication session), private cryptographic keys ***[D] (using clearKeys API)***, shared secret value Z_{AB} ***[D] (using clearKeys API), and*** ephemeral keys ***[D] (using clearKeys API),*** [assignment: *none*].
Note:	Optional proposal to include iterations of FDP_RIP.1 is not implemented in current security target, therefore associated application has been suppressed.
Application Note:	Note that the specification of the Security Module allows the creation and deletion of key objects during operational use. Theoretically it could be possible that a newly created key object uses memory areas which belonged to another key object before. Therefore the Security Module must ensure that contents of the old key object are not accessible by using the new key object.

Export from the TOE (FDP_ETC)

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

FDP_ETC.1	Export of user data without security attributes
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] : fulfilled by FP_ACC.2
FDP_ETC.1.1	The TSF shall enforce the Access Control Smart Meter SFP when exporting user data, controlled under the SFP, outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.

Import from outside of the TOE (FDP_ITC)

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

FDP_ITC.1	Import of user data without security attributes
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.2 FMT_MSA.3 Static attribute initialization
FDP_ITC.1.1	The TSF shall enforce the Access Control Smart Meter SFP when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none.

Inter-TSF User Data Confidentiality Transfer Protection (FDP_UCT)

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

FDP_UCT.1	Basic data exchange confidentiality
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]: 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 to transmit, receive user data in a manner protected from unauthorized disclosure.

Inter-TSF User Data Integrity Transfer Protection (FDP_UIT)
The TOE shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below:

FDP_UIT.1	Data exchange integrity
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.2 [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1.
FDP_UIT.1.1	The TSF shall enforce the Access Control Smart Meter SFP to transmit, receive user data in a manner protected from modification, deletion, insertion, replay errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, replay has occurred.

6.2.3 Class FIA: Identification and Authentication

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

FIA_ATD.1	User attribute definition
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: • for device (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).

Application Note:
Mutual authentication of the Gateway and the TOE 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.

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

FIA_SOS.1	Verification of secrets
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets **provided by the Gateway for the PACE-PIN respective GW-PIN** meet [assignment: *minimal length of 10 octets*].
Application Note:	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) that is required for the PACE protocol the ST defines on base of the requirements made in [TR-03109-2] the required minimum length for the PACE-PIN (as defined quality metric).

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

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 • Establishing a communication channel between the TOE and the external world, • Reading the ATR~~/ATS~~*, • Reading of data fields containing technical information, • [assignment: *none*] 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.
Refinement	****: Only ATR is available (no contactless interface).***
Application Note:	Authentication of the Gateway is performed via the PACE protocol between the Gateway and the TOE, refer to the SFR FCS_CKM.1/PACE.

Application Note: 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 6.2.2) 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.

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

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 • 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), • [assignment:*none*] 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.
Refinement	****: Only ATR is available (no contactless interface).***

Application Note: 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.

Application Note: 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 6.2.2) 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.

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

FIA_UAU.4	Single-use authentication mechanisms
Hierarchical to:	No other components.

Dependencies:	No dependencies.
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to • PACE authentication mechanism • key-based external authentication mechanism

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

FIA_UAU.5	Multiple authentication mechanisms
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide • authentication via the PACE protocol, • secure messaging in encrypt-then-authenticate mode using PACE session keys, • key-based external authentication to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the following rules: • PACE/PIN based authentication shall be used for authenticating a device (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).

User Identification (FIA_UID)

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

FIA_UID.1	Timing of identification
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow • Establishing a communication channel between the TOE and the external world, • Reading the ATR~~/ATS~~*, • Reading of data fields containing technical information, • Carrying out the PACE protocol according to [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03109-3], [TR-03109-2] (by means of command GENERAL AUTHENTICATE), • [assignment: *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.

Refinement ****: Only ATR is available (no contactless interface).***

User-Subject Binding (FIA_USB)
The TOE shall meet the requirement "User-subject binding (FIA_USB.1)" as specified below:

FIA_USB.1	User-subject binding
Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition: fulfilled by FIA_ATD.1
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: • authentication state for the 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 set to "not authenticated".
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: • for device (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.

6.2.4 Class FMT: Security Management

Limited Capabilities and Availability (FMT_LIM)
The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below:

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

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

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

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

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

or conversely

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

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

Specification of Management Functions (FMT_SMF)

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

FMT_SMF.1	Specification of Management Functions
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: • Management of key objects by means of commands CREATE KEY, DELETE KEY, ACTIVATE KEY, DEACTIVATE KEY, GENERATE ASYMMETRIC KEY PAIR, PSO VERIFY CERTIFICATE, • Management of DFs and EFs by means of commands CREATE DF/EF, ACTIVATE DF/EF, DEACTIVATE DF/EF, DELETE DF/EF, TERMINATE DF/EF, • Management of PIN objects by means of command CHANGE REFERENCE DATA, • Life cycle management of the TOE by means of command TERMINATE CARD USAGE, • Update of keys by means of commands GENERATE ASYMMETRIC KEY PAIR, PSO VERIFY CERTIFICATE,

- Update of certificates by means of command UPDATE BINARY,
- Update of symmetric keys (GW-keys) by means of command UPDATE BINARY,
  - [assignment: *none*].

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

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

FMT_SMR.1	Security Roles
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1
FMT_SMR.1.1	The TSF shall maintain the roles • user • authenticated Gateway • authenticated Gateway Administrator • [assignment: *none*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.2.5 Class FPT: Protection of the TSF

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

FPT_EMS.1	TOE Emanation
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit [assignment: *power variations, timing variations, EM variations during command execution*] in excess of [assignment: *intelligible threshold*] enabling access to • PIN, • session keys, • shared secret value Z_{AB}, • ephemeral keys, • [assignment: *none*] and • private asymmetric keys of the user, • symmetric keys of the user (GW-keys), • [assignment: *none*].
FPT_EMS.1.2	The TSF shall ensure any users are unable to use the following interface circuit surface to gain access to • PIN, • session keys,

- shared secret value Z_{AB},
- ephemeral keys,
- [assignment: *none*] and
- private asymmetric keys of the user,
- symmetric keys of the user (GW-keys),
- [assignment: *none*].

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

Fail Secure (FPT_FLS)

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

FPT_FLS.1	Failure with preservation of secure state
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: • power loss, • exposure to operating conditions where therefore a malfunction could occur, • detection of physical manipulation or physical probing, • integrity errors according to FDP_SDI.2, • insufficient entropy during random number generation, • failure detected by the TSF according to FPT_TST.1, • errors during processing cryptographic operations, • errors during evaluation of access control rules, and • [assignment: *none*].

TSF Physical Protection (FPT_PHP)

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

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

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

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

FPT_TST.1	TSF testing
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self-tests during initial start-up, periodically during normal operation to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of TSF.

6.2.6 Class FTP: Trusted path/channels

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

FTP_ITC.1	Inter-TSF trusted channel
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Gateway except reading out the data fields with technical information

Application Note: Trusted IT product here in the GW and the remote server used by the GW Administrator

6.3 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

The SAR for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following components: AVA_VAN.5.

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

Assurance Class	Assurance Component	
Class ADV: Development	Architectural design	(ADV_ARC.1)
	Functional specification	(ADV_FSP.4)
	Implementation representation	(ADV_IMP.1)
	TOE design	(ADV_TDS.3)
Class AGD: Guidance documents	Operational user guidance	(AGD_OPE.1)
	Preparative user guidance	(AGD_PRE.1)
Class ALC: Life-cycle support	CM capabilities	(ALC_CMC.4)
	CM scope	(ALC_CMS.4)
	Delivery	(ALC_DEL.1)
	Development security	(ALC_DVS.1)
	Life-cycle definition	(ALC_LCD.1)
	Tools and techniques	(ALC_TAT.1)
Class ASE: Security Target evaluation	Conformance claims	(ASE_CCL.1)
	Extended components definition	(ASE_ECD.1)
	ST introduction	(ASE_INT.1)
	Security objectives	(ASE_OBJ.2)
	Derived security requirements	(ASE_REQ.2)
	Security problem definition	(ASE_SPD.1)
	TOE summary specification	(ASE_TSS.1)
Class ATE: Tests	Coverage	(ATE_COV.2)
	Depth	(ATE_DPT.1)
	Functional tests	(ATE_FUN.1)
	Independent testing	(ATE_IND.2)
Class AVA: Vulnerability Assessment	Vulnerability analysis	(AVA_VAN.5)

Table 17: List of Security Assurance Requirements

6.3.1 Refinements of the TOE Security Assurance Requirements

The following refinements shall support the comparability of evaluations according to this Security Target. The mandatory documents themselves mentioned below shall be consulted for exact details and overrule the refinements in case of any inconsistency (e.g. due to updates).
The Refinement is pointed out by using the **bold** type.

The Common Criteria assurance component of the family AVA_VAN (Advanced methodical vulnerability analysis) addresses “A methodical vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.”
Since [CEM] does not describe a specific methodical approach available guidance for the present product type shall be used for the vulnerability analysis of the TOE. Especially supporting documents for this product type available for the application of the Common Criteria respective being part of the SOG-IS MRA shall be considered.
The following text reflects the requirements of the selected component AVA_VAN.5:
Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

AVA_VAN.5.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.5.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.5.3E	The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.
AVA_VAN.5.4E	The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

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

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

6.4 SECURITY REQUIREMENTS RATIONALES

6.4.1 Security Functional Requirements Rationale

Security Functional Requirements rationale is not provided in PUBLIC version.
Refer to complete version for details of this section.

6.4.2 Security Assurance Requirements Rationale

Security Assurance Requirements rationale is not provided in PUBLIC version.
Refer to complete version for details of this section.

6.4.3 Security Requirements – Internal Consistency

The following part of the security requirements rationale is not provided in PUBLIC version.
Refer to complete version for details of this section.

7. TOE SUMMARY SPECIFICATION

7.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the SM applet in combination with SF provided by the platform and the IC.

7.1.1 SF provided by SM Applet using platform security services

This section presents the security functions provided by the SM applet in combination with the platform.

Identification	Name
SF.AUTHENTICATION	Authentication management for device (Gateway) and TOE using PACE protocol and for human user (Gateway Administrator). For device, using GW-PIN within the PACE protocol, For human user using asymmetric authentication key (with the external authentication).
SF.DIGITAL_SIGNATURE_GENERATION	Performs Digital Signature Generation management. It generates digital signatures based on elliptic curve cryptography according to the ECDSA specification in [TR-03111-ECC] (FCS_RNG.1, FCS_COP.1/SIG-ECDSA). The TOE uses the curves listed in table 22 with corresponding key lengths.
SF.DIGITAL_SIGNATURE_VERIFICATION	Performs Digital Signature Verification management It verifies digital signatures provided by external entity based on elliptic curve cryptography according to the ECDSA specification in [TR-03111-ECC] (FCS_RNG.1, FCS_COP.1/SIG-ECDSA). The TOE uses the curves listed in table 22 with corresponding key lengths. Signature verification is also required as part of external authentication. The external entity authenticates against the Security Module, which checks the signature of the transmitted security token
SF.VERIFY_CERTIFICATE	Performs verification of certificate For such purpose, TOE has to import of public keys through certificates into the TOE. Successful digital signature verification of certificates transfers the trust to certificate data, the public key of an external entity.
SF.KEY_AGREEMENT_TLS	Key Agreement for TLS During the TLS handshake between GW and other parties, TOE is used to implement ECKA-DH-protocol for deriving a master secret to be used by the gateway for communication with external world.
SF.KEY_AGREEMENT_CDE	Key Agreement for Content Data Encryption Asymmetric content data encryption uses an ephemeral shared value, from which the symmetric algorithm key is derived. It is generated by the ECKA-EG protocol. The key derivation is performed by the Gateway. The confidentiality and the authenticity of the shared ephemeral value is guaranteed by the trusted channel provided by the PACE protocol
SF.CRYPTO	Cryptography management (including asymmetric key pair generation based on elliptic curve cryptography keys and random generation request) and key

	destruction method. Random generation implemented in the TOE is compliant with level DRG.4 according to [AIS20/31],
SF.INTEGRITY	Integrity monitoring for File system and data object reusing primitive of platform.
SF.MANAGEMENT	Operation management and access control for File System and objects including residual information protection.
SF.SECURE_MESSAGING	Secure messaging management includes operations that secure channel is created using PACE protocol, check that sensitive operations are performed by platform and data are retrieved from buffer APDU managed by platform. Only authenticated entity is allowed to establish the trusted channel with TOE and Usage of session keys provides re-authentication, confidentiality and integrity of the trusted channel established in the PACE protocol with a minimal length of 10 bytes for the PIN giving entropy for shared secret.
SF.APPLET_CSM	Card Security Management unsecure state detection (including wrong applet life cycle transition), exception management and reaction at level of applet.

Table 18: TOE Security Function List for SM Applet using platform security services

7.1.2 TSFs provided by the Platform and Platform Pace Module

The evaluation is a composite evaluation using the results of the Platform evaluation and IC evaluation.
The following table provides the list of platform SFs used for security of Smart Meter Gateway Security module.

SF	Description
SF.FW	It implements Firewall providing applet isolation, managing context for each application and sharing mechanism with access control.
SF.API	It provides interfaces to application and more particularly to cryptographic services, including key and RND generation, key destruction, and management of sensitive operations.
SF.CSM	Card Security Management implements resource management (allocation and deallocation), unsecure state detection, exception management and reaction at level of platform level.
SF.AID	AID Management provides application identification and management of rules relevant to application security attributes as package AID, Applet's version number, registered applet's AID, applet selection status.
SF.INST	Installer allows applet installation with preservation of secure state checking respect of rules and completion of operation during applet loading, installation, and sensitive data loading and initialization.
SF.ADEL	Applet Deletion allows secure applet deletion with preservation of secure state checking respect of rules and completion of operation and management of security attributes as ActiveApplets.
SF.ODEL	Object Deletion allows secure object deletion with preservation of secure state checking respect of rules and completion of operation as unreferenced objects handling.
SF.CAR	Secure Carrier maintains the role of Card Manager managing access to APDUs for applets and JCAPI to applets contributing to isolation between applications.
SF.SCP	Smart Card Platform contributes to assure integrity of sensitive assets: Applets, PIN and Keys by providing transaction mechanism and periodically tests the correct operation of security mechanisms of the IC.
SF.CMG	Card Manager contributes to maintain the application secure state during application loading and extradition operation and key importation.
SF.APIS	Specific API provides services to application to control applet execution flow, to detect and react any failure during operation as data transfer. It also provides services leading to unobservability of sensitive operations.
SF.RND	RNG provides Random values consistent with expected variability defined by the standard.

Table 19: Security Functions provided by the Platform

These SF are detailed in [ST-PLTF].

SF	Description
SF.REL	Protection of data
SF.AC	Access control
SF.SYM_AUTH	Symmetric authentication
SF.SM	Secure messaging
SF.PERSO	Provides service for Personalization of data in used in PACE

Table 20: Security Functions provided by the Platform Pace Module

These SF are detailed in [ST-PLTF].

7.2 TOE SUMMARY SPECIFICATION RATIONALE

7.2.1 TOE Security Functions Rationale

The TOE security functions rationale is not provided in PUBLIC version.
Refer to complete version for details of this section.