IDEMIA

SECURITY TARGET LITE
MORPHO_HC_GERMANY_G2_COS V1

Contract no.: N/A

Reference: 2013_1000002707
Version: V1.05
Date: 01.02.2019
Document Categorizations:
ASE_ST

Document status:	Version:	Author:
Final	V1.05	Sebastian Bond, Jörg Greve, Martin Becker

Document status:	Version:	Author:
Final	V1.05	Sebastian Bond, Jörg Greve, Martin Becker

Table of contents

Table of figures

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

DOCUMENT EVOLUTION

Version	Author	Revision
V1.00	Sebastian BOND	Final Version of ST-Lite based on the ST
V1.01	Jörg GREVE	Corrections in chapter 6.2
V1.02	Sebastian BOND	Update References
V1.03	Martin BECKER	Update concerning ALC Re-Evaluation
V1.04	Agnes DILLER	Update concerning ALC Re-Evaluation, updated Certification ID
V1.05	Agnes DILLER	Corrected Certification ID

1 TOE Reference

This Security Target refers to the smartcard product "Morpho_HC_Germany_G2_COS V1" (TOE) provided by Morpho (now Idemia) for a Common Criteria evaluation.

Title:	Security Target Lite – Morpho_HC_Germany_G2_COS V1
Document Category:	Security Target Lite for a CC Evaluation
Document ID:	2013_1000002707
Version:	V1.05
Publisher:	Morpho (now Idemia)
TOE:	"Morpho_HC_Germany_G2_COS V1" (Smartcard Product containing IC with Smartcard Embedded Software, intended to be used within the German Health Care System)
CertificationID:	BSI-DSZ-CC-0938-2016-MA-01
IT Evaluation Scheme:	German CC Evaluation Scheme
Evaluation Body:	SRC Security Research & Consulting GmbH
Certification Body:	Bundesamt für Sicherheit in der Informationstechnik (BSI)

This Security Target has been built in conformance with Common Criteria V3.1 Revision 4 [CC_P1].

This security target states the security requirements that are met by the TOE, provides an overview on the security functionality offered by the product and describes the intended usage of the TOE.

1.1 Security Target and TOE Identification

Security Target identification is described in the table below:

ST Identification	**2013_1000002707 / BSI-DSZ-CC-0938**
Version	V1.05
Origin	Morpho (now Idemia)
TOE Identification	Morpho_HC_Germany_G2_COS V1
Revision number	R1.1.2
Administration guidance	AGD_INI/PERS
User guidances	AGD_OPE
Chip Identifier	M7892 B11 (SLE 78CFX3000P)
Chip Ref. Certificate	BSI-DSZ-CC-0782-V2-2015
Assurance Level	4+
CC Version	3.1 Release 4

1.2 Referenced Literature

Reference	Description
[EXS_EHC_COS]	Title: Spezifikation des Card Operating System (COS) – Elektronische Schnittstelle Version: 3.8.0 Date: 17.07.2015 Publisher: gematik mbH
[EXS_CCDB_COMP]	Title: CCDB, Composite product evaluation for Smart Cards and similar devices Identification: CCDB-2012-04-001 Version: 1.2 - Revision Date: 1, April 2012
[EXS_WRP_COS]	Title: Spezifikation Wrapper Version: 1.7.0 Date: 17.07.2015 Publisher: gematik mbH
[BSI_PP_EHC_G2]	Title Common Criteria Protection Profile – Card Operating System Generation 2 (PP COS G2) Identification BSI-CC-PP-0082-V2 Version 1.9 Date 18th November 2014 Publisher Bundesamt für Sicherheit in der Informationstechnik (BSI)
[BSI_PP_IC]	Title Security IC Platform Protection Profile Identification BSI-PP-0035- 2007 Version 1.00 Date 15.06.2007 Publisher Bundesamt für Sicherheit in der Informationstechnik (BSI)
[ST_IC]	Title Security Target Maintenance - M7892 B11, including optional Software Libraries RSA – EC – SHA-2 - Toolbox Version 1.2 Date 24.07.2012 Author Hans Ulrich Buchmüller Publisher Infineon Technologies AG
[IC_UG]	Title: M7892 - Hardware Reference Manual Version: Revision 1.5 Date: 29.03.2014 Publisher: Infineon Technologies AG

Reference	Description
[IC_CL_UG]	Title: SLE 70 Asymmetric Crypto Library for Crypto@2304T, RSA / ECC / Toolbox, User Interface Version: 1.02.013 Date: 07.06.2011 Publisher: Infineon Technologies AG
[CC_P1]	Title: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model Identification: CCMB-2012-09-001 Version: Version 3.1 Revision 4 Date: September 2012
[ISO_7816_3]	Title: Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocol. Identification: ISO/IEC 7816-3 Version: Edition 3 Date: 2006 Publisher: International Organization for Standardization/International Electrotechnical Commission

References for parts based on the used Protection Profile [BSI_PP_EHC_G2]:

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

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

[5] AIS20: Functionality classes and evaluation methodology for deterministic random number generators, Version 2.1, 02.12.2011, Bundesamt für Sicherheit in der Informationstechnik

[6] AIS31: Functionality classes and evaluation methodology for true (physical) random number generators, Version 2.1, 02.12.2011, Bundesamt für Sicherheit in der Informationstechnik

[7] W. Killmann, W. Schindler, „A proposal for: Functionality classes for random number generators", Version 2.0, September 18, 2011

[8] CC Supporting Document, Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0, Revision 1, CCDB-2007-09-001

[9] Supporting Document Mandatory Technical Document: The Application of CC to Integrated Circuits, March 2009, Version 3.0, Revision 1, CCDB-2009-03-002

[10] Supporting Document Guidance, Smartcard Evaluation, February 2010, Version 2.0, CCDB-2010-03-001

Protection Profiles

[11] Protection Profile Security IC Platform Protection Profile developed by Atmel, Infineon Technologies AG, NXP Semiconductors, Renesas Technology Europe Ltd., STMicrocontrolles, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0035-2007, Version 1.0, 15.06.2007

[12] prEN 14169-2:2012: Protection profiles for secure signature creation device — Part 2: Device with key generation, BSI-CC-PP-0059

[13] prEN 14169-3:2012: Protection profiles for secure signature creation device — Part 3: Device with key import, BSI-CC-PP-0075

[14] prEN 14169-4:2012: Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, BSI-CC-PP-0071

[15] prEN 14169-5:2012: Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, BSI-CC-PP-0072

Technical Guidelines and Specifications

[16] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents Part1 – eMRTDs with BAC/PACEv2 and EACv1, Part 2, Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI), Part 3 – Common Specifications, TR-03110, version 2.10, 24.03.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[17] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, version 2.0, 28.08.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[18] Technische Richtlinie TR-03114 Stapelsignatur mit dem Heilberufsausweis, BSI, Version: 2.0, 22.10.2007

[19] Technische Richtlinie TR-03116, eCard-Projekte der Bundesregierung, Version 3.16 vom 07.08.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[20] Technische Richtlinie TR-03143 „eHealth G2-COS Konsistenz-Prüftool" (in Vorbereitung)

[21] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.8.0 vom 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH (Release 1.5.3)

[22] Einführung der Gesundheitskarte Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem, Version: 3.9.0 vom 24.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[23] Einführung der Gesundheitskarte Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem, Version 3.8.1 vom 30.09.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[24] Einführung der Gesundheitskarte Spezifikation der Secure Module Card SMC-B Objektsystem, Version 3.8.0 vom 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[25] Einführung der Gesundheitskarte Spezifikation der gSMC-K Objektsystem, Version 3.8.0 vom 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[26] Einführung der Gesundheitskarte Spezifikation gSMC-KT Objektsystem, Version 3.8.0 vom 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[27] Einführung der Gesundheitskarte Spezifikation Wrapper, actual version(1.7.0), gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

Cryptography

[28] ISO/IEC 7816-3: 2006 (2nd edition), Identification cards - Integrated circuit cards with contacts Part 3: Electrical interface and transmission protocols
[29] ISO/IEC 7816-4: 2013 (2nd edition) Identification cards - Integrated circuit cards - Part 4: Organisation, security and commands for interchange
[30] ISO/IEC 7816-8: 2004 (2nd edition) Identification cards - Integrated circuit cards- Part 8: Commands for security operations
[31] ISO/IEC 9796-2:2010 Information technology -- Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms
[32] ISO/IEC 9797-1 Information technology - Security techniques - Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher
[33] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001
[34] PKCS #1: RSA Cryptography Standard, RSA Laboratories, Version 2.2, October 27, 2012 (http://www.rsa.com/rsalabs/node.asp?id=2125)
[35] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[36] 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
[37] Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2011 February, 11
[38] NIST SP 800-67, Recommandation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, National Institute of Standards and Technology
[39] American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), November 16, 2005
[40] American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, November 16, 2005
[41] Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, March 2010, http://tools.ietf.org/html/rfc5639
[42] ANSI X9.62 Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005 Other Sources
[43] ISO 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards, 2000
[44] ISO 7498-2 (1989): Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture
[45] Law Governing Framework Conditions for Electronic Signatures of 16 May 2001 (Federal Law Gazette I page 876), last amended by Article 4 of the Act of 17 July 2009 (Federal Law Gazette I page 2091)

[46] Ordinance on Electronic Signature of 16 November 2001 (Federal Law Gazette I page 3074), last amended by the Act of 15 November 2010 (Federal Law Gazette I page 2631)

Additional references

[47] Joint Interpretation Library: PP0084: Changes and Compliance to PP0035 and Transition Phase, JIL application note on the transition from BSI-CC-PP-0035-2007-2007 to BSI-CC-PP-0084-2014, Version 1.1, August 2014

[48] Protection Profile Security IC Platform Protection Profile with Augmentation Packages developed by Inside Secure Infineon Technologies AG NXP Semiconductors Germany GmbH STMicroelectronics, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Version 1.0

2 TOE Overview

The TOE Overview refers to the Chapter 1.2 of the Protection Profile [BSI_PP_EHC_G2].

Target of Evaluation (TOE) and subject of this Security Target (ST) is the smartcard product "Morpho_HC_Germany_G2_COS V1" developed by Morpho (now Idemia).

The TOE is realised as Smartcard Integrated Circuit (IC with contacts) with Smartcard Embedded Software, consisting of the

Card Operating System

as intended to be used for the German Health Care System.

In particular, the TOE´s platform and its technical functionality and inherently integrated security features are designed and developed under consideration of the following specifications, standards and requirements:

- Functional and security requirements defined in the specification **[EXS_EHC_COS]** for the Card Operating System as employed within the German Health Care System
- Requirements from the Protection Profile [BSI_PP_EHC_G2]
- Requirements defined in the specification [EXS_WRP_COS] for the Wrapper.
- Technical requirements defined in ISO 7816, Parts 1, 2, 3, 4, 8, 9, 15

The TOE is intended to be used within the German Health Care System.

The TOE comprises the following components:

- Integrated Circuit (IC) with Crypto Library "Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software(firmware)" (SLE 78CFX3000P) provided by Infineon Technologies AG
- Smartcard Embedded Software comprising the Morpho_HC_Germany_G2_COS V1 as Card Operating System Card (designed as flash implementation) for the German Health Care System provided by Morpho (now Idemia)

- The wrapper for interpretation of exported TSF data
- The associated guidance documentation

The object system is not part of the TOE. Such the TOE will be configured after production as eHC by Morpho (now Idemia)/the external personalizer prior to the delivery of the smart-card plattform.

The TOE contains at its delivery unalterable identification information on the delivered configuration. Furthermore, the TOE provides authenticity information which allows an authenticity proof of the product.

A detailed overview of the different procedural variants which are supported by the product can be found in Chapter 3.4.

In order to be compliant with the requirements from the German Health Care System the TOE will be evaluated according to CC EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

The main objectives of this ST are

- to describe the TOE as a smartcard product
- to define the limits of the TOE
- to describe the assumptions, threats and security objectives for the TOE
- to describe the security requirements for the TOE
- to define the TOE security functions

2.1 Usage and Major Security Features of the TOE

This smart card provides the following main security functionality:

– authentication of human user and external devices,

– storage of and access control on user data,

– key management and cryptographic functions,

– management of TSF data including life cycle support,

– export of non-confidential TSF data of the object systems.

2.2 TOE Type

The TOE type is smart card without the application named as a whole 'Card Operating System Card Platform'.

For more information see Chapter 1.2.3 of [BSI_PP_EHC_G2].

2.3 Required Non-TOE Hardware/Software/Firmware

The TOE requires the following non-TOE hardware, software, and firmware.

The TOE is a card operating system platform which can be used in smart cards within the health care system. For the usage of this smart card an appropriate terminal resp. the health care system is necessary.

For more information see Chapter 1.2.4 of [BSI_PP_EHC_G2].

3 TOE Description

3.1 Physical Scope of the TOE

The physical interface of the TOE related to the usage as a smart card consists of the use of the following pins as described in Table 1 for communication. For details see [IC_UG].

PIN	Description
VCC	Supply voltage
GND	Ground
CLK	CLK pin provides the device with an external clock signal.
RST	This pin is used to reset the internal state of the device through a software interrupt mechanism. This pin is considered as a logical input pin and the reset mechanism is triggered by a software interrupt.
I/O	The device has two serial input/output pins IO0 and IO1 that are either driven hardware-controlled by the IART (ISO/IEC 7816 asynchronous receiver transmitter) or software-controlled by the ISO/IEC 7816 I/O control register. For IO0, the IART has priority over the I/O control register, IO1 can only be driven by the I/O control register.

Table 1: Chip pins

The Infineon M7892 B11 offers a serial communication interface fully compatible with the ISO/IEC 7816-3 standard (T=1).

For details, see [ISO_7816_3].

For this product the contactless functionality over SWIO is not supported.

3.2 Logical Scope of the TOE

The German Health Card COS (GHC) is a native smartcard operating system implementation running on a security IC.

The card operating system is instantiated with a set of applications which are defined as instantiations of the native object system managed by the operating system. The applications in the object system differ with respect to the intended use of the product in the German Health Care System. The different applications for the usage as electronic Health Card

(eHC), the Health Professional Card (HPC), or various types of Secure Module Cards (SMC), as well as customer specific additional applications are out of the scope of the card operating system implementation.

Nonetheless, the card operating system has to support the analysis and validation of object system instantiations because the overall security of a dedicated product depends on the correct instantiation of access rules and other data in the object system structures according to the requirements of the object system specifications. Therefore, the operating system provides a dedicated command interface which allows for extracting information about a loaded object system. This interface is not uniquely defined by the Gematik specifications. Thus, an additional tool the so-called "wrapper" is responsible for managing the information extraction and makes this information available to the proof tool via a standardised interface. Understandably, the transformation of the information presentation has to be correct because otherwise the application of the proof-tool may yield inconsistent conclusions about the object system properties. Therefore, the wrapper is also included in the scope of the card operating system evaluation.

The Morpho_HC_Germany_G2_COS V1 implements the standardised operational command interface (CMD_OPE) as well as a restricted set of command used in the preparative phase of the product (CMD_PREP).

This high-level command implementation is supported by additional aspects of the high-level communication protocol layers. In detail, the operating system implements:

- A strong secure messaging mechanism which allows for encrypting the communication between the card and the external world

- Support for managing logical channels (MANAGE_CHANNEL_RESTORE – command.)

- An implementation of command chaining which allows to split a large command into several data chunks that are transferred by a sequence of basic APDUs to the card

- Due to the fact that the power supply may be cut-off at any point in time, the operating system also provides a strong transaction mechanism to support the recovery of a consistent system state.

The communication itself depends on the implementation of the T=1 (contact-based) interface.

Additionally, the smart card operating system reacts on specific external event, like the first power-on (after cold reset) or a warm reset. The security IC also provides several hardware mechanisms which are capable to detect physical penetration attacks and raise security interrupts. The operating system handles these interrupts properly to enforce internally a secure operating state.

3.2.1 Overview of the Delivery Content

The TOE comprises the following parts

TOE_IC, consisting of:

- the circuitry of the chip (the integrated circuit, IC) and
- the IC Dedicated Software (including cryptolibrary CL70 used for RSA key generation) with the parts IC Dedicated Test Software and IC Dedicated Support Software

TOE_ES,

- the IC Embedded Software (operating system)

Wrapper,

- The adapter tool which has to be provided for tests of the object systems, which are loaded to the product during the product pre-personalisation phase. The Wrapper has to transform the information about the object system into a specified structure, which is used as input for an external test tool, see [EXS_WRP_COS].

and

guidance documentation delivered together with the TOE.

Note: The short terms TOE_IC and TOE_ES will be used were appropriate in the rest of this document in order to refer to these parts of the TOE.

The following table contains an overview of all deliverables associated to the TOE:

TOE component	Description / Additional Information	Type	Transfer Form
TOE_IC	Integrated Circuit (IC) with Crypto Library "Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software(firmware)" (SLE 78CFX3000P) provided by Infineon Technologies AG Detailed information on the IC Hardware, the IC Dedicated Software (in particular the Crypto Library CL70) and the IC interfaces can be found in [ST_IC] and [IC_CL_UG].	HW / SW	Delivery of not-pre-personalised / pre-personalised modules or smartcards Delivery of OS Flashing image Delivery as electronic file
TOE_ES	Smartcard Embedded Software / Part Basic Software (implemented in EEPROM/Flash of the microcontroller)	SW	
Wrapper	Wrapper for interpretation of the exported TSF data.	SW	
Note: A detailed overview of the different procedural variants which are supported by the product can be found in Chapter 3.3.			
Morpho_HC_Germany_G2_COS V1– Operational User Guidance	User guidance for the User of the GHC G2 COS V1.0 platform	DOC	Document in paper / electronic form
Morpho_HC_Germany G2_COS V1– OS Preparation Guidance	User guidance for the Pre-Personaliser/Personaliser of the gHC Card	DOC	Document in paper / electronic form

TOE component	Description / Additional Information	Type	Transfer Form
Morpho_HC_Germany_G2_COS V1– Object System Preparation Guidance			
Morpho_HC_Germany_G2_COS V1 – Data Sheet	Data Sheet with information on the actual identification data and configuration of the gHC Card delivered to the customer	DOC	Document in paper / electronic form
Morpho_HC_Germany_G2_COS V1 –Wrapper Guidance	Guidance for the User of Wrapper.	DOC	Document in paper / electronic form
Aut-Key of the gHC Card	Public part of the authentication key pair relevant for the authenticity of the gHC Card Note: The card´s authentication key pair is generated by Morpho (now Idemia) and depends on the TOE´s configuration delivered to the customer. Furthermore, the key pair may be chosen customer specific.	KEY	Document in paper form / electronic file
Perso-Key of the gHC Card	Personalisation key relevant for the product personalisation of the gHC Card Note: The card´s personalisation key pair is generated by Morpho (now Idemia) and depends on the TOE´s configuration delivered to the customer. Furthermore, the key may be chosen customer specific.	KEY	Document in paper form / electronic file

TOE component	Description / Additional Information	Type	Transfer Form
Object System Signature Key	Object System Signature Key, needed for calculation of the Signature over an Object System.	KEY	Document in paper / electronic file

Note: Deliverables in paper form require a personal passing on or a procedure of at least the same security. For deliverables in electronic form integrity and authenticity attribute will be attached.

3.3 Life Cycle Overview

This chapter describes the details of the life-cycle model of a German Health Card product developed by Morpho (now Idemia). The description is based on a generic life-cycle model used by Morpho (now Idemia) which is compliant to the standard life-cycle models defined by various protection profiles, but which models the different development and production processes more precisely to address different product types.

The subsequent sections will detail which of the general development and production steps are relevant for this German Health Card Operating System and define the points-of-delivery of the product.

For the Morpho_HC_Germany_G2_COS V1 product the generic Morpho (now Idemia) life-cycle model is instantiated as follows:

The product is a flash-product so that the loading of the operating system can be an own step separated from the manufacturing of the IC. This depends on the chosen production variant which can address other OS Flash loading entities than the IC Manufacturer. The subsequent Product Pre-Personalisation and Product Personalisation are out of the scope of the evaluation. Therefore, the point of delivery is the delivery to the Product Pre-Personaliser, who receives the product as a flashed IC from the flash-loading facility and pre-personalisation data from the Morpho (now Idemia) R&D. The pre-personalisation data is required to load specific object system instantiations onto the card. Between the OS Flashing and the Product Pre-Personalisation there is an intermediate step for additional OS configuration called OS PrePersonalisation which is includes the import of additional key material. According to the production variant this role as OS PrePersonliser is covered by the

OS Flash Loader or Product Pre-Personaliser. Compared to the Morpho (now Idemia) generic life-cycle model, several external processes are not applicable or not supported

- There is no *External Applet Development* because the product is not an open platform. There is no *Import from External Development Support processes*

- The *Embedded Software Development* is done by the Morpho (now Idemia) R&D centres. It is supported by external IC dedicated software development which is part of the *Base Evaluation*.

- *In-Field Loading of Software Updates* is not supported by the product, because this feature is explicitly prohibited by the evaluation concept of the BSI.

- The *Export to External Development Support* processes subsume activities which support the qualification of the product. These activities handle usually not the final product, but test configurations with slightly different properties, in order to support the functional qualification of the final product by external approval bodies. For example, acceptance tests in the customer infrastructure or external approval at accredited laboratories fall into this category.

The development support activities are not an integral part of the sensitive product development. Furthermore, they do not handle the final product but some dedicated test or sample configurations so that the interfaces are not TOE delivery points. However, we treat these process blocks like external processes and cover their analysis by:

- the identification of the required delivery and acceptance procedures in the secure R&D within the life-cycle definition of the product in this document

- the identification of the handling requirements for all of the external processes in terms of dedicated guidance documents.

For the Morpho_HC_Germany_G2_COS V1 product there are different possible technical and procedural production variants according to the generic life-cycle model.

3.4 Product Pre-Personalisation and Personalisation

The Product Pre-Personalisation phase loads the object system with the card non individual data onto the card. After the phase has been successfully completed the product enters the personalisation mode in which individual data may be stored but no further extensions of the object system are possible. During Product Personalisation the card individual data can be stored by the Product Personaliser. The product supports the secure Product Personalisation via a secured channel.

Related to the chosen production variant of the TOE the OS PrePersonalisation is done as intermediate step before the Product Pre-Personalisation. In this case the Product Pre-Personaliser can exchange the initial key material for personalisation with its own.

3.5 Definition of the Evaluation Scope

The other process blocks identified in the detailed German Health Card G2 COS life-cycle model are out of the evaluation scope and covered by an assessment of the corresponding guidance documentation or by dedicated baseline evaluations. The IC and crypto lib development as well as the IC Production and Pre-Personalisation is covered by the underlying IC evaluations conducted by the IC vendor. This in particular includes the processes for secured secret exchange and handling, because the exchange of the secrets between the IC Manufacturer and the software developer is the security anchor for whole evaluated flash-loading process. This in particular implies that all required processes for handling the sensitive key material at the IC Manufacturer site are in place and trusted.

3.6 Delivery of the Certified Product

The certified product is delivered in the following delivery package which is defined by the delivery point:

- to an external Pre-Personaliser as a non-pre-personalised smartcard or module with the dedicated load files, the product data sheet, and the guidance for the Pre-Personaliser and the Personaliser. Furthermore, the delivery contains key material required for conducting the Product Pre-Personalisation/Personalisation.

Additionally, Morpho (now Idemia) may ship the product

- to an external Product Personaliser as pre-personalised smartcard or module, the product data sheet and the guidance for the Product Personaliser. Furthermore, the delivery contains key material required for conducting the Personalisation. This is the case if Morpho (now Idemia) conducts the Product Pre-Personalisation.

- to the smartcard issuer as a pre-personalised and personalised smartcard. In this case, only the operational guidance is shipped additionally to the issuer. This is the case if Morpho (now Idemia) also conducts the Product Personalisation

Furthermore, the following delivery procedures are also relevant for the product and considered during the life-cycle assessment:

- The delivery of the Crypto Library Components from Infineon Technologies AG to Morpho (now Idemia).

- The delivery of the OS Flash data from Morpho (now Idemia) to Infineon Technologies AG for flash loading. Additionally, personalisation key data is shipped in this step.

3.7 TOE Intended Usage

Introducing information on the intended usage of the TOE is given within Chapter 2. The present chapter will provide additional and more detailed information on the Operating System platform residing on the card at delivery time point.

In general, the Morpho_HC_Germany_G2_COS V1 is designed as multifunctional platform for high security applications. Therefore, the TOE provides an Operating System platform with a wide range of technical functionality and an adequate set of inherently integrated security features.

The Morpho_HC_Germany_G2_COS V1 supports the following services:

- On-card-generation of RSA and ELC key pairs of high quality (with appropriate key lengths)
- Different signature schemes (based on RSA and ELC with appropriate key lengths and padding schemes)
- Different encryption schemes (based on DES, AES and RSA with appropriate key lengths and padding schemes)
- Key derivation schemes
- PIN based authentication scheme (with support of multi reference PINs)
- Different key based authentication schemes (based on AES, DES, ELC and RSA, with / without session key agreement)
- Hash value calculation
- Random number generation of high quality
- Calculation and verification of cryptographic checksums
- Verification of CV certificates
- Protection of the communication between the TOE and the external world against disclosure and manipulation (Secure Messaging)
- Protection of files and data by access control functionality
- Life-cycle state information related to the Operating System itself as well as to all objects processed by the card
- Confidentiality of cryptographic keys, PINs and further security critical data
- Integrity of cryptographic keys, PINs and further security critical data
- Confidentiality of operating system code and its internal data
- Integrity of operating system code and its internal data (self-test func tionality)
- Resistance of crypto functionality against Side Channel Analysis (SPA, DPA, TA, DFA)
- Card management functionality
- Channel management (with separation of channel related objects)

To support the security of the above mentioned features of the TOE, the Morpho_HC_Germany_G2_COS V1 provides appropriate countermeasures for resistance especially against the following attacks:

- Cloning of the product

- Unauthorised disclosure of confidential data (during generation, storage and processing)
- Unauthorised manipulation of data (during generation, storage and pro cessing)
- Identity usurpation
- Forgery of data to be processed
- Derivation of information on the private key from the related public part for on-card-generated RSA and ELC key pairs
- Side Channel Attacks

The resistance of the TOE against such attack scenarios is reached by usage of appropriate security features already integrated in the underlying IC as well as by implementing additional appropriate software countermeasures.

3.8 Role Mapping to Production Roles

According to the TOE Description there are different life-cycle-phases mentioned which refer to specific roles of responsibilities. Each step is related to a single role which is now mapped to role definitions of external entities listed in this security target. The definition of the external entity variants are defined in the protection profile **[BSI_PP_EHC_G2]**.

External Entity	Role	Production Step
(not in scope of external entity; secured entity under own certificates)	IC Manufacturer	IC Manufacturing
(not in scope of external entity)	Developer of Card Products	Before Product Pre-Personalisation
Device	OS FlashLoader	OS Flashing
Device	OS PrePersonaliser	OS PrePersonalisation (coupled with OS Flashing or Product Pre-Personalisation)
Device	OS Personaliser	Product Pre-Personalisation (Object System PrePersonalisation)
Device	OS Personaliser	Product Personalisation (Object System Personalisation)
Human User	Card Holder	--- In Field Usage (no production step)
World	User of Wrapper	Verification according to Technical Guidance TR-03143 (no production step)

4 Common Criteria Conformance Claims

4.1 Common Criteria conformance

This security target claims conformance to

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

as follows

- Part 2 extended,
- Part 3 conformant,

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

is taken into account.

4.2 Protection Profile claim

This Security Target claims strict conformance with the following Protection Profiles:

Common Criteria Protection Profile Card Operating System Generation 2 (PP COS G2) [BSI_PP_EHC_G2].

4.3 Package claim

The security target is conformant to the following security requirements package: Assurance package EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 as defined in the CC, Part 3.The TOE includes no optional package described in Chapter 1.2.4 of the PP [BSI_PP_EHC_G2].

4.4 Assurance package claim

The set of assurance requirements is the package EAL4+ augmented by:

- ALC_DVS.2, "*Sufficiency of security measures"*
- ATE_DPT.2, "*Testing: security enforcing modules*"
- AVA_VAN.5, "*Advanced methodical vulnerability analysis"*

Assurance requirements are split in two packages, one for the TOE itself and one for its development environment, allowing for separate package assessment. However, both assessments must be combined in order to fulfil the whole set of PP assurance requirements.

In order to avoid redundancy and to minimize the evaluation efforts, the evaluation of the TOE will be conducted as a composite evaluation and will make use of the evaluation results of the CC evaluation of the underlying semiconductor "Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software(firmware)" provided by Infineon Technologies AG. The IC incl. its IC Dedicated Software is evaluated according to Common Criteria EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5. The certification number of the IC is BSI-DSZ-CC-0782-V2-2015.

4.5 Conformance rationale

This variant of the COS includes no optional packages described in [BSI_PP_EHC_G2]. The assets, threats, OSPs, assumptions, statements of SPD, security objectives and security requirements of the optional packages are out of scope.

4.5.1 TOE type consistency

The TOE type is smart card without the application named as a whole 'Card Operating System Card' with is consistent to the [BSI_PP_EHC_G2].

4.5.2 SPD statement consistency

All assets and threats are identical to those in the PP [BSI_PP_EHC_G2].

All OSPs are identical to those in the PP [BSI_PP_EHC_G2].

All assumptions in this ST are identical to those in the PP [BSI_PP_EHC_G2].

The statement of SPD is therefore consistent with those stated in the PPs.

4.5.3 Security Objectives statement consistency

The TOE security objectives are a superset of those in the PP [BSI_PP_EHC_G2]. Actually, all the TOE security objectives from the PP are copied in the ST.

All security objectives for the environment in this ST are identical to those in the PP [BSI_PP_EHC_G2]

4.5.4 Security Requirements statement consistency

The set of SFRs is a superset of those which are mandatory in the PP [BSI_PP_EHC_G2]. Actually, all the taken SFRs from the PP are refined in the ST.

Regarding SARs consistency, the ST and the PP share the same assurance level, which is EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

5 Security Problem Definition

5.1 Assets

User Data stored in EF

Data for the user stored in elementary files of the file hierarchy.

Secret Keys

Symmetric cryptographic key generated as result of mutual authentication and used for encryption and decryption of user data.

Private keys

Confidential asymmetric cryptographic key of the user used for decryption and computation of digital signature.

Public keys

Integrity protected public asymmetric cryptographic key of the user used for encryption and verification of digital signatures and permanently stored on the TOE or provided to the TOE as parameter of the command.

5.2 Users / Subjects

World

Any user independent on identification or successful authentication.

Human User

A person authenticated by password or PUC.

Device

An external device authenticated by cryptographic operation

5.3 Threats

The following threats are defined in the BSI-CC-PP-0035-2007 [11]: T.Leak-Inherent, T.Phys-Probing, T.Malfunction, T.Phys-Manipulation, T.Leak-Forced, T.Abuse-Func, T.RND. All threats are part of this Protection Profile and taken over into this PP.

5.3.1 Security IC Platform Protection Profile

T.Leak-Inherent

Inherent Information Leakage

For more information see paragraph 78 of [BSI_PP_IC].

T.Phys-Probing

Physical Probing

For more information see paragraph 79 of [BSI_PP_IC].

T.Malfunction

Malfunction due to Environmental Stress

For more information see paragraph 80 of [BSI_PP_IC].

T.Phys-Manipulation

Physical Manipulation

For more information see paragraph 81 of [BSI_PP_IC].

T.Leak-Forced

Forced Information Leakage

For more information see paragraph 82 of [BSI_PP_IC].

T.Abuse-Func

Abuse of Functionality

For more information see paragraph 83 of [BSI_PP_IC].

T.RND

Deficiency of Random Numbers

For more information see paragraph 84 of [BSI_PP_IC].

5.3.2 Card Operating System Generation 2 Protection Profile

T.Forge_Internal_Data

Forge of User or TSF data

An attacker with high attack potential tries to forge internal user data or TSF data.

For more information see paragraph 40 of [BSI_PP_EHC_G2].

T.Compromise_Internal_Data

Compromise of confidential User or TSF data

An attacker with high attack potential tries to compromise confidential user data or TSF data through the communication interface of the TOE.

For more information see paragraph 41 of [BSI_PP_EHC_G2].

T.Malicious_Application

Malicious Application

An attacker with high attack potential tries to use the TOE functions to install an additional malicious application in order to compromise or alter User Data or TSF data.

For more information see paragraph 43 of [BSI_PP_EHC_G2].

T.Misuse

Misuse of TOE functions

An attacker with high attack potential tries to use the TOE functions to gain access to the access control protected assets without knowledge of user authentication data or any implicit authorization.

For more information see paragraph 42 of [BSI_PP_EHC_G2].

T.Crypto

Cryptographic attack against the implementation

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.

For more information see paragraph 44 of [BSI_PP_EHC_G2].

T.Intercept

Interception of Communication

An attacker with high attack potential tries to intercept the communication between the TOE and an external entity, to forge, to delete or to add other data to the transmitted sensitive data.

For more information see paragraph 45 of [BSI_PP_EHC_G2].

T.WrongRigths

Wrong Access Rights for User Data or TSF Data

An attacker with high attack potential executes undocumented or inappropriate access rights defined in object system and compromises or manipulate sensitive User data or TSF data.

For more information see paragraph 46 of [BSI_PP_EHC_G2].

5.4 Organisational Security Policies

5.4.1 Security IC Platform Protection Profile

P.Process-TOE

Protection during TOE Development and Production

For more information see paragraph 86 of [BSI_PP_IC].

5.5 Assumptions

5.5.1 Security IC Platform Protection Profile

A.Plat-Appl

Usage of Hardware Platform

For more information see paragraph 93 of [BSI_PP_IC].

Removed.

Usage of Hardware Platform as TOE of BSI-CC-PP-0035-2007 as addressed by A.Plat-Appl is covered by ADV class related to COS as part of the current TOE.

A.Resp-Appl

Treatment of User Data

For more information see paragraph 95 of [BSI_PP_IC].

Refined by A.Resp-ObjS

The user data of the TOE of BSI-CC-PP-0035-2007 are the Security IC Embedded Software, i.e. the COS part of the TOE, the TSF data of the current TOE and the user data of the COS. The object system contains the TSF data and defines the security attributes of the user data of the current TOE.

A.Process-Sec-IC

Protection during Packaging, Finishing and Personalisation

For more information see paragraph 91 of [BSI_PP_IC].

Refined by A.Process-Sec-SC.

While the TOE of BSI-CC-PP-0035-2007 is delivered after Phase 3 IC manufactioring and Testing or Phase or Phase 4 IC Packaging the current TOE is delivered after Phase 5 Composite Product Integration before Phase 6 Personalisation. The protection during Phase 4 may and during Phase 5 shall be addressed by security of the development environment of the current TOE. Only protection during Personalisation is in responsibility of the operational environment.

5.5.2 Card Operating System Generation 2 Protection Profile

A.Plat-COS

Usage of COS

An object system designed for the TOE meets the following documents: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the user guidance, and the application notes, and (ii) findings of the TOE evaluation reports relevant for the COS as documented in the certification report.

For more information see paragraph 52 of [BSI_PP_EHC_G2].

A.Resp-ObjS

Treatment of User Data by the Object System

All User Data and TSF Data of the TOE are treated in the object system as defined for its specific application context.

This assumption refines the A.Plat-Appl.

For more information see paragraph 53 of [BSI_PP_EHC_G2].

A.Process-Sec-SC

Protection during Personalisation

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

This assumption refines the A.Process-Sec-IC.

For more information see paragraph 51 of [BSI_PP_EHC_G2].

6 Security Objectives

6.1 Security Objectives for the TOE

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

For more information see Chapter 4.1 of [BSI_PP_IC].

6.1.1 Security IC Platform Protection Profile

O.Identification

TOE Identification

For more information see paragraph 106 of [BSI_PP_IC].

O.Leak-Inherent

Protection against Inherent Information Leakage

For more information see paragraph 100 of [BSI_PP_IC].

O.Phy-Probing

Protection against Physical Probing

For more information see paragraph 101 of [BSI_PP_IC].

O.Malfunction

Protection against Malfunctions

For more information see paragraph 102 of [BSI_PP_IC].

O.Phys-Manipulation

Protection against Physical Manipulation

For more information see paragraph 103 of [BSI_PP_IC].

O.Leak-Forced

Protection against Forced Information Leakage

For more information see paragraph 104 of [BSI_PP_IC].

O.Abuse-Func

Protection against Abuse of Functionality

For more information see paragraph 105 of [BSI_PP_IC].

O.RND

Random Numbers

For more information see paragraph 107 of [BSI_PP_IC].

The following Application Note was respected in the way indicated in **[bold print]***:*

"*If the TOE provides further services to the Security IC Embedded Software (such as cryptographic functions) this may result in having additional security objectives in the Security Target. Add further security objectives in the Security Target if this Protection Profile is augmented.***[no augmentation of the PP]**"

6.1.2 Card Operating System Generation 2 Protection Profile

This security objectives are conformant to the description in Chapter 4 of [BSI_PP_EHC_G2].

O.Integrity

Integrity of internal data

The TOE must ensure the integrity of the User Data, the security services and the TSF data under the TSF scope of control.

O.Confidentiality

Confidentiality of internal data

The TOE must ensure the confidentiality of private keys and other confidential User Data and confidential TSF data especially the authentication data, under the TSF scope of control against attacks with high attack potential.

O.Resp-COS

Treatment of User and TSF Data

The User Data and TSF data (especially cryptographic keys) are treated by the COS as defined by the TSF data of the object system.

O.TSFDataExport

Support of TSF data export

The TOE must provide correct export of TSF data of the object system excluding confidential TSF data for external review.

O.Authentication

Authentication of external entities

The TOE supports the authentication of human users and external devices. The TOE is able to authenticate itself to external entities.

O.AccessControl

Access Control for Objects

The TOE must enforce that only authenticated entities with sufficient access control rights can access restricted objects and services. The access control policy of the TOE must bind the access control right of an object to authenticated entities. The TOE must provide management functionality for access control rights of objects.

O.KeyManagement

Generation and import of keys

The TOE must enforce the secure generation, import, distribution, access control and destruction of cryptographic keys. The TOE must support the public key import from and export to a public key infrastructure.

O.Crypto

Cryptographic functions

The TOE must provide cryptographic services by implementation of secure cryptographic algorithms for hashing, key generation, data confidentiality by symmetric and asymmetric encryption and decryption, data integrity protection by symmetric MAC and asymmetric signature algorithms, and cryptographic protocols for symmetric and asymmetric entity authentication.

O.SecureMessaging

Secure messaging

The TOE supports secure messaging for protection of the confidentiality and the integrity of the commands received from successful authenticated device and sending responses to this device on demand of the external application. The TOE enforces the use of secure messaging for receiving commands if defined by access condition of an object.

6.2 Security objectives for the Operational Environment

Note: For more information see Chapter 4.2 of [BSI_PP_EHC_G2].

6.2.1 Security IC Platform Protection Profile

OE.Plat-Appl

Usage of Hardware Platform

For more information see paragraph 109 of [BSI_PP_IC].

Removed.

OE.Plat-Appl requires the Security IC Embedded Software to meet the guidance documents of the Security IC. The Security IC Embedded Software is part of the current TOE. This requirement shall be fulfilled in the development process of the TOE.

OE.Resp-Appl

Treatment of User Data

For more information see paragraph 110 of [BSI_PP_IC], refined by "OE.Resp-ObjS".

OE.Resp-Appl requires the Security IC Embedded Software to treat the user data as required by the security needs of the specific application context. This security objective shall be ensured by the TOE and the object system.

OE.Process-Sec-IC

Protection during composite product manufacturing

For more information see paragraph 111 of [BSI_PP_IC].

Refined by OE.Process-Card.

The policy defined for the Security platform IC is extended to the current TOE.

6.2.2 Card Operating System Generation 2 Protection Profile

OE.Plat-COS

Usage of COS

For detailed information see paragraph 69 of [BSI_PP_EHC_G2].

OE.Resp-ObjS

Treatment of User Data

This security objective refines OE.Resp-Appl.

For detailed information see paragraph 70 of [BSI_PP_EHC_G2].

OE.Process-Card

Protection of Smartcard during Personalisation

This security objective refines OE.Process-Sec-IC.

For detailed information see paragraph 71 of [BSI_PP_EHC_G2].

6.3 Security Objectives Rationale

6.3.1 Threats

6.3.1.1 Security IC Platform Protection Profile

T.Leak-Inherent This thread is directly addressed by the security objective O.Leak-Inherent. For more information see paragraph 122 of [BSI_PP_IC].

T.Phys-Probing This thread is directly addressed by the security objective O.Phy-Probing. For more information see paragraph 122 of [BSI_PP_IC].

T.Malfunction This thread is directly addressed by the security objective O.Malfunction. For more information see paragraph 122 of [BSI_PP_IC].

T.Phys-Manipulation This thread is directly addressed by the security objective O.Phys-Manipulation. For more information see paragraph 122 of [BSI_PP_IC].

T.Leak-Forced This thread is directly addressed by the security objective O.Leak-Forced. For more information see paragraph 122 of [BSI_PP_IC].

T.Abuse-Func This thread is directly addressed by the security objective O.Abuse-Func. For more information see paragraph 122 of [BSI_PP_IC].

T.RND This thread is directly addressed by the security objective O.RND. For more information see paragraph 122 of [BSI_PP_IC].

6.3.1.2 Card Operating System Generation 2 Protection Profile

T.Forge_Internal_Data The thread T.Forge_Internal_Data addresses the falsification of internal user data or TSF data by an attacker. This is prevented by O.Integrity that ensures the integrity of user data, the security services and the TSF data. Also, O.Resp-COS addresses this thread because the user data and TSF data are treated by the TOE as defined by the TSF data of the object system.

T.Compromise_Internal_Data The thread T.Compromise_Internal_Data addresses the disclosure of confidential user data or TSF data by an attacker. The

security objective O.Resp-COS requires that the user data and TSF data are treated by the TOE as defined by the TSF data of the object system. Hence, the confidential data are handled correctly by the TSF. The security objective O.Confidentiality ensures the confidentiality of private keys and other confidential TSF data. O.KeyManagement requires that the used keys to protect the confidentiality are generated, imported, distributed, managed and destroyed in a secure way.

T.Malicious_Application The thread T.Malicious_Application addresses the modification of user data or TSF data by the installation and execution of a malicious code by an attacker. The security objective O.TSFDataExport requires the correct export of TSF data in order to prevent the export of code fragments that could be used for analysing and modification of TOE code. O.Authentication enforces user authentication in order to control the access protected functions that could be (mis)used to install and execute malicious code. Also, O.AccessControl requires the TSF to enforce an access control policy for the access to restricted objects in order to prevent unauthorised installation of malicious code.

T.Misuse The thread T.Misuse addresses the usage of access control protected assets by an attacker without knowledge of user authentication data or by any implicit authorization. This is prevented by the security objective O.AccessControl that requires the TSF to enforce an access control policy for the access to restricted objects. Also the security objective O.Authentication requires user authentication for the use of protected functions.

T.Crypto The thread T.Crypto addresses a cryptographic attack to the implementation of cryptographic algorithms or the guessing of keys using brute force attacks. This thread is directly covered by the security objective O.Crypto which requires a secure implementation of cryptographic algorithms.

T.Intercept The thread T.Intercept addresses the interception of the communication between the TOE and an external entity by an attacker. The attacker tries to delete, add or forge transmitted data. This thread is directly addressed by the security objective O.SecureMessaging which requires the TOE to establish a trusted channel that protects the confidentiality and integrity of the transmitted data between the TOE and an external entity.

T.WrongRigths The thread T.WrongRights addresses the compromising or manipulation of sensitive user data or TSF data by using undocumented or inappro-

priate access rights defined in the object system. This thread is addressed by the security objective O.Resp-COS which requires the TOE to treat the user data and TSF data as defined by the TSF data of the object system. Hence the correct access rights are always used and prevent misuse by undocumented or inappropriate access rights to that data.

6.3.2 Organisational Security Policies

6.3.2.1 Security IC Platform Protection Profile

P.Process-TOE The OSP P.Process-TOE addresses the protection during TOE development and production as defined in BSI-CC-PP-0035-2007 [11]. This is supported by the security objective for the operational environment OE.Process-Card that addresses the TOE after the delivery for phase 5 up to 7: It requires that end consumers maintain the confidentiality and integrity of the TOE and its manufacturing and test data.

P.Process-TOE is extended for this TOE. For more information see paragraph 77, 78 and 89 of [BSI_PP_EHC_G2].

According to paragraph 118 of [BSI_PP_IC] the IC related parts of P.Process-TOE are covered by the IC related security objective O.Identification.

6.3.3 Assumptions

6.3.3.1 Security IC Platform Protection Profile

A.Plat-Appl The assumption A.Plat-Appl assumes that the Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report. This is met by the SAR of ADV class and the requirements for composite evaluation [8].

For more information see paragraph 75 of [BSI_PP_EHC_G2].

The IC related A.Plat-Appl addresses the IC related operational environment OE.Plat-Appl.

For more information see paragraph 112 of [BSI_PP_IC].

A.Resp-Appl The assumption A.Resp-Appl assumes that security relevant user data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context. This assumption is split into requirements for the COS part of the TSF to provide appropriate security functionality for the specific application context as defined by SFR of the current PP and the assumption A.Resp-ObjS that assumes all User Data and TSF Data of the TOE are treated in the object system as defined for its specific application context. The security objective for the operational environment OE.Resp-Obj requires the object system to be defined as required by the security needs of the specific application context.

For more information see paragraph 76 of [BSI_PP_EHC_G2].

The IC related A.Resp-Appl addresses the IC related operational environment OE.Resp-Appl.

For more information see paragraph 112 of [BSI_PP_IC].

A.Process-Sec-IC The assumption A.Process-Sec-IC assumes and OE.Process-Sec-IC requires that security procedures are used after delivery of the IC by the IC Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

OE.Process-Sec-IC is refined by OE.Process-Card.

For more information see paragraph 74 of [BSI_PP_EHC_G2].

6.3.3.2 Card Operating System Generation 2 Protection Profile

A.Plat-COS The assumption A.Plat-COS assumes that the object system of the TOE is designed according to dedicated guidance documents and according to relevant findings of the TOE evaluation reports. This assumption is directly addressed by the security objective for the operational environment OE.Plat-COS.

For more information see paragraph 87 of [BSI_PP_EHC_G2].

A.Resp-ObjS The assumption A.Resp-ObjS assumes that all user data and TSF data are treated by the object system as defined for its specific application context. This assumption is directly addressed by the security objective for the operational environment OE.Resp-ObjS.

For more information see paragraph 88 of [BSI_PP_EHC_G2].

A.Process-Sec-SC The A.Process-Sec-SC assumes and OE.Process-Sec-Card requires security procedures during Phase 6 Smartcard personalisation up to the delivery of the smartcard to the end-user.

Requirements of OE.Process-Sec-Card are covered by OE.Process-Card.

For more information see paragraph 74 of [BSI_PP_EHC_G2].

6.3.4 Security objectives for the Operational Environment

6.3.4.1 Security IC Platform Protection Profile

OE.Plat-Appl Since OE.Plat-Appl requires the Security IC Embedded Software developer to implement those measures assumed in A.Plat-Appl, the assumption is covered by the security objective, see paragraph 114 of [BSI_PP_IC].

OE.Resp-Appl Since OE.Resp-Appl requires the developer of the Security IC Embedded Software to implement measures as assumed in A.Resp-Appl, the assumption is covered by the security objective, see paragraph 116 of [BSI_PP_IC].

OE.Process-Sec-IC Since OE.Process-Sec-IC requires the Composite Product Manufacturer to implement those measures assumed in A.Process-Sec-IC, the assumption is covered by this security objective, see paragraph 120 of [BSI_PP_IC].

6.3.4.2 Card Operating System Generation 2 Protection Profile

OE.Process-Card OE.Process-Card requires the protection during Personalisation assumed in P.Process-TOE, the assumption is supported by this security objective, see paragraph 73 and 74 of [BSI_PP_EHC_G2].

OE.Process-Card requires the protection during Personalisation of the smart card which is also required by OE.Process-Sec-Card. So OE.Process-Card covers requirements of OE.Process-Sec-Card which is used for the Security Objective Rationale related to the IC platform, see paragraph 89 of [BSI_PP_EHC_G2]. OE.Process-Sec-Card requires security procedures assumed by A.Process-Sec-SC.

OE.Process-Card refines the IC related OE.Process-Sec-IC, which requires security procedures assumed by A.Process-Sec-IC.

OE.Process-Sec-IC defined in the BSI-CC-PP-0035-2007 is completely ensured by the assurance class ALC of the TOE up to Phase 5 and addressed by OE.Process-Card. See chapter 4 of [BSI_PP_EHC_G2] for more details.

6.3.5 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Leak-Inherent	O.Leak-Inherent	Section 6.3.1
T.Phys-Probing	O.Phy-Probing	Section 6.3.1
T.Malfunction	O.Malfunction	Section 6.3.1
T.Phys-Manipulation	O.Phys-Manipulation	Section 6.3.1
T.Leak-Forced	O.Leak-Forced	Section 6.3.1
T.Abuse-Func	O.Abuse-Func	Section 6.3.1
T.RND	O.RND	Section 6.3.1
T.Forge_Internal_Data	O.Integrity, O.Resp-COS	Section 6.3.1
T.Compromise_Internal_Data	O.Confidentiality, O.Resp-COS, O.KeyManagement	Section 6.3.1
T.Malicious_Application	O.Authentication, O.AccessControl, O.TSFDataExport	Section 6.3.1
T.Misuse	O.Authentication, O.AccessControl	Section 6.3.1
T.Crypto	O.Crypto	Section 6.3.1
T.Intercept	O.SecureMessaging	Section 6.3.1
T.WrongRigths	O.Resp-COS	Section 6.3.1

Table 2 Threats and Security Objectives - Coverage

Security Objectives	Threats	
O.Identification		
O.Leak-Inherent	T.Leak-Inherent	
O.Phy-Probing	T.Phys-Probing	
O.Malfunction	T.Malfunction	
O.Phys-Manipulation	T.Phys-Manipulation	
O.Leak-Forced	T.Leak-Forced	
O.Abuse-Func	T.Abuse-Func	
O.RND	T.RND	
O.Integrity	T.Forge_Internal_Data	
O.Confidentiality	T.Compromise_Internal_Data	
O.Resp-COS	T.Forge_Internal_Data, T.Compromise_Internal_Data, T.WrongRigths	
O.TSFDataExport	T.Malicious_Application	
O.Authentication	T.Malicious_Application, T.Misuse	
O.AccessControl	T.Malicious_Application, T.Misuse	
O.KeyManagement	T.Compromise_Internal_Data	
O.Crypto	T.Crypto	
O.SecureMessaging	T.Intercept	
OE.Plat-Appl		
OE.Resp-Appl		
OE.Process-Sec-IC		
OE.Plat-COS		

Security Objectives	Threats	
OE.Resp-ObjS		
OE.Process-Card		

Table 3 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.Process-TOE	O.Identification, OE.Process-Card	Section 6.3.2

Table 4 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies	Rationale
O.Identification	P.Process-TOE	
O.Leak-Inherent		
O.Phy-Probing		
O.Malfunction		
O.Phys-Manipulation		
O.Leak-Forced		
O.Abuse-Func		
O.RND		
O.Integrity		
O.Confidentiality		
O.Resp-COS		
O.TSFDataExport		
O.Authentication		
O.AccessControl		
O.KeyManagement		
O.Crypto		
O.SecureMessaging		
OE.Plat-Appl		
OE.Resp-Appl		
OE.Process-Sec-IC		
OE.Plat-COS		
OE.Resp-ObjS		
OE.Process-Card	P.Process-TOE	Section 6.3.4

Table 5 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.Plat-Appl	OE.Plat-Appl	Section 6.3.3
A.Resp-Appl	OE.Resp-Appl	Section 6.3.3
A.Process-Sec-IC	OE.Process-Card, OE.Process-Sec-IC	Section 6.3.3
A.Plat-COS	OE.Plat-COS	Section 6.3.3
A.Resp-ObjS	OE.Resp-ObjS	Section 6.3.3
A.Process-Sec-SC	OE.Process-Card	Section 6.3.3

Table 6 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions	Rationale
OE.Plat-Appl	A.Plat-Appl	Section 6.3.4
OE.Resp-Appl	A.Resp-Appl	Section 6.3.4
OE.Process-Sec-IC	A.Process-Sec-IC	Section 6.3.4
OE.Plat-COS	A.Plat-COS	
OE.Resp-ObjS	A.Resp-ObjS	
OE.Process-Card	A.Process-Sec-IC, A.Process-Sec-SC	Section 6.3.4

Table 7 Security Objectives for the Operational Environment and Assumptions - Coverage

7 Extended Requirements

7.1 Extended Families

7.1.1 Extended Family FCS_RNG - Generation of Random Numbers

7.1.1.1 Description

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

7.1.1.2 Extended Components

Extended Component FCS_RNG.1

Description

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

Definition

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid] 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].

Dependencies: No dependencies.

7.1.2 Extended Family FMT_LIM - Limited capabilities and availability

7.1.2.1 Description

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 component Limited Capability of this family requires the functions themselves to be designed in a specific manner.

7.1.2.2 Extended Components

Extended Component FMT_LIM.2

Description

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.

Definition

FMT_LIM.2 Limited availability

FMT_LIM.2.1 The TSF shall be designed in a manner that limits its availability so that in conjunction with"Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: Limited capability and availability policy].

Dependencies: (FMT_LIM.1)

Extended Component FMT_LIM.1

Description

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

Definition

FMT_LIM.1 Limited capabilities

FMT_LIM.1.1 The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with"Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: Limited capability and availability policy].

Dependencies: (FMT_LIM.2)

7.1.3 Extended Family FAU_SAS - Audit data storage

7.1.3.1 Description

This family defines functional requirements for the storage of audit data.

7.1.3.2 Extended Components

Extended Component FAU_SAS.1

Description

Requires the TOE to provide the possibility to store audit data.

Definition

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide [assignment: list of subjects] with the capability to store [assignment: list of audit information] in the [assignment: type of persistent memory].

Dependencies: No dependencies.

7.1.4 Extended Family FPT_EMS - TOE Emanation

7.1.4.1 Description

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. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of 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 being not directly addressed by any other component of CC part 2 [2].

7.1.4.2 Extended Components

Extended Component FPT_EMS.1

Description

Emanation of TSF and User data, defines limits of TOE emanation related to TSF and User data.

Definition

FPT_EMS.1 Emanation of TSF and User data

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].

Dependencies: No dependencies.

7.1.5 Extended Family FIA_API - Authentication Proof of Identity

7.1.5.1 Description

This family defines functions provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment.

7.1.5.2 Extended Components

Extended Component FIA_API.1

Description

Authentication Proof of Identity, provides prove of the identity of the TOE to an external entity.

Definition

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or rule].

Dependencies: No dependencies.

7.1.6 Extended Family FPT_ITE - FPT_ITE TSF image export

7.1.6.1 Description

The family FPT_ITE (TSF image export) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. This family defines rules for fingerprints of TOE implementation and export of TSF data in order to allow verification of their correct implementation in the TOE. The export of a fingerprint of the TOE implementation, e.g. a keyed hash value over all implemented executable code, provides the ability to compare the implemented executable code with the known intended executable code. The export of all non-confidential TSF data, e.g. data security attributes of subjects and objects and public authentication verification data like public keys, provides the ability to verify their correctness e.g. against a specification. The exported TSF images must be correct, but do not need protection of confidentiality or integrity if the export is performed in a protected environment. This family describes the functional requirements for unprotected export of TSF data and export of TOE implementation images not being addressed by any other component of CC part 2 [2].

7.1.6.2 Extended Components

Extended Component FPT_ITE.1

Description

Export of TSF implementation fingerprint, provides the ability to export the TSF implementation fingerprint without protection of confidentiality or integrity.

Definition

FPT_ITE.1 Export of TSF implementation fingerprint

FPT_ITE.1.1 The TOE shall export fingerprint of TSF implementation given the following conditions [assignment: conditions for export].

FPT_ITE.1.2 The TSF shall use [assignment: list of generation rules to be applied by TSF] for the exported data.

Dependencies: No dependencies.

Extended Component FPT_ITE.2

Description

Export of TSF data, provides the ability to export the TSF data without protection of confidentiality or integrity.

Definition

FPT_ITE.2 Export of TSF data

FPT_ITE.2.1 The TOE shall export [assignment: list of types of TSF data] given the following conditions [assignment: conditions for export].

FPT_ITE.2.2 The TSF shall use [assignment: list of encoding rules to be applied by TSF] for the exported data.

Dependencies: No dependencies.

8 Security Requirements

8.1 Security Functional Requirements

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 Part 1 [1] of the CC. These operations are used in this ST.

The refinement operation is used to add detail to a requirement, and, thus, further restricts a requirement. In some cases a interpretation refinement is given. In such a case a extra paragraph starting with "Refinement" is given.

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.

The main reference for this Chapter is Chapter 6 of [BSI_PP_EHC_G2].

The selections and assignment made by the ST author are visualised by italicised text like *this*.

The referenced literature shown in brackets [xx] can be found in Chapter 1.2 of this document or in Chapter 13 of [BSI_PP_EHC_G2].

All tables and figures referenced in the description of the SFRs and their application notes can be found in this document. They are shown in the related protection profile [BSI_PP_EHC_G2].

8.1.1 General Protection of User data and TSF data

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 *Original PP quote: "The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] the following objects: [assignment: list of objects]."*

The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects:

password objects, secret cryptographic keys, private cryptographic keys, session keys, *and data in all files*.

The following Application Note was respected in the way indicated in **[bold print]***:*

"The writer of the Security Target may want to use iterations of FDP_RIP.1 in order to distinguish between data, which must be deleted already upon deallocation and those which can be deleted upon allocation. It is recommended to delete secret/private cryptographic keys and all passwords upon deallocation. For secret user data deletion upon allocation should be sufficient (depending on the resistance of the concrete TOE against physical attacks). **[deletion upon deallocation was chosen for all cases (passwords, secret/private keys, user data (i.e. data in all files)].** Note that the COS specification allows management of applications during operational use. Therefore it is theoretically possible that a newly created object uses memory areas, which belonged to another object before. Therefore the COS must ensure that contents of the deleted objects are not accessible by reading the new object. The open assign operation may be "none". **[this option was not chosen]"**

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 *Original PP quote: "The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: integrity errors] on all objects, based on the following attributes: [assignment: user data attributes]."*

The TSF shall monitor user data stored in containers controlled by the TSF for ***integrity errors*** on all objects, based on the following attributes:

(1) key objects,

(2) PIN objects,

(3) *affectedObject.flagTransactionMode=TRUE,*

(4) *user data in protected files,*

(4) *external input data for digital signature*.

FDP_SDI.2.2 *Original PP quote:* "Upon detection of a data integrity error, the TSF shall [assignment: action to be taken]."

Upon detection of a data integrity error, the TSF shall ***prevent the usage of the altered data***.

FPT_FLS.1 Failure with preservation of secure state

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

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

(1) exposure to operating conditions where therefore a malfunction could occur,

(2) failure detected by TSF according to FPT_TST.1.

FPT_EMS.1 Emanation of TSF and User data

FPT_EMS.1.1 *Original PP quote: "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]."*

The TOE shall not emit ***information on IC power consumption, information on command execution time, information on electromagnetic emanations*** in excess of ***non-useful information*** enabling access to **the following TSF data**

(1) Regular password

(2) Multi-Reference password

(3) PUC

(4) Session keys

(5) Symmetric authentication keys

(6) Private authentication keys

(7) *no other TSF data* and **the following user data**

(8) Private asymmetric keys

(9) Symmetric keys

(10) *no other user data*.

FPT_EMS.1.2 *Original PP quote: "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]."*

The TSF shall ensure **any user** are unable to use the following interface **circuit interfaces** to gain access to **the following TSF data**

(1) Regular password
(2) Multi-Reference password
(3) PUC
(4) Session keys
(5) Symmetric authentication keys
(6) Private authentication keys
(7) *no other TSF data* and **the following user data**
(8) Private asymmetric keys
(9) Symmetric keys
(10) *no other user data*.

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 *Original PP quote: "The TSF shall provide the capability to consistently interpret [assignment: list of TSF data types] when shared between the TSF and another trusted IT product."*

The TSF shall provide the capability to consistently interpret **Card Verifiable Certificate (CVC)** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 *Original PP quote: "The TSF shall use [assignment: list of interpretation rules to be applied by the TSF] when interpreting the TSF data from another trusted IT product."*

The TSF shall use **[21], chapter 7 "CV-Certificate" and [21], appendix H "CV-Certificate for ELC-keys"** when interpreting the TSF data from another trusted IT product.

FPT_ITE.1 Export of TSF implementation fingerprint

FPT_ITE.1.1 *Original PP quote: "The TOE shall export fingerprint of TSF implementation given the following conditions [assignment: conditions for export]."*

The TOE shall export fingerprint of TSF implementation given the following conditions **execution of the command FINGERPRINT [21]**.

FPT_ITE.1.2 *Original PP quote: "The TSF shall use [assignment: list of generation rules to be applied by TSF] for the exported data."*

The TSF shall use ***SHA-256 based fingerprint of the TOE implementation*** for the exported data.

For information, the following Application Note is kept in this document:

"The command FINGERPRINT calculates a hash value or CMAC based fingerprint over the complete executable code actually implemented by the TOE. The TOE implementation includes IC Dedicated Support Software, the Card Operating System and application specific code loaded on the smartcard by command LOAD CODE or any other means. The hash function respective the CMAC based calculation uses the prefix send in the command FINGERPRINT for "fresh" fingerprints over all executable code, i.e. no precomputed values over fixed parts of the code only."

FPT_ITE.2 Export of TSF data

FPT_ITE.2.1 *Original PP quote: "The TOE shall export [assignment: list of types of TSF data] given the following conditions [assignment: conditions for export]."*

The TOE shall export

(1) all public authentication reference data,

(2) all security attributes of the object system and for all objects of the object system for all commands,

(3) *none* given the following conditions

(1) no export of secret data,

(2) no export of private keys,

(3) no export of secure messaging keys,

(4) no export of passwords and PUC.

FPT_ITE.2.2 *Original PP quote: "The TSF shall use [assignment: list of encoding rules to be applied by TSF] for the exported data."*

The TSF shall use

Morpho (now Idemia) proprietary encoding rules which can transformed by the Morpho (now Idemia) wrapper implementation into the specified coding format of the Gematik for the exported data.

The following Application Note was respected in the way indicated in **[bold print]***:*

"The public TSF data addressed as TSF data in bullet (1) in the element FPT_ITE.2.1 covers at least all root public key and other public keys used as authentication reference data persistent stored in the object system (cf. applicationPublicKeyList and persistentCache) and exported by command LIST PUBLIC KEY. (cf. [21], persistentPublicKeyList in [21] and [27], application-PublicKeyList and persistentCache in [21]). **["all public authentication reference data" includes all the data listed]** The bullet (2) in the element FPT_ITE.2.1 covers all security attributes of the object system (cf. [21], (N019.900), [27], objectLocator 'E0') and of all objects of object types listed in Table 18 and all TOE specific security attributes and parameters (except secrets)**[exactly these security attributes are addressed]**. The COS specification [21] identifies optional functionality the TOE may support. The TOE (as COS, wrapper and guidance documentation) must support the user to find all objects and to export all security attributes of these objects. Note while MF, DF and EF are hierarchically structured the Application and Application Dedicated File are directly referenced which may require special methods to find all objects in the object system. Note the listOfApplication as security attribute of the object system contains at least one applicationIdentifier of each Application or Application Dedicated File (cf. [27]). The exported data shall be encoded by wrapper to allow interpretation of the TSF data. The encoding rules shall meet the requirements of the Technical Guidance TR-03143 describing the verification tool used for examination of the object system against the specification of the object system**[the wrapper encodes accordingly]**."

FPT_TST.1 TSF testing

FPT_TST.1.1 *Original PP quote: "The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of [selection: [assignment: parts of TSF], the TSF]."*

The TSF shall run a suite of self tests **during initial start-up** to demonstrate the correct operation of **the TSF**.

FPT_TST.1.2 *Original PP quote: "The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: parts of TSF data], TSF data]."*

The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**.

FPT_TST.1.3 *Original PP quote: "The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF]."*

The TSF shall provide authorised users with the capability to verify the integrity of **TSF**.

8.1.2 Authentication

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 *Original PP quote: "The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric]."*

The TSF shall provide a mechanism to verify that secrets meet **the quality metric: length not lower than *minimumLength* and not greater than *maximumLength***.

FIA_AFL.1/PIN Authentication failure handling

FIA_AFL.1.1/PIN *Original PP quote: "The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to [assignment: list of authentication events]."*

The TSF shall detect when **configurable positive integer within 1 to 15** unsuccessful authentication attempts occur related to **consecutive failed human user authentication for the PIN via VERIFY, ENABLE VERIFICATION REQUIREMENT, DISABLE VERIFICATION REQUIREMENT or CHANGE REFERENCE DATA command**.

FIA_AFL.1.2/PIN *Original PP quote: "When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: list of actions]."*

When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **block the password for authentication until successful unblock using command RESET RETRY COUNTER**

(1) P1='00' or P1='01' with presenting unblocking code PUC of this password object,

(2) P1='02' or P1='03' without presenting unblocking code PUC of this password object.

For information, the following Application Note is kept in this document:

"The component FIA_AFL.1/PIN addresses the human user authentication by means of a password. The configurable positive integer of unsuccessful authentication attempts is defined in the password objects of the object system."Consecutive failed authentication attemps" are counted separately for each PIN and interrupted by successful authentication attempt for this PIN, i.e. the PIN object has a retryCounter wich is initially set to startRetryCounter, decremented by each failed authentication attempt and reset to startRetryCounter by successful authentication with the PIN or be successful execution of the command RESET RETRY COUNTER. The command RESET RETRY COUNTER (CLA,INS,P1)=(00,2C,02) and (CLA,INS,P1)=(00,2C,03) unblock the PIN without presenting unblocking code PUC of this password object. In order to prevent bypass of the human user authentication defined by the PIN or PUC the object system shall define access control to this command as required by the security needs of the specific application context, cf. OE.Resp-ObjS."

FIA_AFL.1/PUC Authentication failure handling

FIA_AFL.1.1/PUC *Original PP quote: "The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to [assignment: list of authentication events]."*

The TSF shall detect when **configurable positive integer within 1 to 15** authentication attempts occur related to **usage of a password unblocking code using the RESET RETRY COUNTER command**.

FIA_AFL.1.2/PUC *Original PP quote: "When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: list of actions]."*

When the defined number of authentication attempts has been **met**, the TSF shall

warn the entity connected

not unblock the referenced blocked PIN

block the PUC resp. the verification mechanism for this PUC such that any subsequent authentication attempt with this PUC will fail and an unblocking of the blocked PIN related to this PUC is no longer possible.

For information, the following Application Note is kept in this document:

"The component FIA_AFL.1/PUC addresses the human user authentication by means of a PUC. The configurable positive integer of usage of password unblocking code is defined in the password objects of the object system.

The command RESET RETRY COUNTER can be used to change a password or reset a retry counter. In certain cases, for example for digital signature applications, the usage of the command RESET RETRY COUNTER must be restricted to the ability to reset a retry counter only."

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 *Original PP quote: "The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes]."*

The TSF shall maintain the following list of security attributes belonging to individual users:

(1) for Human User: authentication state gained

a. with password: pwdIdentifier in globalPasswordList and pwdIdentifier in dfSpecificPasswordList,

b. with Multi-Reference password: pwIdentifier in globalPasswordList and pwIdentifier in dfSpecificPasswordList,

(2) for Device: authentication state gained

a. by CVC with CHA in globalSecurityList if CVC is stored in MF and dfSpecificSecurityList if CVc is stored in a DF,

b. by CVC with CHAT in bitSecurityList,

c. with symmetric authentication key: keyIdentity of the key,

d. with secure messaging keys: keyIdentity of the key used for establishing the session key.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 *Original PP quote: "The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated."*

The TSF shall allow

(1) reading the ATR,

(2) *GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT and SELECT*

(3) commands with access control rule ALWAYS for the current life cycle status and depending on the interface,

(4) *LIST PUBLIC KEY* on behalf of the user to be performed before the user is authenticated.

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

The following Application Note was respected in the way indicated in **[bold print]***:*

"ATR means Cold ATR and Warm ATR (cf. COS specification [21], (N019.900)b). The TOE may or may not define TOE specific access control rules for the commands GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT and SELECT, cf. COS specification [21], (N022.810) **[no TOE specific access control rules defined]**. If the TOE does not define access control limitation for a command than the TOE shall allow the access for anybody (ALWAYS) and the ST author shall list the command in the element FIA_UAU.1.1**[all these commands are listed in FIA_UAU.1.1]**."

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 *Original PP quote: "The TSF shall prevent reuse of authentication data related to [assignment: identified authentication mechanism(s)]."*

The TSF shall prevent reuse of authentication data related to

(1) external device authentication by means of executing the command EXTERNAL AUTHENTICATE with symmetric or asymmetric key,

(2) external device authentication by means of executing the command MUTUAL AUTHENTICATE with symmetric or asymmetric key,

(3) external device authentication by means of executing the command GENERAL AUTHENTICATE with symmetric or asymmetric key.

(4) *none*.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 *Original PP quote: "The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication."*

The TSF shall provide

(1) the execution of the VERIFY command,

(2) the execution of the CHANGE REFERENCE DATA command,

(3) the execution of the RESET RETRY COUNTER command,

(4) the execution of the EXTERNAL AUTHENTICATE command,

(5) the execution of the MUTUAL AUTHENTICATE command,

(6) the execution of the GENERAL AUTHENTICATE command,

(7) a secure messaging channel,

(8) a trusted channel to support user authentication.

FIA_UAU.5.2 *Original PP quote: "The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication]."*

The TSF shall authenticate any user's claimed identity according to the

(1) password based authentication shall be used for authenticating a human user by means of commands VERIFY, CHANGE REFERENCE DATA and RESET RETRY COUNTER,

(2) key based authentication mechanisms shall be used for authenticating of devices by means of commands EXTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE and GENERAL AUTHENTICATE,

(3) *none*.

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 *Original PP quote: "The TSF shall re-authenticate the sender of a message under the conditions [assignment: list of conditions under which re-authentication is required]."*

The TSF shall re-authenticate the sender of a message under the conditions

(1) each command sent to the TOE after establishing the secure messaging channel by successful authentication by execution of the INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE, or MUTUAL AUTHENTICATE or GENERAL AUTHENTICATE commands shall be verified as being sent by the authenticated device,

For information, the following Application Note is kept in this document:

"The entities establishing a secure messaging channel respective a trusted channel authenticate each other and agree symmetric session keys. The sender of a command authenticates its message by MAC calculation for the command (cf. PSO COMPUTE CRYPTOGRAPHIC CHECKSUM using SK4TC, cf. Package Crypto Box) and the receiver of the commands verifies the authentication by MAC verification of commands (using SK4SM). The receiver of the commands authenticates its message by MAC calculation (using SK4SM) and the sender of a command verifies the authentication by MAC verification of responses (cf. PSO VERIFY CRYPTOGRAPHIC CHECKSUM using SK4TC). If secure messaging is used with encryption the re-authentication includes the encrypted padding in the plaintext as authentication attempt of the message sender (cf. PSO ENCIPHER for commands) and the reciever (cf. secure messaging for responses) and verification of the correct padding as authentication verification by the message receiver (cf. secure messaging for received commands and PSO DECIPHER for received responses). The specification [21] states in section 13.1.2 item (N031.600): This re-authentication is controlled by the external entity (e.g. the connector in the eHealth environment). If no Secure Messaging is indicated in the CLA byte (see [ISO7816-4] Clause 5.1.1) and SessionkeyContext.flagSessionEnabled has the value SK4SM, then the security status of the key that was involved in the negotiation of the session keys MUST be deleted by means of clearSessionKeys(...)." Furthermore item (N031.700) states that the security status of the key that was involved in the negotiation of the session keys MUST be deleted by means of clearSessionKeys(...) if the check of the command CMAC (cf. FCS_COP.1/COS.CMAC) or Retail-MAC (cf.

FCS_COP.1/COS.RMAC) fails. The TOE does not execute any command with incorrect message authentication code. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on a MAC, whether it was sent by the successfully authenticated communication partner. The TOE does not execute any command with incorrect MAC. Therefore, the TOE re-authenticates the communication partner connected, if a secure messaging error occurred, and accepts only those commands received from the initially communication partner."

FIA_UID.1 Timing of identification

FIA_UID.1.1 *Original PP quote: "The TSF shall allow [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified."*

The TSF shall allow

(1) reading the ATR

(2) *GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT and SELECT*

(3) commands with access control rule ALWAYS for the current life cycle status and depending on the interface,

(4) *LIST PUBLIC KEY* 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.

The following Application Note was respected in the way indicated in **[bold print]***:*

"The TOE may or may not define TOE specific access control rules for the commands GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT and SELECT, cf. COS specification [21], (N022.810). If the TOE does not define access control limitation for these commands then the TOE shall allow the access for anybody (ALWAYS) and the ST author shall list the command in the element FIA_UID.1.1**[no TOE specific access control rules defined, all these commands are listed in FIA_UID.1.1]**."

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 *Original PP quote: "The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or rule]."*

The TSF shall provide a

(1) INTERNAL AUTHENTICATE,

(2) MUTUAL AUTHENTICATE,

(3) GENERAL AUTHENTICATE to prove the identity of the

TSF itself.

Refinement:

The TSF shall provide

(1) INTERNAL AUTHENTICATE,

(2) MUTUAL AUTHENTICATE,

(3) GENERAL AUTHENTICATE to prove the identity of the

TSF itself to an external entity.

FMT_SMR.1 Security roles

FMT_SMR.1.1 *Original PP quote: "The TSF shall maintain the roles [assignment: the authorised identified roles]."*

The TSF shall maintain the roles

(1) World as unauthenticated user without authentication reference data,

(2) Human User authenticated by password in the role defined for this password,

(3) Human User authenticated by PUC as holder of the corresponding password,

(4) Device authenticated by means of symmetric key in the role defined for this key,

(5) Device authenticated by means of asymmetric key in the role defined by the Certificate Holder Authorisation in the CVC,

(6) *none*.

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

The following Application Note was respected in the way indicated in **[bold print]***:*

"The protection profile BSI-CC-PP-0035-2007 does not explicitly define role because roles are linked to life cycle of the chip not addressed by SFR. Therefore the current PP defines the role "World" relevant for all parts of the TOE (e.g. physical protection) and roles for COS related SFR. The ST may add developer specific roles, e. g. for TSF data export according to FPT_ITE.1/EXP **[no additional roles added]**.

Human users authenticate themselves by identifying the password or Multi-reference password and providing authentication verification data to be matched to the secret of the password object or PUC depending on the command used. The role gained by authorization with a password is defined in the security attributes of the objects and related to identified commands. The authorization status is valid for the same level and in the level below in the file hierarchy as the password object is stored. The role gained by authentication with a symmetric key is defined in the security attributes of the objects and related to identified commands. The assignment may assign additional role like the role defined for authentication by means of PACE protocol (if PACE is supported by the TOE) or "none" **[no additional roles added]**."

FIA_USB.1 User-subject binding

FIA_USB.1.1 *Original PP quote: "The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes]."*

The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

(1) For Human User authenticated with password: pwIdentifier and Authentication Context globalPasswordList and dfSpecificPasswordList.

(2) for Human User authenticated with PUC: pwIdentifier of corresponding password,

(3) for Device the Role authenticated by RSA based CVC: the Certificate Holder Authorisation (CHA) in the CVC,

(4) for Device the Role authenticated by ECC based CVC: the Certificate Holder Authorisation Template (CHAT),

(5) for Device the Role authenticated by symmetric key: keyIdentifier and Authentication Context.

FIA_USB.1.2 *Original PP quote: "The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes]."*

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

(1) If the logical channel is reset by command Manage Channel (INS,P1,P2)=('70','40','00') the initial authentication state is set to "not authenticated" (i.e. globalPasswordList, dfSpecificPasswordList, globalSecurityList, dfSpecificSecurityList and keyReferenceList are empty, SessionkeyContext.flagSessionEnabled=noSK).

(2) If the command SELECT is executed and the newFile is an folder the initial authentication state of the selected folder inherit the authentication state of the folder above up the root.

FIA_USB.1.3 *Original PP quote: "The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes]."*

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

(1) The authentication state is changed to "authenticated Human User" for the specific context when the Human User has successfully authenticated via one of the following procedures:

a) VERIFY command using the context specific password or the context specific Multi-Reference password,

b) If the security attribute flagEnabled of password object is set to False the authentication state for this specific password is changed to "authenticated Human User".

c) If the security attribute flagEnabled of Multi-Reference password object is set to False the authentication state for this specific Multi-Reference password is changed to "authenticated Human User".

(2) The authentication state is changed to "authenticated Device" for the specific authentication context when a Device has successfully authenticated via one of the following procedures:

a) EXTERNAL AUTHENTICATE with symmetric or public keys,

b) MUTUAL AUTHENTICATE with symmetric or public keys,

c) GENERAL AUTHENTICATE with mutual ELC authentication and

d) GENERAL AUTHENTICATE for asynchronous secure messaging.

(3) The effective access rights gained by ECC based CVC: the CHAT are the intersection of the access rights encoded in the CHAT of the CVC chain used as authentication reference data of the Device.

(4) All authentication contexts are lost and the authentication state is set to "not authenticated" for all contexts if the TOE is reset.

(5) If a DELETE command is executed for a password object or symmetric authentication key the entity is authenticated for the authentication state has to be set to "not authenticated". If a DELETE command is executed for a folder (a) authentication states gained by password objects in the deleted folder shall be set to "not authenticated" and (b) all entires in keyReferenceList and allPublicKeyList related to the deleted folder shall be removed.

(6) If an authentication attempt using one of the following commands failed the authentication state for the specific context has to be set to "not authenticated": EXTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE,MANAGE SECURITY ENVIRONMENT (variant with restore).

(7) If a context change by using the SELECT command is performed the authentication state for all objects of the old authentication context not belonging to the new context of the performed SELECT command have to be set to "not authenticated".

(8) If failure of secure messaging (not indicated in CLA-byte, or erroneous MAC, or erroneous cryptogram) is detected the authentication status of the device in the current context set to "not authenticated" (i.e. the element in globalSecurityList respective in dfSpecificSecurityList and the used SK4SM are deleted).

(9) *none*.

For information, the following Application Note is kept in this document:

"Note the security attributes of the user are defined by the authentication reference data. The user may chose security attributes of the subjects interface in the power on session and seIdentifier by execution of command MANAGE SECURITY ENVIRONMENT for the current directory. The initial authentication state is set when the command SELECT is executed and the newFile is a folder (cf. [21], clause (N076.100) and (N048.200))."

8.1.3 Access Control

For information, the following Application Note is kept in this document:

"This section defines SFR for access control on User data in the object system. The SFR FDP_ACF.1/MF_DF, FDP_ACF.1/EF, FDP_ACF.1/TEF, FDP_ACF.1/SEF and FDP_ACF.1/KEY describe the security attributes of the subject gaining access to these objects. The COS specification [21] describes the attributes of logical channels (i.e. subjects in CC terminology) which is valid for the core of COS including all packages. The globalSecurityList and dfSpecificSecurityList contain all keyIdentifier used for successful device authentications, i.e. the list may be empty, may contain a CHA, a key identifier of a symmetric authentication key or CAN (in form of the keyIdentifier of the derived key) used with PACE if PACE is supported by the TOE. Because of this common structure there is no need for separate SFR in package Contactless."

FDP_ACC.1/MF_DF Subset access control

FDP_ACC.1.1/MF_DF *Original PP quote: "The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]."*

The TSF shall enforce the **access control MF_DF SFP** on

(1) the subjects logical channel bind to users

a. World,

b. Human User,

c. Device,

d. Human User and Device,

e. *none,*

(2) the objects

a. all executable code implemented by the TOE,

b. MF,

c. Application,

d. Dedicated file,

e. Application dedicated file,

f. persistent stored public keys,

g. *none,*

(3) the operation by command following

a. command SELECT,

b. create objects with command LOAD APPLICATION with and without command chaining,

c. delete objects with command DELETE,

d. read fingerprint with command FINGERPRINT,

e. command LIST PUBLIC KEY,

f. *retrieve a challenge from the card with GET_CHALLENGE, export data with the command GET DATA*.

For information, the following Application Note is kept in this document:

"Note the commands ACTIVATE, DEACTIVATE and, TERMINATE DF for current file applicable to MF, DF, Application and Application dedicated file manage the security life cycle attributes. Therefore access control to theses commands are described by FMT_MSA.1/Life. The object "all executable code implemented by the TOE" includes IC Dedicated Support Software, the Card Operating System and application specific code loaded on the smartcard by command LOAD CODE or any other means."

FDP_ACF.1/MF_DF Security attribute based access control

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

The TSF shall enforce the **access control MF_DF SFP** to objects based on the following:

(1) the subject logical channel with security attributes

a. interface,

b. globalPasswordList,

c. globalSecurityList,

d. dfSpecificPasswordList,

e. dfSecurityList,

f. bitSecurityList,

g. SessionkeyContext,

h. *none*

(2) the objects

a. all executable code implemented by the TOE,

b. MF with security attributes lifeCycleStatus, seIdentifier and interfaceDependentAccessRules,

c. DF with security attributes lifeCycleStatus, seIdentifier and interfaceDependentAccessRules,

d. Application with security attributes lifeCycleStatus, seIdentifier and interfaceDependentAccessRules,

e. Application dedicated file with security attributes lifeCycleStatus, seIdentifier and interfaceDependentAccessRules,

f. persistent stored public keys,

g. *none*.

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

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) SELECT is *ALWAYS allowed*.

(2) GET_CHALLENGE is *ALWAYS allowed*.

(3) A subject is allowed to create new objects (user data or TSF data) in the current folder MF if the security attributes interface, globalPasswordList, globalSecurityList and SessionkeyContext of the subject meet the access rules for the command LOAD APPLICATION of the MF dependent on lifeCycleStatus, seIdentifier and interfaceDependentAccessRules.

(4) A subject is allowed to create new objects (user data or TSF data) in the current folder Application, Dedicated file or Application Dedicated file if the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command LOAD APPLICATION of this object dependent on lifeCycleStatus, seIdentifier and interfaceDependentAccessRules.

(5) A subject is allowed to DELETE objects in the current folder MF if the security attributes interface, globalPasswordList, globalSecurityList and SessionkeyContext of the subject meet the access rules for the command DELETE of the MF dependent on lifeCycleStatus, seIdentifier and interfaceDependentAccessRules.

(6) A subject is allowed to DELETE objects in the current Application, Dedicated file or Application, Dedicated file if the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList,

dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command DELETE of this object dependent on lifeCycleStatus, seIdentifier and interfaceDependentAccessRules.

(7) A subject is allowed to read fingerprint according to FPT_ITE.1 if it is allowed to execute the command FINGERPRINT in the currentFolder.

(8) All subjects are allowed to execute command LIST PUBLIC KEY to export all persistent stored public keys.

(9) GET_DATA is *ALWAYS allowed*..

FDP_ACF.1.3/MF_DF *Original PP quote: "The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]."*

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **None**.

FDP_ACF.1.4/MF_DF *Original PP quote: "The TSF shall explicitly deny access of subjects to objects based on the following additional rules:[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]."*

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***If the access condition of an object is NEVER than the access to it is denied***.

The following Application Note was respected in the way indicated in **[bold print]***:*

"The object system defines sets of access control rules depending on the life cycle status, security environment and the used interface (i.e. contact based or contactless interface). The security environment may be chosen for the current folder by means of command MANAGE SECURITY ENVIRONMENT. The command SELECT is therefore pre-requisite for many other commands. The access control rule defines for each command, which is defined by CLA, INS, P1 and P2 and acceptable for the type of the object, the necessary security state, which is reached by successful authentication of human user and devices, to allow the access to the selected object. Note the command FINGERPRINT process the data representing the TOE implementation like user data (i.e. hash value calculation, no execution or interpretation as code) and is developer specific. Therefore the ST writer shall describe the TOE specific access control rules for these commands **[Access control rules for SELECT and FINGERPRINT described]**. The ST writer shall perform the open operations where "none" is allowed **[all operations performed – added GET DATA (see following application note)]**."

FDP_ACC.1/EF Subset access control

FDP_ACC.1.1/EF *Original PP quote: "The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]."*

The TSF shall enforce the **access rule EF SFP** on

(1) the subjects logical channel bind to users

a. World,

b. Human User,

c. Device,

d. Human User and Device,

e. *none*

(2) the objects

a. EF

b. Transparent EF

c. Structured EF

d. *none*

(3) the operation by command following

a. SELECT

b. DELETE of the current file.

c. *none*.

The following Application Note was respected in the way indicated in **[bold print]***:*

"Note the commands ACTIVATE, DEACTIVATE and, TERMINATE DF for current file applicable to EF, Transparent EF and Structured EF manage the security life cycle attributes. Therefore access control to theses commands are described by FMT_MSA.1/Life. The commands CREATE, GET DATA, GET RESPONSE and PUT DATA are optional. If implemented by the TOE these commands shall be added to the corresponding FDP_ACC.1 and FDP_ACF.1 SFR **[CREATE, GET RESPONSE and PUT DATA are not implemented. GET DATA was added to FDP_ACC.1 and FDP_ACF.1]**. The commands specific for transparent files are described in FDP_ACC.1/TEF and FDP_ACF.1/TEF SFR. The commands specific for structured files are described in FDP_ACC.1/SEF and FDP_ACF.1/SEF SFR."

FDP_ACF.1/EF Security attribute based access control

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

The TSF shall enforce the **access rule EF SFP** to objects based on the following:

(1) the subject logical channel with security attributes

a. interface,

b. globalPasswordList,

c. globalSecurityList,

d. dfSpecificPasswordList,

e. dfSpecificSecurityList,

f. bitSecurityList,

g. SessionkeyContext,

h. *none*

(2) the objects

a. EF with security attributes seIdentifier of the current folder, lifeCycleStatus and interfaceDependentAccessRules of the EF and *transaction protection Mode, checksum*

b. *none*.

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

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) SELECT is *ALWAYS allowed*.

(2) A subject is allowed to DELETE the current EF if the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command DELETE of this object dependent on lifeCycleStatus, interfaceDependentAccessRules and seIdentifier of the current folder.

(3) *none*.

FDP_ACF.1.3/EF *Original PP quote: "The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]."*

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/EF *Original PP quote: "The TSF shall explicitly deny access of subjects to objects based on the following additional rules:[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]."*

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***If the access condition of a object is NEVER than the access to it is denied***.

The following Application Note was respected in the way indicated in **[bold print]***:*

"The EF stands here for transparent EF and structured EF, which access control is further refined by FDP_ACF.1/TEF and FDP_ACF.1/SEF. The selection of "transaction protection Mode" and "checksum" may be empty because they are optional in the COS specification [21] **[transaction protection Mode and checksum selected]**."

FDP_ACC.1/TEF Subset access control

FDP_ACC.1.1/TEF *Original PP quote: "The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]."*

The TSF shall enforce the **access rule TEF SFP** on

(1) the subject logical channel bind to users

a. World,

b. Human User,

c. Device,

d. Human User and Device,

e. *none*

(2) the objects

a. Transparent EF,

b. *none*

(3) the operation by following command

a. ERASE BINARY,

b. READ BINARY,

c. SET LOGICAL EOF,

d. UPDATE BINARY,

e. WRITE BINARY,

f. *none*.

FDP_ACF.1/TEF Security attribute based access control

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

The TSF shall enforce the **access rule TEF SFP** to objects based on the following:

(1) the subjects logical channel with security attributes

a. interface,

b. globalPasswordList,

c. globalSecurityList,

d. dfSpecificPasswordList,

e. dfSpecificSecurityList,

f. bitSecurityList,

g. SessionkeyContext,

h. *none*

(2) the objects

a. with security attributes seIdentifier of the current folder, lifeCycleStatus and interfaceDependentAccessRules of the current Transparent EF, and *transaction protection Mode and checksum*

b. *none*.

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

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) The subject is allowed to execute the command listed in FDP_ACC.1.1/TEF for the current Transparent EF if the security attributes interface, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules of this object for this command dependent on seIdentifier of the current folder, lifeCycleStatus and interfaceDependentAccessRules of the current Transparent EF.

(2) ***none***.

FDP_ACF.1.3/TEF *Original PP quote: "The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]."*

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/TEF *Original PP quote: "The TSF shall explicitly deny access of subjects to objects based on the following additional rules:[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]."*

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Rules defined in FDP_ACF.1.4/EF apply, and *no other rules***.

The following Application Note was respected in the way indicated in **[bold print]***:*

"The selection of "transaction protection Mode" and "checksum" may be empty because they are optional in the COS specification [21] **[transaction protection Mode and checksum selected]**. If the checksum of the data to be read by READ BINARY is malicious the TOE must append a warning when exporting. Exporting of malicious data should be taken into account by the evaluator during evaluation of class AVA: vulnerability assessment."

FDP_ACC.1/SEF Subset access control

FDP_ACC.1.1/SEF *Original PP quote: "The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]."*

The TSF shall enforce the **access rule SEF SFP** on

(1) the subjects logical channel bind to users

a. World,

b. Human User,

c. Device,

d. Human User and Device,

e. *none*

(2) the objects

a. record in Structured EF,

b. *none*

(3) the operation by command following

a. APPEND RECORD,

b. ERASE RECORD,

c. DELETE RECORD,

d. READ RECORD,

e. SEARCH RECORD,

f. UPDATE RECORD,

g. *none*.

FDP_ACF.1/SEF Security attribute based access control

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

The TSF shall enforce the **access rule SEF SFP** to objects based on the following:

(1) the subjects logical channel with security attributes

a. interface,

b. globalPasswordList,

c. globalSecurityList,

d. dfSpecificPasswordList,

e. dfSpecificSecurityList,

f. bitSecurityList,

g. SessionkeyContext,

h. *none*

(2) the objects

a. with security attributes seIdentifier of the current folder, lifeCycleStatus and interfaceDependentAccessRules of the current Structured EF, and lifeCycleStatus of the record,

b. *none*.

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

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) The subject is allowed to execute the command listed in FDP_ACC.1.1/SEF for the record of the current Structered EF if the security attributes interface, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules of this object for this command dependent on seIdentifier of the current folder, lifeCycleStatus and interfaceDependentAccessRules of the current Structered EF, and lifeCycleStatus of the record.

(2) *none*.

FDP_ACF.1.3/SEF *Original PP quote: "The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]."*

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/SEF *Original PP quote: "The TSF shall explicitly deny access of subjects to objects based on the following additional rules:[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]."*

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Rules defined in FDP_ACF.1.4/EF apply, and *none***.

The following Application Note was respected in the way indicated in **[bold print]***:*

"Keys can be TSF or user data. As SFR FDP_ACC.1/KEY and FDP_ACF.1/KEY address protection of user data the keys defined in these SFR as objects are user keys only. Keys used for authentication are TSF data and are therefore not in the scope of these two SFR. Please note that the PSO ENCIPHER, PSO DECIPHER, PSO COMPUTE CRYPTOGRAPHIC CHECKSUM, and PSO VERIFY CRYPTOGRAPHIC CHECKSUM are used with the SK4TC for trusted channel. If these commands are used in the context trusted channel the key used is TSF data and not user data. Therefore the SFR FDP_ACC.1/KEY and FDP_ACF.1/KEY are not applicable on the commands used for trusted channel. The commands PSO COMPUTE CRYPTOGRAPHIC CHECKSUM, and PSO VERIFY CRYPTOGRAPHIC CHECKSUM are required if the TOE supports the package Crypto Box **[package Crypto Box not supported].**

If the checksum of the record to be read by READ RECORD is malicious the TOE must append a warning when exporting. Exporting of malicious data should be taken into account by the evaluator during evaluation of class AVA: vulnerability assessment"

FDP_ACC.1/KEY Subset access control

FDP_ACC.1.1/KEY *Original PP/CC quote: "The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]."*

Refinement: The TSF shall enforce the **access control key SFP** on

(1) the subjects logical channel bind to users

a. World,

b. Human User

c. Device

f. Human User and Device,

e. *none*

(2) the objects

a. symmetric key used for user data,

b. private asymmetric key used for user data,

c. public asymmetric key for signature verification used for user data,

d. public asymmetric key for encryption used for user data,

e. ephemeral keys used during Diffie-Hellmann key exchange,

f. *none*.

(3) the operation by command following

a. DELETE for private, public and symmetric key objects,

b. MANAGE SECURITY ENVIRONMENT,

c. GENERATE ASYMMETRIC KEY PAIR,

d. PSO COMPUTE DIGITAL SIGNATURE,

e. PSO VERIFY DIGITAL SIGNATURE,

f. PSO VERIFY CERTIFICATE,

g. PSO ENCIPHER (access control is required only in the case when the PSO_ENCIPHER operates on persistent keys, in the given key case the key is constructed from the command data representation),

h. PSO DECIPHER,

i. PSO TRANSCIPHER,

---,

---,

j. *none*.

Comment: as option PSO COMPUTE CRYPTOGRAPHIC CHECKSUM and PSO VERIFY CRYPTOGRAPHIC CHECKSUM are not supported by the TOE, the above SFR was refined and these options deleted. The last assignment is "none" and has now item-identification "j".

FDP_ACF.1/KEY Security attribute based access control

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

The TSF shall enforce the **access control key SFP** to objects based on the following:

(1) the subjects logical channel with security attributes

a. interface,

b. globalPasswordList,

c. globalSecurityList,

d. dfSpecificPasswordList,

e. dfSpecificSecurityList,

f. bitSecurityList,

g. SessionkeyContext,

h. *none*.

(2) the objects

a. symmetric key used for user data with security attributes seIdentifier of the current folder, lifeCycleStatus and interfaceDependentAccessRules, the key type (encryption key or mac key), interfaceDependentAccessRules for session keys,

b. private asymmetric key used for user data with security attributes seIdentifier of the current folder, lifeCycleStatus, keyAvailable and interfaceDependentAccessRules,

c. public asymmetric key for signature verification used for user data with security attributes seIdentifier of the current folder, lifeCycleStatus and interfaceDependentAccessRules,

d. public asymmetric key for encryption used for user data with security attributes seIdentifier of the current folder, lifeCycleStatus and interfaceDependentAccessRules,

e. CVC with security attributes certificate content and signature,

f. ephemeral keys used during Diffie-Hellmann key exchange

g. *none*.

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

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) MANAGE SECURITY ENVIRONMENT is *ALWAYS allowed* in cases defined in FDP_ACF.1.4/KEY.

(2) A subject is allowed to DELETE an object listed in FDP_ACF.1.1/KEY if the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command DELETE of this object dependent on seIdentifier of the current folder, lifeCycleStatus and interfaceDependentAccessRules,

(3) A subject is allowed to generate a new asymmetric key pair or change the content of existing objects if the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command GENERATE ASYMMETRIC KEY PAIR of this object dependent on seIdentifier of the current folder, lifeCycleStatus, key type and interfaceDependentAccessRules. In case P1='80' or P1='84 the security attribute keyAvailable must be set to FALSE.

(4) A subject is allowed to import a public key as part of a CVC by means of the command PSO VERIFY CERTIFICATE if

a) the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command PSO VERIFY CERTIFICATE of the signature public key to be used for verification of the signature of the CVC dependent on seIdentifier of the current folder, lifeCycleStatus, key type and interfaceDependentAccessRules,b) the CVC has valid certificate content and signature, where the expiration date is checked against pointInTime.

(5) A subject is allowed to compute digital signatures using the private asymmetric key for user data if the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command PSO COMPUTE DIGITAL SIGNATURE of this object dependent on seIdentifier of the current folder, lifeCycleStatus, the key type and interfaceDependentAccessRules.

(6) Any subject is allowed to verify digital signatures using the public asymmetric key for user data using the command PSO VERIFY DIGITAL SIGNATURE.

(7) A subject is allowed encrypt user data using the asymmetric key if the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command PSO ENCIPHER of this object dependent on seIdentifier of the current folder, lifeCycleStatus, the key type and interfaceDependentAccessRules.

(8) A subject is allowed decrypt user data using the asymmetric key if the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command PSO DECIPHER of this object dependent on seIdentifier of the current folder, lifeCycleStatus, the key type and interfaceDependentAccessRules.

(9) A subject is allowed decrypt and to encrypt user data using the asymmetric keys if the security attributes interface, dfSpecificPasswordList, globalPasswordList, globalSecurityList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command PSO TRANSCIPHER of both keys dependent on seIdentifier of the current folder, lifeCycleStatus, the key type and interfaceDependentAccessRules.

(10) If the command PSO COMPUTE CRYPTOGRAPHIC CHECKSUM is supported by the TSF than the following rule applies: a subject is allowed to compute a cryptographic checksum with a symmetric key used for user data if the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command PSO COMPUTE CRYPTOGRAPHIC CHECKSUM of this object dependent on seIdentifier of the current folder, lifeCycleStatus, the key type and interfaceDependentAccessRules.

(11) If the command PSO VERIFY CRYPTOGRAPHIC CHECKSUM is supported by the TSF than the following rule applies: a subject is allowed to verify a cryptographic checksum with a symmetric key used for user data if the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList and SessionkeyContext of the subject meet the access rules for the command PSO VERIFY CRYPTOGRAPHIC CHECKSUM of this object dependent on seIdentifier of the current folder, lifeCycleStatus, the key type and interfaceDependentAccessRules.

(12) *none*.

FDP_ACF.1.3/KEY *Original PP quote: "The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]."*

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/KEY *Original PP quote: "The TSF shall explicitly deny access of subjects to objects based on the following additional rules:[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]."*

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(1) If the security attribute keyAvailable=TRUE the TSF shall prevent generation of a private key by means of the command GENERATE ASYMMETRIC KEY PAIR with P1='80' or P1='84.

(2) ***none***.

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 *Original PP quote: "The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection: choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP."*

The TSF shall enforce the **access control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

Refinement:

The TSF shall enforce the **access control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

After reset the security attributes of the subject are set as follows

(1) currentFolder is root,

(2) keyReferenceList, globalSecurityList, globalPasswordList, dfSpecificSecurityList, dfSpecificPasswordList and bitSecurityList are empty,

(3) SessionkeyContext.flagSessionEnabled is set to noSK,

(4) seIdentifier is #1,

(5) currentFile is undefined.

FMT_MSA.3.2 *Original PP quote: "The TSF shall allow the [assignment: the authorised identified roles] to specify alternative initial values to override the default values when an object or information is created."*

The TSF shall allow the **subjects allowed to execute the command LOAD APPLICATION** to specify alternative initial values to override the default values when an object or information is created.

For information, the following Application Note is kept in this document:

"The refinements provide rules for setting restrictive security attributes after reset."

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 *Original PP/CC quote: "The TSF shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF]."*

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

(1) Initialization,

(2) Personalization,

(3) Life Cycle Management by means of commands GENERATE ASYMMETRIC KEY PAIR, DELETE, LOAD APPLICATION, TERMINATE, TERMINATE DF, TERMINATE CARD USAGE, *none*

(4) Management of access control security attributes by means of commands ACTIVATE, DEACTIVATE, ACTIVATE RECORD, DEACTIVATE RECORD, ENABLE VERIFICATION REQUIREMENT, DISABLE VERIFICATION REQUIREMENT, LOAD APPLICATION,

(5) Management of password objects attributes by means of commands CHANGE REFERENCE DATA, RESET RETRY COUNTER, GET PIN STATUS, VERIFY, LOAD APPLICATION,

(6) Management of device authentication reference data by means of commands PSO VERIFY CERTIFICATE, GET SECURITY STATUS KEY LOAD APPLICATION,

(7) *Initialization by means of command LOAD APPLICATION, Personalization by means of command LOAD APPLICATION.*

The following Application Note was respected in the way indicated in **[bold print]***:*

"The protection profile BSI-CC-PP-0035-2007 [11] describes initialisation and personalisation as management functions. The ST author shall assign the COS commands dedicated for these management functions. **[the command LOAD APPLICATION was assigned – this is the command used both for initialization and personalization]**

LOAD APPLICATION creates new objects together with their TSF data (cf. FMT_MSA.1/Life). In case of folders this includes authentication reference data as passwords and public keys. CREATE is an optional command. The ST writer should add it to the commands for the Life Cycle Management listed in FMT_SMF.1 and FMT_MSA.1/Life if implemented. **[CREATE is not implemented]**"

FMT_MSA.1/Life Management of security attributes

FMT_MSA.1.1/Life *Original PP/CC quote: "The TSF shall enforce the [assignment: access control SFP(s), information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles]."*

Refinement: The TSF shall enforce the **access control MF_DF SFP, access control EF SFP, access rule TEF SFP, access rule SEF SFP and access control key SFP** to restrict the ability to

(1) create all security attributes **of the new object DF, Application, Application dedicated file, EF, TEF and SEF, as well as PIN and key objects** to **subjects allowed execution of command LOAD APPLICATION for the MF, DF, Application, Application dedicated file where the new object is created,**

(2) change security attributes of the object MF, DF, Application, Application dedicated file, EF, TEF and SEF by means of command LOAD APPLICATION to none

(3) change the security attributes lifeCycleStatus to "Operational state (active)" to subjects allowed execution of command ACTIVATE for the selected object,

(4) change the security attributes lifeCycleStatus to "Operational state (deactivated)" to subjects allowed execution of command DEACTIVATE for the selected object,

(5) change the security attributes lifeCycleStatus to "Termination state" to subjects allowed execution of command TERMINATE for the selected EF, the key object or the password object

(6) change the security attributes lifeCycleStatus to "Termination state" to subjects allowed execution of command TERMINATE DF for the selected DF, Application or Application File,

(7) change the security attributes lifeCycleStatus to "Termination state" to subjects allowed execution of command TERMINATE CARD USAGE,

(8) qurey the security attributes lifeCycleStatus to by means of command SELECT to *ALWAYS allowed*,

(9) delete all security attributes of the selected object to subjects allowed execution of command DELETE for the selected object to *none*.

The subject logical channel is allowed to execute a command if the security attributes interface, globalPasswordList, globalSecurityList, dfPass-

wordList, dfSecurityList, bitSecurityList SessionkeyContext of the subject meet the security attributes lifeCycleStatus, seIdentifier and interfaceDependentAccessRules of the affected object..

Comment of PP: in (1) the object types "PIN" and "Key objects" seem to miss in the PP. Therefore the above SFR was refined to include them. *The following Application Note was respected in the way indicated in* **[bold print]***:*

"The subject logical channel is allowed to execute a command if the security attributes interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList, bitSecurityList SessionkeyContext of the subject meet the security attributes lifeCycleStatus, seIdentifier and interfaceDependentAccessRules of the affected object.

The refinements repeat the structure of the element in order to avoid iteration of the same SFR. The command LOAD APPLICATION allows to create new objects and may allow update of objects MF, DF, Application, Application dedicated file and their security attributes (cf. [21], (N039.300)). The ST writer shall perform the selection in FMT_MSA.1.1/Life, clause (2) in order to indicate possible security implications of changes in the TSF data of existing objects **[selection performed taking into account the consequences of LOAD APPLICATION]**."

FMT_MSA.1/SEF Management of security attributes

FMT_MSA.1.1/SEF *Original PP quote: "The TSF shall enforce the [assignment: access control SFP(s), information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles]."*

The TSF shall enforce the **access control SEF SFP** to restrict the ability to

(1) change the security attributes **lifeCycleStatus of the selected record to "Operational state (active)" to subjects allowed to execute the command ACTIVATE RECORD**

(2) change the security attributes lifeCycleStatus of the selected record to "Operational state (deactivated)" to subjects allowed to execute the command DEACTIVATE RECORD,

(3) delete all security attributes of the selected record to **subjects allowed to execute the command DELETE RECORD,**

(4) *none*

The subject logical channel is allowed to execute a command if the security attributes interface, globalPasswordList, globalSecurityList,

dfSpecificPasswordList, dfSpecificSecurityList, bitSecurityList SessionkeyContext of the subject meet the security attributes lifeCycleStatus, seIdentifier and interfaceDependentAccessRules of the affected object..

The following Application Note was respected in the way indicated in **[bold print]***:*

"The access rights can be described in FMT_MSA.1/SEF in more detail. The "authorised identified roles" could therefore be interpreted in a wider scope including the context where the command is allowed to be executed. The refinements repeat the structure of the element in order to avoid iteration of the same SFR **[it was chosen not to make use of the wider scope]**."

FMT_MTD.1/PIN Management of TSF data

FMT_MTD.1.1/PIN *Original PP quote: "The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles]."*

The TSF shall restrict the ability to

(1) set new secret of the **password objects by means of command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00) to subjects successful authenticated with the old secret of this password object,**

(2) set new secret and change transportStatus to regularPassword of the password objects with transportStatus equal to Leer-PIN by means of command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01) to World,

(3) set new secret of the password objects by means of command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,00) to subjects successful authenticated with the PUC of this password object

(4) set new secret of the password objects by means of command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) to **World**.

The following Application Note was respected in the way indicated in **[bold print]***:*

"The TOE provides access control to the commands depending on the object system. The refinements repeat the structure of the element in order to avoid iteration of the same SFR. The commands CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01) and RESET RETRY COUNTER (CLA,INS,P1)=(00,2C,02) set a new password without need of authentication by PIN

or PUC. In order to prevent bypass of the human user authentication defined by the PIN or PUC the object system shall define access control to this command as required by the security needs of the specific application context, cf. OE.Resp-ObjS **[access control is defined as specified in relation to the password object]**."

FMT_MSA.1/PIN Management of security attributes

FMT_MSA.1.1/PIN *Original PP/CC quote: "The TSF shall enforce the [assignment: access control SFP(s), information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles]."*

The TSF shall enforce the **access control MF_DF SFP, access control EF SFP, access rule TEF SFP, access rule SEF SFP and access control key SFP** to restrict the ability to

(1) reset by means of commands VERIFY the security attributes **retry counter of password objects** to **subjects successful authenticated with the secret of this password object,**

(2) reset by means of commands CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00) the security attribute retry counter of password objects to subjects successful authenticated with the old secret of this password object,

(3) change by means of commands CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00) the security attribute transportStatus from Transport-PIN to regularPassword to subjects allowed to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00),

(4) change by means of commands CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01) the security attribute transportStatus from Leer-PIN to regularPassword to subjects allowed to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01),

(5) reset by means of commands DISABLE VERIFICATION REQUIREMENT with (CLA,INS,P1)=(00,26,00) the security attribute retry counter of password objects to subjects successful authenticated with the old secret of this password object,

(6) reset by means of commands ENABLE VERIFICATION REQUIREMENT with (CLA,INS,P1)=(00,28,00) the security attribute retry counter of password objects to subjects successful authenticated with the old secret of this password object,

(7) reset by means of command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,00) or (CLA,INS,P1)=(00,2C,01) the security attribute retry counter of password objects to subjects successful authenticated with the PUC of this password object,

(8) reset by means of command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or (CLA,INS,P1)=(00,2C,03) the security attribute retry counter of password objects to subjects allowed to execute the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or CLA,INS,P1)=(00,2C,03) ,

(9) query by means of command GET PIN STATUS the security attribute flagEnabled, retry counter, transportStatus to World

(10) enable the security attributes flagEnabled requiring authentication with the selected password to subjects authenticated with passwaord and allowed to execute the command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,28,00),

(11) enable the security attributes flagEnabled requiring authentication with the selected password to subjects allowed to execute the command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,28,01),

(120) disable the security attributes flagEnabled requiring authentication with the selected password to subjects authenticated with passwaord and allowed to execute the command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,00)

(13) disable the security attributes flagEnabled requiring authentication with the selected password to subjects allowed to execute the command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,01).

The following Application Note was respected in the way indicated in **[bold print]***:*

"The TOE provides access control to the commands depending on the object system. The refinements repeat the structure of the element in order to avoid iteration of the same SFR. The command DISABLE VERIFICATION REQUIREMENT can be used to disable the need to perform successful authentication via the selected password or Multi-Reference password, i.e. any authentication attempt will be successful. The command ENABLE VERIFICATION REQUIREMENT can be used to enable the need to perform an authentication. The access rights to execute these commands can be limited to specific authenticated subjects. For example: the execution of DISABLE VERIFICATION REQUIREMENT should not be allowed for signing applications. The command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,01) allows to disable the verification requirement with the PIN. The command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,28,01) allows anybody to enable the verification requirement with the PIN. The commands RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or (CLA,INS,P1)=(00,2C,03) allows to reset the RESET RETRY COUNTER without authentication

with PUC. In order to prevent bypass of the human user authentication defined by the PIN the object system shall define access control to these commands as required by the security needs of the specific application context, cf. OE.Resp-ObjS. **[access control is defined as specified limiting the access to these commands]**."

FMT_MTD.1/Auth Management of TSF data

FMT_MTD.1.1/Auth *Original PP/CC quote: "The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles]."*

The TSF shall restrict the ability to

(1) import by means of commands LOAD APPLICATION the **root public keys** to **roles autorized to execute this command,**

(2) import by means of commands PSO VERIFY CERTIFICATE the root public keys to roles autorized to execute this command,

(3) import by means of commands PSO VERIFY CERTIFICATE the certificates as device authentication reference data to roles autorized to execute this command,

(4) select by means of command MANAGE SECURITY ENVIRONMENT the device authentication reference data to *World*.

The subject logical channel is allowed to execute a command if the security attributes interface, globalPasswordList, globalSecurityList, dfPasswordList, dfSecurityList and bitSecurityList SessionkeyContext of the subject meet the security attributes lifeCycleStatus, seIdentifier and interfaceDependentAccessRules of the affected object..

For information, the following Application Note is kept in this document:

"The TOE provides access control to the commands depending on the object system. The refinements repeat the structure of the element in order to avoid iteration of the same SFR. If root public keys are imported according to clause (2) this public key will be stored in the persistentPublicKeyList or the persistentCache of the object system."

FMT_MSA.1/Auth Management of security attributes

FMT_MSA.1.1/Auth *Original PP/CC quote: "The TSF shall enforce the [assignment: access control SFP(s), information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles]."*

The TSF shall enforce the **access control key SFP** to restrict the ability to **query** the security attributes **access control rights set for the key** to **meet the access rules of command GET SECURITY STATUS KEYof the object dependent on lifeCycleStatus, seIdentifier and interfaceDependentAccessRules**.

FMT_MTD.1/NE Management of TSF data

FMT_MTD.1.1/NE *Original PP/CC quote: "The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles]."*

The TSF shall restrict the ability to

(1) export TSF data according to FPT_ITE.2 the

(a) public authentication reference data,

(b) security attributes for objects of the object system

to subjects allowed to execute the commands LIST PUBLIC KEY or GET ATTRIBUTE

(2) export TSF data according to FPT_ITE.2 the *no further data* to subjects allowed to execute the commands LIST PUBLIC KEY or GET ATTRIBUTE

(3) export the following TSF-data

(a) Password

(b) Multi-Reference password

(c) PUC

(d) Private keys

(e) Session keys

(f) Symmetric authentication keys

(g) Private authentication keys
(h) *no further TSF data*
and the following user data
(i) Private keys of the user
(j) Symmetric keys of the user
(k) *no further user data* to **nobody**.

8.1.4 Cryptographic Functions

The TOE provides cryptographic services based on elliptic curve cryptography (ECC) using the following curves refered to as COS standard curves in the following

(1) length 256 bit

(a) brainpoolP256r1 defined in RFC5639 [41], (b) ansix9p256r1] defined in ANSI X.9.62 [42],

(2) length 384

(a) brainpoolP384r1 defined in RFC5639 [41], (b) ansix9p384r1 defined in ANSI X.9.62 [42],

(3) length 512 bit

(a) brainpoolP512r1] defined in RFC5639 [41].

FCS_RNG.1 Random number generation

FCS_RNG.1.1 *Original PP quote: "The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid] random number generator that implements: [assignment: list of security capabilities]."*

[Editorially Refined] The TSF shall provide a ***hybrid physical*** random number generator ***PTG.3*** [7] that implements:

(PTG.3.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output.

(PTG.3.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.

(PTG.3.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG is started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.

(PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

(PTG.3.5) The online test procedure checks the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

(PTG.3.6) The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.

FCS_RNG.1.2 *Original PP quote: "The TSF shall provide random numbers that meet [assignment: a defined quality metric]."*

The TSF shall provide random numbers that meet

(PTG.3.7) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A.

(PTG.3.8) The internal random numbers shall use PTRNG of class PTG.2 as random source for the post-processing.

The following Application Note was respected in the way indicated in **[bold print]***:*

"This SFR requires the TOE to generate random numbers used for key generation according to TR-03116 [19] section 3.5, requiring RNG classes identified in the selection in element FCS_RNG.1.1 and recommending RNG of class PTG.3. **[PTG.3 chosen]** Note that the RNG of class DRG4 are hybrid deterministic and of class PTG3 are hybrid physical which are not addressed in BSI-CC-PP-0035. The implementation of the PACE protocol requires RNG of class PTG.3 (cf. [16]). **[n/a, PACE protocol not supported]** The COS specification [21] requires to implement RNG for

the command GET CHALLENGE,

the command GET RANDOM if package Logical Channel is supported, **[n/a, package Logical Channel not supported]**

the authentication protocols as required by FIA_UAU.4,

the key agreement for secure messaging

according to TR-03116 [19] section 3.4,. The selection in the element FCS_RNG.1.1 includes RNG of classes DRG.3 and DRG.4. **[n/a, PTG.3 chosen]** The quality metric assigned in element FCS_RNG.1.2 shall be chosen to resist attacks with high attack potential **[metric chosen accordingly].”**

FCS_COP.1/SHA Cryptographic operation

FCS_COP.1.1/SHA *Original PP quote: “The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].”*

The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm

(1) SHA-1,

(2) SHA-256,

(3) SHA-384,

(4) SHA-512 and cryptographic key sizes **none** that meet the following: **TR-03116 [19], FIPS 180-4[37]**.

FCS_CKM.1/3TDES_SM Cryptographic key generation

FCS_CKM.1.1/3TDES_SM *Original PP/CC quote: “The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].”*

The TSF shall generate **session** cryptographic keys in accordance with a specified cryptographic key generation algorithm **Key Derivation Function specified in sec. 5.6.3 in ANSI X9.63** and specified cryptographic key sizes **192 bit (168 bit effectively)** that meet the following: **ANSI X9.63[40]**.

FCS_COP.1/COS.3TDES Cryptographic operation

FCS_COP.1.1/COS.3TDES *Original PP quote: "The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]."*

The TSF shall perform **decryption and encryption for secure messaging** in accordance with a specified cryptographic algorithm **3TDES in CBC mode** and cryptographic key sizes **192 bit (168 bit effectively)** that meet the following: **TR-03116 [19], NIST SP 800-67 [38]**.

FCS_COP.1/COS.RMAC Cryptographic operation

FCS_COP.1.1/COS.RMAC *Original PP quote: "The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]."*

The TSF shall perform

(1) computation and verification of cryptographic checksum for command

a. MUTUAL AUTHENTICATE,

b. EXTERNAL AUTHENTICATE,

(2) computation and verification of cryptographic checksum for secure messaging in accordance with a specified cryptographic algorithm **Retail MAC** and cryptographic key sizes **192 bit (168 bit effectively)** that meet the following: **TR-03116 [19], COS specification [21]**.

FCS_COP.1/COS.AES Cryptographic operation

FCS_COP.1.1/COS.AES *Original PP quote: "The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [as-*

signment: cryptographic key sizes] that meet the following: [assignment: list of standards].”

The TSF shall perform

1. encryption and decryption with card internal key for commands

a. MUTUAL AUTHENTICATE,

b. EXTERNAL AUTHENTICATE,

2. encryption with card internal key for command INTERNAL AUTHENTICATE,

3. encryption and decryption with card internal key for command GENERAL AUTHENTICATE,

4. encryption and decryption for secure messaging in accordance with a specified cryptographic algorithm **AES in CBC mode** and cryptographic key sizes **128 bit, 192 bit, 256 bit** that meet the following: **TR-03116 [19], COS specification [21], FIPS 197 [33]**.

FCS_CKM.1/AES.SM Cryptographic key generation

FCS_CKM.1.1/AES.SM *Original PP/CC quote: “The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].”*

The TSF shall generate **session** cryptographic keys in accordance with a specified cryptographic key generation algorithm **Key Derivation for AES as specified in sec. 4.3.3 in [17]** and specified cryptographic key sizes **128 bit, 192 bit, 256 bit** that meet the following: **TR-03111 [17], COS specification [21], FIPS 197 [33]**.

For information, the following Application Note is kept in this document:

“The Key Generation FCS_CKM.1/AES.SM is done during MUTUAL AUTHENTICATE, EXTERNAL AUTHENTICATE, INTERNAL AUTHENTICATE or GENERAL AUTHENTICATE with establishment of secure messaging (with option Crypto Box also for trusted channel).”

FCS_COP.1/COS.CMAC Cryptographic operation

FCS_COP.1.1/COS.CMAC *Original PP quote: "The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]."*

The TSF shall perform

(1) computation and verification of cryptographic checksum for command

a. MUTUAL AUTHENTICATE,

b. EXTERNAL AUTHENTICATE,

(2) computation of cryptographic checksum for command INTERNAL AUTHENTICATE,

(3) computation and verification of cryptographic checksum for secure messaging in accordance with a specified cryptographic algorithm **CMAC** and cryptographic key sizes **128 bit, 192 bit, and 256 bit** that meet the following: **TR-03116 [19], COS specification [21], NIST SP 800-38B [36]**.

FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1/RSA *Original PP quote: "The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]."*

[Editorially Refined] The TSF shall generate cryptographic **RSA** keys in accordance with a specified cryptographic key generation algorithm ***CRT based*** and specified cryptographic key sizes **2048 bit and 3072 bit modulo length** that meet the following: **TR-03116 [19]**.

FCS_CKM.1/ELC Cryptographic key generation

FCS_CKM.1.1/ELC *Original PP quote: "The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assign-*

ment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].”

[Editorially Refined] The TSF shall generate cryptographic **ELC** keys in accordance with a specified cryptographic key generation algorithm ***ECDH (ISO 15946)*** **with COS standard curves** and specified cryptographic key **256 bit, 384 bit and 512 bit** that meet the following: **TR-03111 [17], COS specification [21]**.

The following Application Note was respected in the way indicated in **[bold print]***:*

“The COS specification [21] requires the TOE to support elliptic curves listed in COS specification [21], chapter 6.5 (refered as COS standard curves in this PP) and to implement the command GENERATE ASYMMETRIC KEY PAIR. Depending on the characteristic needs of the TOE should support the generation of asymmetric key pairs for the following operations:

qualified electronic signatures,

authentication of external entities,

document cipher key decipherment.

The ST writer shall perform the missing operations in the element FCS_CKM.1/RSA and FCS_CKM.1/ELC according to the implemented key generation algorithms.**[The operations were performed according to the implemented key generation algorithms *CRT based* for *FCS_CKM.1/RSA* and *ECDH (ISO 15946) with COS standard curves* for *FCS_CKM.1/ELC]”***

FCS_COP.1/COS.RSA.S Cryptographic operation

FCS_COP.1.1/COS.RSA.S *Original PP quote: “The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].”*

The TSF shall perform **digital signature generation for commands**

(1) PSO COMPUTE DIGITAL SIGNATURE

(2) INTERNAL AUTHENTICATE in accordance with a specified cryptographic algorithm

(1) RSASSA-PSS-SIGN with SHA-256,

(2) RSA SSA PKCS1-V1_5,

(3) RSA ISO9796-2 DS1 with SHA-256 (for INTERNAL AUTHENTICATE only),

(4) RSA ISO9796-2 DS2 with SHA-256 (for PSO Compute DIGITAL SIGNATURE only) and cryptographic key sizes **2048 bit and 3072 bit modulo length** that meet the following: **TR-03116 [19], COS specification [21], [31], [34]**.

FCS_COP.1/COS.RSA.V Cryptographic operation

FCS_COP.1.1/COS.RSA.V *Original PP quote: "The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]."*

The TSF shall perform **digital signature verification for import of RSA keys and authenticating external devices using the commands**

(1) PSO VERIFY CERTIFICATE

(2) EXTERNAL AUTHENTICATE in accordance with a specified cryptographic algorithm **RSA ISO9796-2 DS1** and cryptographic key sizes **2048 bit modulo length (3072 bit keys are additionally supported in EXTERNAL_AUTHENTICATE case)** that meet the following: **TR-03116 [19], COS specification [21], [31], [34]**.

For information, the following Application Note is kept in this document:

"The command PSO VERIFY CERTIFICATE may store the imported public keys for RSA and ELC temporarily in the volatileCache or permanently in the persistentCache or applicationPublicKeyList. These keys may be used as authentication reference data for asymmetric key based device authentication (cf. FIA_UAU.5) or user data."

FCS_COP.1/COS.ECDSA.V Cryptographic operation

FCS_COP.1.1/COS.ECDSA.V *Original PP/CC quote: "The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]."*

The TSF shall perform **digital signature verification for import of ELC keys, for digital signature verification, or for the verification of external devices for the commands**

(1) PSO VERIFY CERTIFICATE

(2) PSO VERIFY DIGITAL SIGNATURE

(3) EXTERNAL AUTHENTICATE in accordance with a specified cryptographic algorithm **ECDSA with COS standard curves using**

(4) SHA-256,

(5) SHA-384,

(6) SHA-512 and cryptographic key sizes **256 bits, 384 bits, 512 bits** that meet the following: **TR-03111 [17], TR-03116 [19], COS specification [21], [40]**.

FCS_COP.1/COS.ECDSA.S Cryptographic operation

FCS_COP.1.1/COS.ECDSA.S *Original PP quote: "The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]."*

The TSF shall perform **digital signature generation for command**

(1) PSO COMPUTE DIGITAL SIGNATURE

(2) INTERNAL AUTHENTICATE in accordance with a specified cryptographic algorithm **ECDSA with COS standard curves using**

(1) SHA-256,

(2) SHA-384,

(3) and SHA-512 and cryptographic key sizes **256 bits, 384 bits, 512 bits** that meet the following: **TR-03111 [17], TR-03116 [19], COS specification, [21], [40]**.

For information, the following Application Note is kept in this document:

"The TOE shall support two variants of the PSO COMPUTE DIGITAL SIGNATURE.

PSO COMPUTE DIGITAL SIGNATURE without Message Recovery shall be used for the signing algorithms

RSASSA-PSS-SIGN with SHA-256 (see FCS_COP.1/ COS.RSA.S),

RSA SSA PKCS1-V1_5, RSA (see FCS_COP.1/COS.RSA.S),

ECDSA with SHA-256, SHA-384 and SHA-512 (see FCS_COP.1/COS.ECDSA.S)

PSO COMPUTE DIGITAL SIGNATURE with Message Recovery shall be used for the for the following signing algorithm

RSA ISO9796-2 DS2 with SHA-256 (see FCS_COP.1/COS.ECDSA.S)"

FCS_COP.1/COS.RSA Cryptographic operation

FCS_COP.1.1/COS.RSA *Original PP quote: "The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]."*

The TSF shall perform

(1) encryption with passed key for command PSO ENCIPHER,

(2) decryption with stored key for command PSO DECIPHER,

(3) decryption and encryption for command PSO TRANSCIPHER using RSA (transcipher of data using RSA keys),

(4) decryption for command PSO TRANSCIPHER using RSA (transcipher of data from RSA to ELC),

(5) encryption for command PSO TRANSCIPHER using ELC (transcipher of data from ELC to RSA) in accordance with a specified cryptographic algorithm

(6) for encryption:

a. RSAES-PKCS1-v1_5, Encrypt ([34] section 7.2.1),

b. RSA-OAEP-Encrypt ([34] section 7.1.1])

(7) for decryption:

a. RSAES-PKCS1-v1_5, Decrypt ([34] section 7.2.2])

b. RSA-OAEP-Decrypt ([34] section 7.1.2]) and cryptographic key sizes **2048 bit and 3072 bit modulo length for RSA private key operation, 2048 bit length for RSA public key operation, and 256 bit, 384 bit and 512 bit for the COS standard curves** that meet the following: **TR-03116 [19], COS specification [21], [34]**.

FCS_COP.1/COS.ELC Cryptographic operation

FCS_COP.1.1/COS.ELC *Original PP quote: "The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]."*

The TSF shall perform **(1) encryption with passed key for command PSO ENCIPHER,**

(2) decryption with stored key for command PSO DECIPHER,

(3) decryption and encryption for command PSO TRANSCIPHER using ELC (transcipher of data using ELC keys),

(4) decryption for command PSO TRANSCIPHER using ELC (transcipher of data from ELC to RSA),

(5) encryption for command PSO TRANSCIPHER using ELC (transcipher of data from RSA to ELC) in accordance with a specified cryptographic algorithm

(1) for encryption ELC encryption

(2) for decryption ELC decryption and cryptographic key sizes **2048 bit and 3072 bit modulo length for RSA private key operation, 2048 bit length for RSA public key operation, and 256 bits, 384 bits, 512 bits for ELC keys with COS standard curves** that meet the following: **TR-03111 [17], TR-03116 [19], and COS specification [21]**.

The following Application Note was respected in the way indicated in **[bold print]***:*

"The TOE can support or reject the command PSO HASH (following standard [30]) and ENVELOPE (following standard [29]). If the command is supported the ST writer is asked to add a SFR FCS_COP.1/CB_HASH specifying the supported hash algorithms. **[n/a: command not supported]**"

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 *Original PP quote: "The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards]."*

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***erasure of the key*** that meets the following: ***physical erasure of the key***.

For information, the following Application Note is kept in this document: The TOE shall destroy the encryption session keys and the message authentication keys for secure messaging after reset or termination of 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. Explicit deletion of a secret using the DELETE command should also be taken into account by the ST writer.

8.1.5 Additional Cryptographic Functions

FCS_COP.1/COS.ECDSA.SigData.V Cryptographic operation

FCS_COP.1.1/COS.ECDSA.SigData.V *Original PP/CC quote: "The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]."*

The TSF shall perform ***digital signature verification for signed data import*** in accordance with a specified cryptographic algorithm ***ECDSA with COS standard curves using SHA-256,*** and cryptographic key sizes **256 bits** that meet the following: ***TR-03111 [17], TR-03116 [19]***.

Comment: This Morpho (now Idemia)-proprietary SFR FCS_COP.1/COS.ECDSA.SigData.V is added for signature verification dedicated to the securisation of the import of data.

8.1.6 Protection of communication

FTP_ITC.1/TC Inter-TSF trusted channel

FTP_ITC.1.1/TC 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/TC *Original PP quote: "The TSF shall permit [selection: the TSF, another trusted IT product] to initiate communication via the trusted channel."*

The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/TC *Original PP quote: "The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required]."*

The TSF shall initiate communication via the trusted channel for **none**.

The following Application Note was respected in the way indicated in **[bold print]***:*

"The TOE responds only to commands establishing secure messaging channels. **[by assigning "none" it is reflected that the TOE does not initiate, only responds]"**

8.1.7 Protection against Malfunction

FRU_FLT.2/SICP Limited fault tolerance

FRU_FLT.2.1/SICP *Original PP/CC quote: "The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [assignment: list of type of failures]."*

The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: **exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1)**.

Note:

This SFR is taken over from [BSI_PP_IC].

FPT_FLS.1/SICP Failure with preservation of secure state

FPT_FLS.1.1/SICP *Original PP/CC quote: "The TSF shall preserve a secure state when the following types of failures occur: [assignment: list of types of failures in the TSF]."*

The TSF shall preserve a secure state when the following types of failures occur: **exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur**.

Note: This SFR is taken over from [BSI_PP_IC].

8.1.8 Protection against Abuse of Functionality

FMT_LIM.1/SICP Limited capabilities

FMT_LIM.1.1/SICP *Original PP/CC quote: "The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with"Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: Limited capability and availability policy]."*

The TSF shall be designed and implemented 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.**

Note: This SFR is taken over from [BSI_PP_IC].

FMT_LIM.2/SICP Limited availability

FMT_LIM.2.1/SICP *Original PP/CC quote: "The TSF shall be designed in a manner that limits its availability so that in conjunction with"Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: Limited capability and availability policy]."*

The TSF shall be designed and implemented 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.**

Note:This SFR is taken over from [BSI_PP_IC].

FAU_SAS.1/SICP Audit storage

FAU_SAS.1.1/SICP *Original PP/CC quote: "The TSF shall provide [assignment: list of subjects] with the capability to store [assignment: list of audit information] in the [assignment: type of persistent memory]."*

The TSF shall provide the test process before TOE Delivery with the capability to store the Initialisation Data and/or Pre-personalisation Data and/or supplements of the Security IC Embedded Software in the **not changeable configuration page area and non-volatile memory**.

For information, the following Application Note is kept in this document: "This SFR is taken over from [ST_IC]."

8.1.9 Protection against Physical Manipulation and Probing

FPT_PHP.3/SICP Resistance to physical attack

FPT_PHP.3.1/SICP *Original PP/CC quote: "The TSF shall resist [assignment: physical tampering scenarios] to the [assignment: list of TSF devices/elements] by responding automatically such that the SFRs are always enforced."*

The TSF shall resist **physical manipulation and physical probing** to the **TSF** by responding automatically such that the SFRs are always enforced.

Note:This SFR is taken over from [BSI_PP_IC].

8.1.10 Protection against Leakage

FDP_ITT.1/SICP Basic internal transfer protection

FDP_ITT.1.1/SICP *Original PP/CC quote: "The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to prevent the [selection: disclosure, modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE."*

The TSF shall enforce the **Data Processing Policy** to prevent the **disclosure** of user data when it is transmitted between physically-separated parts of the TOE.

Note:This SFR is taken over from [BSI_PP_IC].

FPT_ITT.1/SICP Basic internal TSF data transfer protection

FPT_ITT.1.1/SICP *Original PP/CC quote: "The TSF shall protect TSF data from [selection: disclosure, modification] when it is transmitted between separate parts of the TOE."*

The TSF shall protect TSF data from **disclosure** when it is transmitted between separate parts of the TOE.

Note:This SFR is taken over from [BSI_PP_IC].

FDP_IFC.1/SICP Subset information flow control

FDP_IFC.1.1/SICP *Original PP/CC quote: "The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]."*

The TSF shall enforce the **Data Processing Policy** on **all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software**.

Note:This SFR is taken over from [BSI_PP_IC].

8.1.11 Generation of Random Numbers

FCS_RNG.1/SICP Random number generation

FCS_RNG.1.1/SICP *Original PP quote: "The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid] random number generator that implements: [assignment: list of security capabilities]."*

Refinement: The TSF shall provide a **physical** random number generator that implements:

PTG.2.1 A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

PTG.2.2 If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.

PTG.2.3 The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.

PTG.2.4 The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

PTG.2.5 The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

FCS_RNG.1.2/SICP *Original PP/CC quote: "The TSF shall provide random numbers that meet [assignment: a defined quality metric]."*

The TSF shall provide random numbers that meet

PTG.2.6 Test procedure A, as defined in [6] does not distinguish the internal random numbers from output sequences of an ideal RNG.

PTG.2.7 The average Shannon entropy per internal random bit exceeds 0.997.

For information, the following Application Note is kept in this document: "This SFR is taken over from [ST_IC]."

8.2 Security Assurance Requirements

For more information see Chapter 6.2 of [BSI_PP_EHC_G2].

8.2.1 ADV Development

8.2.1.1 ADV_ARC Security Architecture

ADV_ARC.1 Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Refinement:

If a feature or command identified as optional in the COS specification is implemented in the TOE or any other additional functionality of the TOE is not part of the TSF the security architecture description shall demonstrate that it do not bypass the SFR-enforcing functionality.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

For information, the following Application Note is kept in this document: "The COS specification [21] allows implementation of optional features and commands. The following refinement for

ADV_ARC.1.5C defines specific evidence required for these optional features and commands if implemented by the TOE and not being part of the TSF."

8.2.1.2 ADV_FSP Functional specification

ADV_FSP.4 Complete functional specification

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

Refinement:

The functional specification shall describe the purpose and method of use for all TSFI **including**

(1) the physical and logical interface of the smart card platform, both contact based and contactless as implemented by the TOE,

(2) the logical interface of the wrapper to the verification tool.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

For information, the following Application Note is kept in this document: "The IC surface as external interface of the TOE provides the TSFI for physical protection (cf. FPT_PHP.3) and evaluated in the IC evaluation as base evaluation for the composite evaluation of the composite TOE (cf. [9], chapter 2.5.2, for details). This interface is also analysed as attack surface in the vulnerability analysis e.g. in respect to perturbation and emanation side channel analysis."

8.2.1.3 ADV_IMP Implementation representation

ADV_IMP.1 Implementation representation of the TSF

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

Refinement:

The developer shall make available the implementation representation for the entire **TOE**.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

For information, the following Application Note is kept in this document: "The refinement extends the TSF implementation representation to the TOE implementation representation, i.e. the complete executable code implemented on the Security platform IC including all IC Embedded Software and especially the Card Operating System, (COS)."

8.2.1.4 ADV_TDS TOE design

ADV_TDS.3 Basic modular design

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

ADV_TDS.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

8.2.2 AGD Guidance documents

8.2.2.1 AGD_OPE Operational user guidance

AGD_OPE.1 Operational user guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

Refinement:

The operational user guidance shall describe the method of use of the wrapper interface.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

For information, the following Application Note is kept in this document: "The wrapper will be used to interact with the smartcard for export of all public TSF data of all objects in an object system according to "Export of TSF data (FPT_ITE.2)". Because the COS specification [21] identifies optional functionality the TOE may support the guidance documentation shall describe method of use of the TOE (as COS, wrapper) to find all objects in the object system and to export all security attributes of these objects."

8.2.2.2 AGD_PRE Preparative procedures

AGD_PRE.1 Preparative procedures

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

8.2.3 ALC Life-cycle support

8.2.3.1 ALC_CMC CM capabilities

ALC_CMC.4 Production support, acceptance procedures and automation

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.3.2 ALC_CMS CM scope

ALC_CMS.4 Problem tracking CM coverage

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.3.3 ALC_DEL Delivery

ALC_DEL.1 Delivery procedures

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.3.4 ALC_DVS Development security

ALC_DVS.2 Sufficiency of security measures

ALC_DVS.2.1D The developer shall produce and provide development security documentation.

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_DVS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

8.2.3.5 ALC_LCD Life-cycle definition

ALC_LCD.1 Developer defined life-cycle model

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.3.6 ALC_TAT Tools and techniques

ALC_TAT.1 Well-defined development tools

ALC_TAT.1.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.4 ASE Security Target evaluation

8.2.4.1 ASE_CCL Conformance claims

ASE_CCL.1 Conformance claims

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.4.2 ASE_ECD Extended components definition

ASE_ECD.1 Extended components definition

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

8.2.4.3 ASE_INT ST introduction

ASE_INT.1 ST introduction

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

8.2.4.4 ASE_OBJ Security objectives

ASE_OBJ.2 Security objectives

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.4.5 ASE_REQ Security requirements

ASE_REQ.2 Derived security requirements

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.4.6 ASE_SPD Security problem definition

ASE_SPD.1 Security problem definition

ASE_APD.1.1D The developer shall provide a security problem definition.

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.4.7 ASE_TSS TOE summary specification

ASE_TSS.1 TOE summary specification

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

8.2.5 ATE Tests

8.2.5.1 ATE_COV Coverage

ATE_COV.2 Analysis of coverage

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.5.2 ATE_DPT Depth

ATE_DPT.2 Testing: security enforcing modules

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.2.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design.

ATE_DPT.2.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.2.3C The analysis of the depth of testing shall demonstrate that the SFR-enforcing modules in the TOE design have been tested.

ATE_DPT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.5.3 ATE_FUN Functional tests

ATE_FUN.1 Functional testing

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

Refinement:

The test plan shall include typical uses cases applicable for the TOE and the intended application eHC [22], eHPC [23], SMC-B [24], SMC-K [25] or SMC-KT [26].

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

For information, the following Application Note is kept in this document: "The developer should agree the typical uses cases with the evaluation laboratory and the certification body in order to define an effective test approach and to use synergy for appropiate test effort. The agreed test cases support comparable test effort for TSF defined in the main part of this PP and the optional packages included in the security target."

8.2.5.4 ATE_IND Independent testing

ATE_IND.2 Independent testing - sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

Refinement:

The evaluator tests shall include typical uses cases applicable for the TOE and the intended application eHC [22], eHPC [23], SMC-B [24], SMC-K [25] and SMC-KT [26].

For information, the following Application Note is kept in this document: "The evaluator should agree the typical uses cases with the certification body in order to define an effective test approach and to use synergy for appropiate test effort. The agreed test cases support comparable test effort for TSF defined in the main part of this PP and the optional packages included in the security target."

8.2.6 AVA Vulnerability assessment

8.2.6.1 AVA_VAN Vulnerability analysis

AVA_VAN.5 Advanced methodical vulnerability analysis

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

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

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.

8.3 Security Requirements Rationale

8.3.1 Objectives

8.3.1.1 Security Objectives for the TOE

Security IC Platform Protection Profile

O.Identification For more information about the requirements rationale for FAU_SAS.1/SICP see paragraph 244ff of [BSI_PP_IC].

O.Leak-Inherent For more information of the security objective rationale for FDP_IFC.1/SICP, FDP_ITT.1/SICP, FPT_ITT.1/SICP see paragraph 227ff of [BSI_PP_IC].

O.Phy-Probing For more information about the requirement rationale for FPT_PHP.3/SICP see paragraph 230ff of [BSI_PP_IC].

O.Malfunction For more information about the requirement rationale for see FPT_FLS.1/SICP, FRU_FLT.2/SICP paragraph 233ff of [BSI_PP_IC].

O.Phys-Manipulation For more information about the requirement rationale for FPT_PHP.3/SICP see paragraph 235 of [BSI_PP_IC].

O.Leak-Forced For more information about the requirement rationale for FDP_IFC.1/SICP FPT_ITT.1/SICP FDP_ITT.1/SICP see paragraph 238 of [BSI_PP_IC].

O.Abuse-Func For more information about the requirement rationale for FMT_LIM.1/SICP FMT_LIM.2/SICP see paragraph 240ff of [BSI_PP_IC].

O.RND For more information about the requirement rationale for FCS_RNG.1 and FCS_RNG.1/SICP see paragraph 247 of [BSI_PP_IC].

Card Operating System Generation 2 Protection Profile

O.Integrity For more information about the requirement rationale for FPT_FLS.1 FPT_TST.1 FDP_SDI.2 see paragraph 253 of [BSI_PP_EHC_G2].

Additionally, the TOE meets the SFR FCS_COP.1/COS.ECDSA.SigData.V which also contributes to the integrity protection of imported user and TSF data.

O.Confidentiality For more information about the requirement rationale for FDP_RIP.1 FPT_FLS.1 FPT_TST.1 FMT_MTD.1/NE FPT_EMS.1 see paragraph 254 of [BSI_PP_EHC_G2].

O.Resp-COS For more information about the requirement rationale for FPT_TST.1 see paragraph 255 of [BSI_PP_EHC_G2].

O.TSFDataExport For more information about the requirement rationale for FPT_TDC.1 FPT_ITE.1 FPT_ITE.2 see paragraph 256 of [BSI_PP_EHC_G2].

O.Authentication For more information about the requirement rational for FIA_SOS.1 FIA_AFL.1/PIN FIA_AFL.1/PUC FIA_ATD.1 FIA_UAU.1 FIA_UAU.4 FIA_UAU.5 FIA_UAU.6 FIA_UID.1 FMT_SMR.1 FMT_MSA.1/Life FMT_MTD.1/PIN FMT_MSA.1/PIN FMT_MTD.1/Auth FMT_MSA.1/Auth FIA_USB.1 FIA_API.1 see paragraph 257 of [BSI_PP_EHC_G2].

O.AccessControl For more information about the requirement rationale for FMT_SMR.1 FIA_USB.1 FDP_ACC.1/MF_DF FDP_ACF.1/MF_DF FDP_ACC.1/EF FDP_ACF.1/EF FMT_MSA.3 FMT_SMF.1 FMT_MSA.1/Life FMT_MSA.1/SEF FMT_MTD.1/PIN FMT_MSA.1/PIN FMT_MTD.1/Auth FMT_MSA.1/Auth FMT_MTD.1/NE FDP_ACC.1/TEF FDP_ACF.1/TEF FDP_ACC.1/SEF FDP_ACF.1/SEF FDP_ACC.1/KEY FDP_ACF.1/KEY see paragraph 258 of [BSI_PP_EHC_G2].

O.KeyManagement For more information about the requirement rationale for FCS_CKM.4 FCS_RNG.1 FCS_CKM.1/3TDES_SM FCS_CKM.1/AES.SM FCS_CKM.1/RSA FCS_CKM.1/ELC FDP_ACC.1/KEY FDP_ACF.1/KEY FMT_MSA.1/Life see paragraph 259 of [BSI_PP_EHC_G2].

O.Crypto For more information about the requirement rationale for

FCS_COP.1/SHA FCS_COP.1/COS.3TDES FCS_COP.1/COS.RMAC FCS_CKM.1/3TDES_SM FCS_COP.1/COS.AES FCS_CKM.1/AES.SM FCS_CKM.1/RSA FCS_CKM.1/ELC FCS_COP.1/COS.CMAC FCS_COP.1/COS.RSA.S FCS_COP.1/COS.RSA.V FCS_COP.1/COS.ECDSA.S FCS_COP.1/COS.RSA FCS_COP.1/COS.ELC FCS_RNG.1 FCS_COP.1/COS.ECDSA.V

see paragraph 260 of [BSI_PP_EHC_G2].

As extension to the PP FCS_COP.1/COS.ECDSA.SigData.V requires that the TSF provides the verification of digital signatures based on the ECDSA with hash SHA-256 and key size 256 bits.

O.SecureMessaging For more information about the requirement rationale for FCS_COP.1/COS.3TDES FCS_COP.1/COS.RMAC FCS_COP.1/COS.AES FCS_CKM.1/3TDES_SM FTP_ITC.1/TC see paragraph 261 of [BSI_PP_EHC_G2].

8.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
O.Identification	FAU_SAS.1/SICP	Section 6.3.1
O.Leak-Inherent	FDP_IFC.1/SICP, FDP_ITT.1/SICP, FPT_ITT.1/SICP	Section 6.3.1
O.Phy-Probing	FPT_PHP.3/SICP	Section 6.3.1
O.Malfunction	FPT_FLS.1/SICP, FRU_FLT.2/SICP	Section 6.3.1
O.Phys-Manipulation	FPT_PHP.3/SICP	Section 6.3.1
O.Leak-Forced	FDP_IFC.1/SICP, FPT_ITT.1/SICP, FDP_ITT.1/SICP	Section 6.3.1
O.Abuse-Func	FMT_LIM.1/SICP, FMT_LIM.2/SICP	Section 6.3.1
O.RND	FCS_RNG.1, FCS_RNG.1/SICP	Section 6.3.1
O.Integrity	FPT_FLS.1, FPT_TST.1, FDP_SDI.2, FCS_COP.1/COS.ECDSA.SigData.V	Section 6.3.1
O.Confidentiality	FDP_RIP.1, FPT_FLS.1, FPT_TST.1, FMT_MTD.1/NE, FPT_EMS.1	Section 6.3.1
O.Resp-COS	FPT_TST.1	Section 6.3.1
O.TSFDataExport	FPT_TDC.1, FPT_ITE.1, FPT_ITE.2	Section 6.3.1
O.Authentication	FIA_AFL.1/PIN, FIA_AFL.1/PUC, FIA_ATD.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UID.1, FMT_SMR.1, FMT_MTD.1/PIN, FMT_MSA.1/PIN, FMT_MTD.1/Auth, FMT_MSA.1/Auth, FIA_USB.1, FIA_API.1, FIA_SOS.1, FMT_MSA.1/Life	Section 6.3.1

Security Objectives	Security Functional Requirements	Rationale
O.AccessControl	FMT_SMR.1, FIA_USB.1, FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF, FDP_ACC.1/EF, FDP_ACF.1/EF, FMT_MSA.3, FMT_SMF.1, FMT_MSA.1/Life, FMT_MSA.1/SEF, FMT_MTD.1/PIN, FMT_MSA.1/PIN, FMT_MTD.1/Auth, FMT_MSA.1/Auth, FMT_MTD.1/NE, FDP_ACC.1/TEF, FDP_ACF.1/TEF, FDP_ACC.1/SEF, FDP_ACF.1/SEF, FDP_ACC.1/KEY, FDP_ACF.1/KEY	Section 6.3.1
O.KeyManagement	FCS_CKM.4, FCS_RNG.1, FCS_CKM.1/3TDES_SM, FCS_CKM.1/AES.SM, FCS_CKM.1/RSA, FCS_CKM.1/ELC, FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.1/Life	Section 6.3.1
O.Crypto	FCS_COP.1/SHA, FCS_COP.1/COS.3TDES, FCS_COP.1/COS.RMAC, FCS_CKM.1/3TDES_SM, FCS_COP.1/COS.AES, FCS_CKM.1/AES.SM, FCS_CKM.1/RSA, FCS_CKM.1/ELC, FCS_COP.1/COS.CMAC, FCS_COP.1/COS.RSA.S, FCS_COP.1/COS.RSA.V, FCS_COP.1/COS.ECDSA.S, FCS_COP.1/COS.RSA, FCS_COP.1/COS.ELC, FCS_RNG.1, FCS_COP.1/COS.ECDSA.SigData.V, FCS_COP.1/COS.ECDSA.V	Section 6.3.1
O.SecureMessaging	FCS_COP.1/COS.3TDES, FCS_COP.1/COS.RMAC, FCS_COP.1/COS.AES, FCS_CKM.1/3TDES_SM, FTP_ITC.1/TC	Section 6.3.1

Table 8 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives	
FDP_RIP.1	O.Confidentiality	
FDP_SDI.2	O.Integrity	
FPT_FLS.1	O.Integrity, O.Confidentiality	
FPT_EMS.1	O.Confidentiality	
FPT_TDC.1	O.TSFDataExport	
FPT_ITE.1	O.TSFDataExport	
FPT_ITE.2	O.TSFDataExport	
FPT_TST.1	O.Integrity, O.Confidentiality, O.Resp-COS	
FIA_SOS.1	O.Authentication	
FIA_AFL.1/PIN	O.Authentication	
FIA_AFL.1/PUC	O.Authentication	
FIA_ATD.1	O.Authentication	
FIA_UAU.1	O.Authentication	
FIA_UAU.4	O.Authentication	
FIA_UAU.5	O.Authentication	
FIA_UAU.6	O.Authentication	
FIA_UID.1	O.Authentication	
FIA_API.1	O.Authentication	
FMT_SMR.1	O.Authentication, O.AccessControl	
FIA_USB.1	O.Authentication, O.AccessControl	
FDP_ACC.1/MF_DF	O.AccessControl	
FDP_ACF.1/MF_DF	O.AccessControl	

Security Functional Requirements	Security Objectives	
FDP_ACC.1/EF	O.AccessControl	
FDP_ACF.1/EF	O.AccessControl	
FDP_ACC.1/TEF	O.AccessControl	
FDP_ACF.1/TEF	O.AccessControl	
FDP_ACC.1/SEF	O.AccessControl	
FDP_ACF.1/SEF	O.AccessControl	
FDP_ACC.1/KEY	O.AccessControl, O.KeyManagement	
FDP_ACF.1/KEY	O.AccessControl, O.KeyManagement	
FMT_MSA.3	O.AccessControl	
FMT_SMF.1	O.AccessControl	
FMT_MSA.1/Life	O.Authentication, O.AccessControl, O.KeyManagement	
FMT_MSA.1/SEF	O.AccessControl	
FMT_MTD.1/PIN	O.Authentication, O.AccessControl	
FMT_MSA.1/PIN	O.Authentication, O.AccessControl	
FMT_MTD.1/Auth	O.Authentication, O.AccessControl	
FMT_MSA.1/Auth	O.Authentication, O.AccessControl	
FMT_MTD.1/NE	O.Confidentiality, O.AccessControl	
FCS_RNG.1	O.RND, O.KeyManagement, O.Crypto	
FCS_COP.1/SHA	O.Crypto	

Security Functional Requirements	Security Objectives	
FCS_CKM.1/3TDES_SM	O.KeyManagement, O.Crypto, O.SecureMessaging	
FCS_COP.1/COS.3TDES	O.Crypto, O.SecureMessaging	
FCS_COP.1/COS.RMAC	O.Crypto, O.SecureMessaging	
FCS_COP.1/COS.AES	O.Crypto, O.SecureMessaging	
FCS_CKM.1/AES.SM	O.KeyManagement, O.Crypto	
FCS_COP.1/COS.CMAC	O.Crypto	
FCS_CKM.1/RSA	O.KeyManagement, O.Crypto	
FCS_CKM.1/ELC	O.KeyManagement, O.Crypto	
FCS_COP.1/COS.RSA.S	O.Crypto	
FCS_COP.1/COS.RSA.V	O.Crypto	
FCS_COP.1/COS.ECDSA.V	O.Crypto	
FCS_COP.1/COS.ECDSA.S	O.Crypto	
FCS_COP.1/COS.RSA	O.Crypto	
FCS_COP.1/COS.ELC	O.Crypto	
FCS_CKM.4	O.KeyManagement	
FCS_COP.1/COS.ECDSA.SigData.V	O.Integrity, O.Crypto	
FTP_ITC.1/TC	O.SecureMessaging	
FRU_FLT.2/SICP	O.Malfunction	
FPT_FLS.1/SICP	O.Malfunction	

Security Functional Requirements	Security Objectives	
FMT_LIM.1/SICP	O.Abuse-Func	
FMT_LIM.2/SICP	O.Abuse-Func	
FAU_SAS.1/SICP	O.Identification	
FPT_PHP.3/SICP	O.Phy-Probing, O.Phys-Manipulation	
FDP_ITT.1/SICP	O.Leak-Inherent, O.Leak-Forced	
FPT_ITT.1/SICP	O.Leak-Inherent, O.Leak-Forced	
FDP_IFC.1/SICP	O.Leak-Inherent, O.Leak-Forced	
FCS_RNG.1/SICP	O.RND	

Table 9 SFRs and Security Objectives

8.3.3 Dependencies

8.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FDP_RIP.1	No Dependencies	
FDP_SDI.2	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_EMS.1	No Dependencies	
FPT_TDC.1	No Dependencies	
FPT_ITE.1	No Dependencies	
FPT_ITE.2	No Dependencies	
FPT_TST.1	No Dependencies	
FIA_SOS.1	No Dependencies	
FIA_AFL.1/PIN	(FIA_UAU.1)	FIA_UAU.1
FIA_AFL.1/PUC	(FIA_UAU.1)	FIA_UAU.1
FIA_ATD.1	No Dependencies	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FIA_UAU.4	No Dependencies	
FIA_UAU.5	No Dependencies	

Requirements	CC Dependencies	Satisfied Dependencies
FIA_UAU.6	No Dependencies	
FIA_UID.1	No Dependencies	
FIA_API.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FIA_USB.1	(FIA_ATD.1)	FIA_ATD.1
FDP_ACC.1/MF_DF	(FDP_ACF.1)	FDP_ACF.1/MF_DF
FDP_ACF.1/MF_DF	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/MF_DF, FMT_MSA.3
FDP_ACC.1/EF	(FDP_ACF.1)	FDP_ACF.1/EF
FDP_ACF.1/EF	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/EF, FMT_MSA.3
FDP_ACC.1/TEF	(FDP_ACF.1)	FDP_ACF.1/TEF
FDP_ACF.1/TEF	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/TEF, FMT_MSA.3
FDP_ACC.1/SEF	(FDP_ACF.1)	FDP_ACF.1/SEF
FDP_ACF.1/SEF	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SEF, FMT_MSA.3
FDP_ACC.1/KEY	(FDP_ACF.1)	FDP_ACF.1/KEY
FDP_ACF.1/KEY	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/KEY, FMT_MSA.3

Requirements	CC Dependencies	Satisfied Dependencies
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Life, FMT_MSA.1/SEF, FMT_MSA.1/PIN, FMT_MSA.1/Auth
FMT_SMF.1	No Dependencies	
FMT_MSA.1/Life	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY, FMT_SMF.1
FMT_MSA.1/SEF	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY, FMT_SMF.1
FMT_MTD.1/PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/PIN	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY, FMT_SMF.1
FMT_MTD.1/Auth	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1

Requirements	CC Dependencies	Satisfied Dependencies
FMT_MSA.1/Auth	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY, FMT_SMF.1
FMT_MTD.1/NE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FCS_RNG.1	No Dependencies	
FCS_COP.1/SHA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	
FCS_CKM.1/3TDES_SM	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/COS.3TDES, FCS_CKM.4
FCS_COP.1/COS.3TDES	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/3TDES_SM, FCS_CKM.4
FCS_COP.1/COS.RMAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/3TDES_SM, FCS_CKM.4

Requirements	CC Dependencies	Satisfied Dependencies
FCS_COP.1/COS.AES	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/AES.SM, FCS_CKM.4
FCS_CKM.1/AES.SM	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/COS.AES, FCS_CKM.4
FCS_COP.1/COS.CMAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/AES.SM, FCS_CKM.4
FCS_CKM.1/RSA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/COS.RSA.S, FCS_COP.1/COS.RSA.V, FCS_COP.1/COS.RSA, FCS_CKM.4
FCS_CKM.1/ELC	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/COS.ECDSA.S, FCS_COP.1/COS.ELC, FCS_CKM.4
FCS_COP.1/COS.RSA.S	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/RSA, FCS_CKM.4
FCS_COP.1/COS.RSA.V	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/RSA, FCS_CKM.4

Requirements	CC Dependencies	Satisfied Dependencies
FCS_COP.1/COS.ECDSA.V	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/ELC, FCS_CKM.4
FCS_COP.1/COS.ECDSA.S	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/ELC, FCS_CKM.4
FCS_COP.1/COS.RSA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/RSA, FCS_CKM.4
FCS_COP.1/COS.ELC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/ELC, FCS_CKM.4
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/3TDES_SM, FCS_CKM.1/AES.SM, FCS_CKM.1/RSA, FCS_CKM.1/ELC
FCS_COP.1/COS.ECDSA.SigData.V	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/ELC, FCS_CKM.4
FTP_ITC.1/TC	No Dependencies	
FRU_FLT.2/SICP	(FPT_FLS.1)	FPT_FLS.1/SICP
FPT_FLS.1/SICP	No Dependencies	

Requirements	CC Dependencies	Satisfied Dependencies
FMT_LIM.1/SICP	(FMT_LIM.2)	FMT_LIM.2/SICP
FMT_LIM.2/SICP	(FMT_LIM.1)	FMT_LIM.1/SICP
FAU_SAS.1/SICP	No Dependencies	
FPT_PHP.3/SICP	No Dependencies	
FDP_ITT.1/SICP	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/SICP
FPT_ITT.1/SICP	No Dependencies	
FDP_IFC.1/SICP	(FDP_IFF.1)	
FCS_RNG.1/SICP	No Dependencies	

Table 10 SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FCS_CKM.4 of FCS_COP.1/SHA is discarded. The dependent SFRs are not applicable here because FCS_COP.1/SHA does not use any keys.

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/SHA is discarded. The dependent SFRs are not applicable here because FCS_COP.1/SHA does not use any keys.

The dependency FDP_IFF.1 of FDP_IFC.1/SICP is discarded. The rationale for this unsatisfied dependency can be found in the PP-0035.

8.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	

Requirements	CC Dependencies	Satisfied Dependencies
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.2	(ADV_ARC.1) and (ADV_TDS.3) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.2

Table 11 SARs Dependencies

8.3.4 Rationale for the Security Assurance Requirements

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs. The TOE shall be shown to be resistant to penetration attacks with high attack potential as described in the threats. Therefore the component AVA_VAN.5 was chosen in order to meet the security objectives. In addition ATE_DPT.2 is taken for to improve the test depth and ALC_DVS.2 to improve the security of development.

Please refer section 6.3.3"Rationale for the Assurance Requirements" in BSI-PP-0035 [11] for the details regarding the chosen assurance level EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

The selection of the component ATE_DPT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR- enforcing modules. The functional testing of SFR-enforcing modules is due to the TOE building a smartcard platform with very broad and powerful security functionality but without object system. An augmentation with ATE_DPT.2 only for the SFR specified in BSI-PP-0035 [11] would have been sufficient to fulfil the conformance, but this would contradict the intention of BSI-PP-0035. Therefore the augmentation with ATE_DPT.2 is required for the complete Protection Profile.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the development and manufacturing, especially for the secure handling of sensitive material. This augmentation was chosen due to the broad application of the TOE in security critical applications.

The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential.

The set of assurance requirements being part of EAL4 fulfils all dependencies a priori.

8.3.5 ALC_DVS.2 Sufficiency of security measures

This requirement is the most adequate for a manufacturing process in which several actors (Platform Developer, Operator, Application Developers, IC Manufacturer, etc) exchange and store highly sensitive information (confidential code, cryptographic keys, personalisation data, etc).

8.3.6 ATE_DPT.2 Testing: security enforcing modules

The selection of this component increases the test depth from subsystem to module level for more precise tests with a higher granularity.

8.3.7 AVA_VAN.5 Advanced methodical vulnerability analysis

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential.

9 TOE Summary Specification

9.1 TOE Summary Specification

The product is a secure element which implements an access controlled data storage system, strong authentication mechanisms, and functionality for handling of electronic certificates and signatures. These features are based on strong cryptographic functions like 3TDES, AES, RSA, and Elliptic Curve Cryptography.

The product implements PIN-based user authentication and various standardized external and internal device authentication mechanisms based on 3TDES, AES, RSA, and Elliptic Curve Cryptographic Functions. Whenever an external entity like a user or an external device has authenticated itself against the product, this fact is tracked internally in a security state model. The security states mitigate the access to the object system and the usage of key material stored in the card. This way, the product controls the use of functions like the creation of digital signatures or the access to sensitive user data in the object system.

The product is subject to a Common Criteria security evaluation at the assurance level EAL4 augmented with AVA_VAN.5 and capable to resist against attacks with a high attack potential in a hostile environment where an attacker has physical access to the product. Therefore, the product additionally provides strong self-protection, non-bypassability, and secure start-up mechanism to protect the user data and the data like PIN values and cryptographic keys used by the security functionality.

The following sections provide more details about the implemented security features of the product

User Authentication

The authentication of users is supported by the following security services.

The product implements a classical PIN-based user authentication. It is possible to flexibly instantiate the service, e.g. by a minimum required password length, or varying user or retry counter values.

The system allows for unblocking of a block PIN using a PIN unblocking code and to user roles which have the right to unblock the PIN.

For convenience purposes, the product implements multi-reference PINs which share the same personal identification number and other attributes. This way it is possible that a user keeps several different PINs in sync with each other.

A role with the required rights is allowed to activate or deactivate the verification requirement. This is also a convenience function which leverages the requirement to enter PINs.

Internal and External Device Authentication

The product is capable to authenticate an external role. After a successful role authentication, the product grants additional access and usage rights to the external entity.

The product also implements internal authentication services, which proof the authenticity of the card to an external entity. These services can either be used as one step of a mutual authentication protocol or to use the product as an authentication token in a larger eco-system.

Mutual Authentication protocols with the establishment of secure sessions between the card and a trusted external entity are also a major security service provided by the product. Via the secured channels it is possible to import and export data protecting the data integrity and confidentiality.

Security State Model

The product effectively models, stores and manages the security states acquired by external entities via user or device authentication. The proper modelling of security states is a prerequisite for controlling the access to the object system and the usage of cryptographic services.

Access-Controlled Cryptographic Services

The product implements several cryptographic services and controls the access to these services.

The card is capable to verify and import digital certificates. This way it is possible to load key material of a public key infrastructure onto the card for further processing.

The generation of digital signatures is an additional security services which enables the card holder to effectively sign electronic data.

Various enciphering, deciphering, and trans-ciphering services support cryptographic use cases in collaboration with the background system and other cards.

As an additional service, the product implements the generation of a fingerprint over the effective code-base which allows for precisely identifying a specific product release.

Secure Access-Controlled Object System

The object system that acts as storage for PINs, cryptographic keys, and user data provides strict access control mechanisms.

It is possible to model access rules in a fine grained manner based on the effective command currently executed, the life-cycle state of the affected object and the product, the security environment the product operates in and the current IO state, i.e. the IO interface used or the status of a secure session.

It is also possible to extend the object system by the loading of new application dedicated files containing additional data and key material in the field. This feature is also subject to the access control enforced by the object system.

The object system provides additional means to authorised users which allow for analysing the content of the object system. This feature is used in the approval process of object systems to ensure that a specific instantiation of an object system adheres to a given specification.

Elementary Cryptographic Functions

The elementary cryptographic functions of the product form the basis for the different authentication protocols and cryptographic services.

The product supports the 3TDES and the AES symmetric ciphers with up to 256bits as well as additional modes of operation like cipher-block-chaining, or retail-MAC computations.

Both the RSA and ECC crypto operations support asymmetric crypto services and authentication protocols. Additionally, the product supports on-card key generation

Several hash-functions like SHA1 and SHA2 support cryptographic operations like the generation of digital signatures or the derivation of session keys for secure channelling.

A high-quality random number generator is used internally e.g. for the generation of cryptographic key material of a high quality and also supports the implementation of many cryptographic protocols.

For the implementation of the elementary cryptographic functions the embedded software uses the cryptographic features of the underlying high-secure IC and (partially) its dedicated crypto library.

High Attack Resistance

The product is a secure element which exhibits a high attack resistance even if an attacker has physical access to the product. This attack resistance is achieved by strong self-protection mechanisms and a security design which prevents the

bypassing of security features. Furthermore, the start-up phase of the product is secured to ensure that the product properly initialises from a down-state to a secure mode of operation.

The security features implemented by the product closely collaborate with the protection mechanisms of the underlying security IC.

9.2 SFRs and TSS

9.2.1 SFRs and TSS - Rationale

9.2.1.1 TOE Summary Specification

User Authentication The user authentication services directly implement the handling of authentication failures as specified by FIA_AFL.1/PIN and FIA_AFL.1/PUC.

Furthermore, the user authenication mechanism allows for the management of user authentication data according to FMT_SMF.1, FMT_MTD.1/PIN, FMT_MSA.1/PIN.

Internal and External Device Authentication The internal and external device authentication services contribute to the implementation of the following security requirements:

FIA_UAU.4 and FIA_UAU.5 specify the requirement for implementing single-use authentication mechanisms which effectively prevent replay attacks and the implementation of multiple authentication mechanisms.

FIA_UAU.6 refers to the implicit re-authentication which is an inherent property of a secure channel which is protected by message authentication code (MAC) values which depend on a sent sequence counter.

The internal authentication mechansims implemented by the product target the SFR FIA_API.1.

the protection of communication as mandated by FTP_ITC.1/TC is also implementated by the secure channel establishment based on mutual device authentication.

Security State Model The Security State Model controls the security states acquired by external entities and is the basis for the subsequent access control on cryptographic services and on the usage of the object system. As such, the Security State Model conributes to the implementation of the following SFRs:

- the SFR FIA_ATD.1 defines the attributes assigned to external entities like human users and devices. These attributes are essential elements of the security state model.
- the security roles by the SFR FMT_SMR.1 define the roles for external entities which are maintained by the Security State Model.
- the SFR FIA_USB.1 defines the binding of users to subjects in the product which act on behalf of the external user which is also maintained ni the Security State Model of the product.
- the SFR FMT_MSA.3 defines requirements for the secure initialisatio of security attributes. As such, it defines the proper initialisation of the Security State Model.

Access-Controlled Cryptographic Services The access controlled cryptographic services contribute to the implementation of the following SFRs:

- the SFR FPT_TDC.1 mandates that the product properly interprets CV-certificates which is part of the certificate import service provided by the product. Additionally, the certificate import is related to the management of authentication data as specified in FMT_MTD.1/Auth and FMT_MSA.1/Auth.
- the export of the fingerprint specified in SFR FPT_ITE.1 is one of the cryptographic services supplied by the product.
- the access control releated to the usage of cryptographic services is specified by the SFRs FDP_ACC.1/KEY and FDP_ACF.1/KEY

Secure Access-Controlled Object System The Secure Access-Controlled Object System implements most of the SFRs related the access rule management. Furthermore, the system also allows for using a specific subset of commands without authentication requirements and is therefore also related to the SFRs that specify timing constraints. In detail:

- the capability to export TSF data according to SFR FPT_ITE.2 is a feature of the object system. The fact that the object system does not export sensitive data is captured by SFR FMT_MTD.1/NE
- the timing of authentication according to SFR FIA_UAU.1 and of the identification according to SFR FIA_UID.1 specify the operations allowed without authentication which is the opposite part to the access enforcing features of the object system.
- The SFR family FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF,FDP_ACC.1/EF, FDP_ACF.1/EF,FDP_ACC.1/TEF, FDP_ACF.1/TEF,FDP_ACC.1/SEF, FDP_ACF.1/SEF

specifiy the access rules enforce by the object system before granting access to the MF, DF, EF, TEF, and SEF respectively.

The management of security attributes as modelled by FMT_MSA.1/Life and FMT_MSA.1/SEF is also implemented by the access rule enforcement in the object system.

the object system is also enforces the effective erasure of key material as mandated by SFR FCS_CKM.4

Elementary Cryptographic Functions The Elemenatry Cryptographic Functions supplied by the system directly implement the SFRs of the "FCS"-family. In detail:

the SFR FCS_RNG.1 mandates the implementation of a high-quality random number generator. This is achieved based upon the physical random number generation supplied by the security IC in accordance to the SFR FCS_RNG.1/SICP

the SFR FCS_COP.1/SHA requires the implementation of SHA-1, SHA-256, and SHA-384 hash functions.

the SFR FCS_CKM.1/3TDES_SM specifies the DES based derivation of session keys

the SFR FCS_COP.1/COS.3TDES specifies the elementary 3TDES cipher and decipher operations

the SFR FCS_COP.1/RMAC specifies the computation of a retail MAC

the SFR FCS_COP.1/COS.AES defines the elementary AES cipher and decipher operations.

the SFR FCS_CKM.1/AES.SM specifies the elementary operation for the derivation of AES session keys

the SFR FCS_COP.1/COS.CMAC specifies the CMAC operation

the SFR FCS_CKM.1/RSA specifies on-card RSA key generation

the SFR FCS_CKM.1/ELC specifies on-card ELC key generation

the SFR FCS_COP.1/COS.RSA.S specifies the different RSA signature generation schemes supported by the product.

the SFR FCS_COP.1/COS.RSA.V specifies the different RSA signature verificaiton schemes supported by the product.

the SFR FCS_COP.1/COS.ECDSA.S specifies the different ELC signature generation schemes supported by the product.

the SFR FCS_COP.1/COS.ECDSA.V specifies the different ELC signature verificaiton schemes supported by the product.

the SFRs FCS_COP.1/COS.RSA and FCS_COP.1/COS_ELC specify the elementary RSA and ELC cipher and decipher mechanisms.

the product also implements the proprietary SFR FCS_COP.1/COS.ECDSA.SigData.V which is a signature verification dedicated to the securisation of the import of data.

High Attack Resistance The product achieves the resistance against a high attack potential by implementing the SFRs of the group "General Protection of User Data and TSF Data" and in collaboration with the security requirements enforced by the underlying security IC. In detail:

the SFR FDP_RIP.1 mandates the product to effectively erase sensitive data if it is no longer used.

the SFR FDP_SDI.2 addresses the need to monitor the stored data in order to detect induced errors.

the fact that the product automatically preserves a secure state even in the failure case as mandated by SFR FPT_FLS.1 is an essential self-protecion property

the SFR FPT_EMS.1 mandates that the product prohibits the emanation of information about confidential data. This is an important aspect to enforce the non-bypassability of the security functions.

the SFR FPT_TST.1 is directly related to the secure start-up enforced by the product.

the SFRs FRU_FLT.2/SICP, FPT_FLS.1/SICP, FMT_LIM.1/SICP, FMT_LIM.2/SICP, FAU_SAS.1/SICP,, FPT_PHP.3/SICP, FDP_ITT.1/SICP, FPT_ITT.1/SICP, FDP_IFC.1/SICP are enforced by the underlying security IC and contribute to the protection of the product against attacks.

9.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FDP_RIP.1	High Attack Resistance
FDP_SDI.2	High Attack Resistance
FPT_FLS.1	High Attack Resistance
FPT_EMS.1	High Attack Resistance
FPT_TDC.1	Access-Controlled Cryptographic Services
FPT_ITE.1	Access-Controlled Cryptographic Services
FPT_ITE.2	Secure Access-Controlled Object System
FPT_TST.1	High Attack Resistance
FIA_SOS.1	User Authentication
FIA_AFL.1/PIN	User Authentication
FIA_AFL.1/PUC	User Authentication
FIA_ATD.1	Security State Model
FIA_UAU.1	Secure Access-Controlled Object System
FIA_UAU.4	Internal and External Device Authentication
FIA_UAU.5	Internal and External Device Authentication
FIA_UAU.6	Internal and External Device Authentication
FIA_UID.1	Secure Access-Controlled Object System
FIA_API.1	Internal and External Device Authentication
FMT_SMR.1	Security State Model
FIA_USB.1	Security State Model
FDP_ACC.1/MF_DF	Secure Access-Controlled Object System
FDP_ACF.1/MF_DF	Secure Access-Controlled Object System
FDP_ACC.1/EF	Secure Access-Controlled Object System
FDP_ACF.1/EF	Secure Access-Controlled Object System
FDP_ACC.1/TEF	Secure Access-Controlled Object System

Security Functional Requirements	TOE Summary Specification
FDP_ACF.1/TEF	Secure Access-Controlled Object System
FDP_ACC.1/SEF	Secure Access-Controlled Object System
FDP_ACF.1/SEF	Secure Access-Controlled Object System
FDP_ACC.1/KEY	Access-Controlled Cryptographic Services
FDP_ACF.1/KEY	Access-Controlled Cryptographic Services
FMT_MSA.3	Security State Model
FMT_SMF.1	User Authentication
FMT_MSA.1/Life	Secure Access-Controlled Object System
FMT_MSA.1/SEF	Secure Access-Controlled Object System
FMT_MTD.1/PIN	User Authentication
FMT_MSA.1/PIN	User Authentication
FMT_MTD.1/Auth	Access-Controlled Cryptographic Services
FMT_MSA.1/Auth	Access-Controlled Cryptographic Services
FMT_MTD.1/NE	Secure Access-Controlled Object System
FCS_RNG.1	Elementary Cryptographic Functions
FCS_COP.1/SHA	Elementary Cryptographic Functions
FCS_CKM.1/3TDES_SM	Elementary Cryptographic Functions
FCS_COP.1/COS.3TDES	Elementary Cryptographic Functions
FCS_COP.1/COS.RMAC	Elementary Cryptographic Functions
FCS_COP.1/COS.AES	Elementary Cryptographic Functions
FCS_CKM.1/AES.SM	Elementary Cryptographic Functions
FCS_COP.1/COS.CMAC	Elementary Cryptographic Functions
FCS_CKM.1/RSA	Elementary Cryptographic Functions
FCS_CKM.1/ELC	Elementary Cryptographic Functions
FCS_COP.1/COS.RSA.S	Elementary Cryptographic Functions
FCS_COP.1/COS.RSA.V	Elementary Cryptographic Functions

Security Functional Requirements	TOE Summary Specification
FCS_COP.1/COS.ECDSA.V	Elementary Cryptographic Functions
FCS_COP.1/COS.ECDSA.S	Elementary Cryptographic Functions
FCS_COP.1/COS.RSA	Elementary Cryptographic Functions
FCS_COP.1/COS.ELC	Elementary Cryptographic Functions
FCS_CKM.4	Secure Access-Controlled Object System
FCS_COP.1/COS.ECDSA.SigData.V	Elementary Cryptographic Functions
FTP_ITC.1/TC	Internal and External Device Authentication
FRU_FLT.2/SICP	High Attack Resistance
FPT_FLS.1/SICP	High Attack Resistance
FMT_LIM.1/SICP	High Attack Resistance
FMT_LIM.2/SICP	High Attack Resistance
FAU_SAS.1/SICP	High Attack Resistance
FPT_PHP.3/SICP	High Attack Resistance
FDP_ITT.1/SICP	High Attack Resistance
FPT_ITT.1/SICP	High Attack Resistance
FDP_IFC.1/SICP	High Attack Resistance
FCS_RNG.1/SICP	Elementary Cryptographic Functions

Table 12 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
User Authentication	FIA_SOS.1, FIA_AFL.1/PIN, FIA_AFL.1/PUC, FMT_SMF.1, FMT_MTD.1/PIN, FMT_MSA.1/PIN
Internal and External Device Authentication	FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_API.1, FTP_ITC.1/TC
Security State Model	FIA_ATD.1, FMT_SMR.1, FIA_USB.1, FMT_MSA.3
Access-Controlled Cryptographic Services	FPT_TDC.1, FPT_ITE.1, FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MTD.1/Auth, FMT_MSA.1/Auth
Secure Access-Controlled Object System	FPT_ITE.2, FIA_UAU.1, FIA_UID.1, FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF, FDP_ACC.1/EF, FDP_ACF.1/EF, FDP_ACC.1/TEF, FDP_ACF.1/TEF, FDP_ACC.1/SEF, FDP_ACF.1/SEF, FMT_MSA.1/Life, FMT_MSA.1/SEF, FMT_MTD.1/NE, FCS_CKM.4
Elementary Cryptographic Functions	FCS_RNG.1, FCS_COP.1/SHA, FCS_CKM.1/3TDES_SM, FCS_COP.1/COS.3TDES, FCS_COP.1/COS.RMAC, FCS_COP.1/COS.AES, FCS_CKM.1/AES.SM, FCS_COP.1/COS.CMAC, FCS_CKM.1/RSA, FCS_CKM.1/ELC, FCS_COP.1/COS.RSA.S, FCS_COP.1/COS.RSA.V, FCS_COP.1/COS.ECDSA.V, FCS_COP.1/COS.ECDSA.S, FCS_COP.1/COS.RSA, FCS_COP.1/COS.ELC, FCS_COP.1/COS.ECDSA.SigData.V, FCS_RNG.1/SICP
High Attack Resistance	FDP_RIP.1, FDP_SDI.2, FPT_FLS.1, FPT_EMS.1, FPT_TST.1, FRU_FLT.2/SICP, FPT_FLS.1/SICP, FMT_LIM.1/SICP, FMT_LIM.2/SICP, FAU_SAS.1/SICP, FPT_PHP.3/SICP, FDP_ITT.1/SICP, FPT_ITT.1/SICP, FDP_IFC.1/SICP

Table 13 TSS and SFRs - Coverage

10 Notice

This document has been generated with TL SET version 3.1.3 (for CC3). For more information about the security editor tool of Trusted Labs visit our website at www.trusted-labs.com.

11 Statement of Compatibility

The statement of compatibility address the specific requirements for composite evaluation as stated in the document "Composite product evaluation for Smartcards and similar devices" **[EXS_CCDB_COMP]**.

11.1 Separation of the Platform-TSF

This section describes the separation of relevant security functionality described in the ST of the INF SLE78 platform (M7892 B11) being used by this ST. The security functionality provided by the IC platform is summarized in **[ST_IC]**. The following table lists the relevant security functionality of the platform regarding cryptography with regards to those of the composite TOE defined in the present ST.

Platform functionality	Usage by the composite TOE
SF_DPM	Device Phase Management
SF_PS	Protection against Snooping
SF_PMA	Protection against Modification Attacks
SF_PLA	Protection against Logical Attacks
SF_CS	Cryptographic Support

Table 1: Coverage of IC platform functionality

In the following table those SFRs of the IC platform are designated as "relevant" or "used by this composite ST". The table also lists irrelevant Platform-SFRs not being used by the Composite-ST. In the first part of the table there are SFRs which are taken from the **[BSI_PP_IC]** and are conformant to SFRs which are listed in this document with the extension «/SICP» (FAU_SAS.1/SICP).

Platform SFRs	Usage by TOE, TOE-SFR	Result
FCS_RNG.1	FCS_RNG.1	The random number generator provided by the IC is used for the initialization (seeding) of the random number generator of the embedded software of the TOE.
FMT_LIM.1	Not applicable	Extended functionality provided by the IC No contradiction to Composite-ST
FMT_LIM.2	Not applicable	Extended functionality provided by the IC No contradiction to Composite-ST
FAU_SAS.1	Not applicable	No operations are performed on platform SFR No contradiction to Composite-ST
FRU_FLT.2	Not applicable	No contradiction to Composite-ST
FPT_FLS.1	This SFR matches the FPT_FLS.1.	The functionality of the IC is directly used to fulfill the SFR of the TOE. No contradiction to Composite-ST
FPT_PHP.3	Not applicable	Not contributing directly to an SFR of the composite product but providing baseline protection for the composite security architecture. No contradiction to Composite-ST
FDP_ITT.1	Not applicable	Internal operations of the IC No contradiction to Composite-ST
FPT_ITT.1	Not applicable	Not contributing directly to an SFR of the composite product but providing baseline protection for the composite security architecture. No contradiction to Composite-ST
FDP_IFC.1	Not applicable	Not contributing directly to an SFR of the composite product but providing baseline protection for the composite security architecture. No contradiction to Composite-ST
FDP_ACC.1	Not applicable	Not contributing directly to an SFR of the composite product but providing baseline protection for the composite security architecture. No contradiction to Composite-ST
FDP_ACF.1	Not applicable	Not contributing directly to an SFR of the composite product but providing baseline protection for the composite security architecture. No contradiction to Composite-ST

Platform SFRs	Usage by TOE, TOE-SFR	Result
FMT_MSA.1	Not applicable	Not contributing directly to an SFR of the composite product but providing baseline protection for the composite security architecture. No contradiction to Composite-ST
FMT_MSA.3	Not applicable	Not contributing directly to an SFR of the composite product but providing baseline protection for the composite security architecture. No contradiction to Composite-ST
FMT_SMF.1	Not applicable	Not contributing directly to an SFR of the composite product but providing baseline protection for the composite security architecture. No contradiction to Composite-ST
FCS_COP.1/DES	FCS_COP.1/COS_3TDES	The composite TOE uses the 3DES cryptographical operation of the IC for encryption and decryption needed for secure messaging. No contradiction to Composite-ST
FCS_COP.1/AES	FCS_COP.1/COS.AES	The composite TOE uses the AES cryptographical operation of the IC for encryption and decryption needed for secure messaging and authenticatioin. No contradiction to Composite-ST
FCS_COP.1/RSA	FCS_COP.1/COS.RSA FCS_COP.1/COS.RSA.S FCS_COP.1/COS.RSA.V	The TOE uses the coprocessor for modular exponentiation and Large integer operation. The RSA crypto library functionality is not used. No contradiction to Composite-ST
FCS_COP.1/ECDSA	FCS_COP.1/COS.ELC FCS_COP.1/COS.ECDSA.V FCS_COP.1/COS.ECDSA.S	The composite TOE uses the ECC cryptographical operation of the IC for encryption, decryption and signature generation and verification. No contradiction to Composite-ST
FCS_COP.1/ECDH	FCS_COP.1/COS.ELC	The platform provides functionality for implementation of a DH key exchange protocol.
FCS_COP.1/SHA	not applicable	Extended functionality provided by the IC which is not used by the composite TOE. No contradiction to Composite-ST

Platform SFRs	Usage by TOE, TOE-SFR	Result
FCS_CKM.1/RSA	FCS_CKM.1/RSA	The platform provides RSA key generation functionality.
FCS_CKM.1/EC	FCS_CKM.1/ELC	The platform provides cryptographic operations which are used for the ELC key generation.
FDP_SDI.1	Not applicable	Internal operations of the IC No contradiction to Composite-ST
FDP_SDI.2	Not applicable	Internal operations of the IC No contradiction to Composite-ST
FPT_TST.2	Not applicable	Extended functionality provided by the IC No contradiction to Composite-ST

Table 2: Coverage of IC platform SFRs

11.2 Statement of compatibility for the security assurance requirements

This statement of compatibility address the requirement specified in **[EXS_CCDB_COMP]** for the security assurance requirements.

The security requirement for the underlying IC M7892 B11 specified in its security target **[ST_IC]** is EAL5 augmented with the following components: ALC_DVS.2 and AVA_VAN.5 where the security assurance requirement for the composite TOE is EAL4 augmented with the following components: ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

Therefore, the security assurance requirements for the composite TOE represent a subset of the security assurance requirements of the underlying platform.

11.3 Statement of compatibility for the security environment and the security objectives

11.3.1 Security objectives

The **[ST_IC]** is conformant to the standard IC platform security objectives defined in **[BSI_PP_IC]**. The security objectives defined in **[BSI_PP_IC]** are directly used as part of the PP for the COS **[BSI_PP_EHC_G2]**. This ST is conformant to **[BSI_PP_EHC_G2]** and so there is no conflict between security objectives of the

Composite Security Target and the IC Security Target. All IC platform security objectives are relevant.

The additional security objectives of the platform O.Add-Functions and O.Mem-Access provides additional specific security functionality for the TOE and do not contradict to the Composite-ST.

Security objectives for the IC	Security objectives for the composite TOE	Remarks
O.Phys-Manipulation (not relevant for compatibility)	O.Phys-Manipulation	Security objective is identical to one in **[BSI_PP_IC]**
O.Phys-Probing (not relevant for compatibility)	O.Phys-Probing	Security objective is identical to one in **[BSI_PP_IC]**
O.Malfunction	O.Malfunction	Security objective is identical to one in **[BSI_PP_IC]**
O.Leak-Inherent (not relevant for compatibility)	O.Leak-Inherent	Security objective is identical to one in **[BSI_PP_IC]**
O.Leak-Forced	O.Leak-Forced	Security objective is identical to one in **[BSI_PP_IC]**
O.Abuse-Func	O.Abuse-Func	Security objective is identical to one in **[BSI_PP_IC]**
O.Identification (not relevant for compatibility)	O.Identification	Security objective is identical to one in **[BSI_PP_IC]**
O.RND	O.RND	Security objective is identical to one in **[BSI_PP_IC]**
O.Add-Functions		Adds additional service (selection of optional libraries) to the composite product with no contradiction to the Composite-ST.
O.Mem Access		Adds additional services to the composite product with no contradiction to the Composite-ST.
OE.Plat-Appl	OE.Plat-COS	Identical to corresponding one in **[BSI_PP_IC]** according to the operational environment
OE.Resp-Appl	OE.Resp-ObjS	Identical to corresponding one in **[BSI_PP_IC]** according to the operational environment
OE.Process-Sec-IC	OE.Process-Card	Identical to corresponding one in **[BSI_PP_IC]** according to the operational environment

Table 3: Coverage of IC platform security objectives

Note that all additional security objectives on the environment for the composite TOE are for the operational environment, and do not contradict the IC security objectives.

11.3.2 Threats

There is no conflict between threats of the Composite Security Target and the IC Security Target.

Threats for the IC	Threats for the composite TOE	Remarks
T.Phys-Manipulation (not relevant for compatibility)	T.Phys-Manipulation	Threat is identical to one in **[BSI_PP_IC]**
T.Phys-Probing (not relevant for compatibility)	T.Phys-Probing	Threat is identical to one in **[BSI_PP_IC]**
T.Malfunction	T.Malfunction	Threat is identical to one in **[BSI_PP_IC]**
T.Leak-Inherent (not relevant for compatibility)	T.Leak-Inherent	Threat is identical to one in **[BSI_PP_IC]**
T.Leak-Forced	T.Leak-Forced	Threat is identical to one in **[BSI_PP_IC]**
T.Abuse-Func	T.Abuse-Func	Threat is identical to one in **[BSI_PP_IC]**
T.RND	T.RND	Threat is identical to one in **[BSI_PP_IC]**
T.Mem-Access	No correspondence	Additional thread which is taken into account by the composite product. No contradiction to composite-ST

Table 4: Coverage of threats

11.3.3 Organisational security policies

There is no conflict between OSPs of the Composite Security Target and the IC Security Target.

OSPs for the IC	OSPs for the composite TOE	Remarks
P.Process-TOE (not relevant for compatibility)	P.Process-TOE	Policy is identical to one in **[BSI_PP_IC]**
P.Add-Functions	No correspondence	Additional policy which is taken into account by the composite product. No contradiction to composite-ST

Table 5: Coverage of OSPs

The P.Add-functions introduces the IC cryptographic services to be used by the embedded software. There is no contradiction with the threats or security objectives for the composite TOE.

11.3.4 Assumptions

There is no conflict between assumption of the Composite Security Target and the IC Security Target.

Assumption for the IC	Assumptions/ Security objectives/SAR for the composite TOE	Remarks
A.Process-Sec-IC	Covered by OE.Process-Sec-IC	Taken over by **[BSI_PP_IC]**
A.Plat-Appl	Refined by A.Plat-COS (covered by OE.Plat-COS)	Identical to corresponding one in **[BSI_PP_IC]** according to the operational environment
A.Resp-Appl	Refined by A.Resp-ObjS (covered by OE.Resp-ObjS)	Identical to corresponding one in **[BSI_PP_IC]** according to the operational environment
A.Key-Function	Covered by OE.Plat-Appl and OE.Resp-Appl	Assumption is covered by internal programming guidelines supported by SFRs according to O.Leak-Inherent and O.Leak-Forced and the SFR FMT_MTD.1/NE

Table 6: Coverage of assumptions

There is only one significant assumption for the composite TOE that is fully addressed by the current composite security target.

Note that all additional assumptions for the composite TOE are for the operational environment, and do not contradict the IC threats.