IDEMIA

# SECURITY TARGET LITE

## IDEMIA_HC_GERMANY_NEO_G2.1_COS, V3

Version: V1.29

Date: 2025-07-07

# About IDEMIA

OT-Morpho is now IDEMIA, the global leader in trusted identities for an increasingly digital world, with the ambition to **empower** citizens and consumers alike to interact, pay, connect, travel and vote in ways that are now possible in a connected environment.

Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, we reinvent the way we think, produce, use and protect this asset, whether for individuals or for objects. We ensure privacy and trust as well as guarantee secure, authenticated and verifiable transactions for international clients from Financial, Telecom, Identity, Security and IoT sectors.

With close to €3bn in revenues, IDEMIA is the result of the merger between OT (Oberthur Technologies) and Safran Identity & Security (Morpho). This new company counts 14,000 employees of more than 80 nationalities and serves clients in 180 countries.

# Evolutions of the Document

| REVISION | IDEX | DATE | NATURE OF MODIFICATION |
|---|---|---|---|
| V1.00 | N/A | 2019-11-04 | First issue |
| V1.01 | N/A | 2019-11-08 | Corrected missing SHA 512 |
| V1.02 | N/A | 2020-06-23 | Multiple modifications |
| V1.03 | N/A | 2020-06-26 | Add Errata Sheet Reference |
| V1.04 | N/A | 2020-06-26 | Some minor corrections |
| V1.05 | N/A | 2020-07-02 | Add delivery content |
| V1.26 | N/A | 2025-06-23 | Multiple modifications |
| V1.27 | N/A | 2025-06-25 | Editorial modifications |
| V1.28 | N/A | 2025-07-02 | Editorial modifications |
| V1.29 | N/A | 2025-07-07 | Editorial modifications |

# Table of content

# List of tables

# List of figures

# 1 ST Introduction

## 1.1 ST and TOE Reference

This Security Target refers to the smartcard product "IDEMIA_HC_Germany_NEO_G2.1_COS, V3" (TOE) provided by Idemia for a Common Criteria evaluation.

| | |
|---|---|
| Title: | Security Target – IDEMIA_HC_Germany_NEO_G2.1_COS, V3 |
| Document Category: | Security Target for a CC Evaluation |
| Version: | V1.29 |
| Publisher: | Idemia |
| Confidentiality: | **PUBLIC** |
| TOE: | "IDEMIA_HC_Germany_NEO_G2.1_COS, V3" (Smartcard Product containing IC with Smartcard Embedded Software, intended to be used within the German Health Care System) |
| CertificationID: | BSI-DSZ-CC-1261 |
| 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 5 [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.

### 1.1.1 Security Target and TOE Identification

Security Target identification is described in the table below:

| **ST Identification** | **Security Target Lite – IDEMIA_HC_Germany_NEO_G2.1_COS, V3 / BSI-DSZ-CC-1261** |
|---|---|
| Version | V1.29 |
| Origin | Idemia |
| TOE Identification | IDEMIA_HC_Germany_NEO_G2.1_COS, V3 |
| Administration guidance | AGD_INI/PERS |
| User guidances | AGD_OPE |
| Chip Identifier | Chip family H13, Infineon Technologies AG |
| Chip Ref. Certificate | BSI-DSZ-CC-1110-V7-2024 |
| Assurance Level | 4+ |
| CC Version | 3.1 Release 5 |

### 1.1.2 Referenced Literature

| Reference | Description |
|---|---|
| [AGD_OPE] | Title: IDEMIA_HC_GERMANY_NEO_G2.1_COS, V3 - Operational User Guidance<br>Version: V2.7<br>Publisher: IDEMIA |
| [AGD_PRE] | Title: IDEMIA_HC_GERMANY_NEO_G2.1_COS, V3 Preparative Guidance AGD_PRE<br>Version: 1.16<br>Publisher: IDEMIA |
| [AGD_WRP] , [DEV_FSP_WRP] | Title: IDEMIA_HC_GERMANY_G2.1_COS, V3 – Wrapper Guidance<br>Category: AGD_OPE<br>Identification: 2018_2000039571<br>Version: V1.13<br>Publisher: IDEMIA |
| [ASE_ST] | Title: SECURITY TARGET IDEMIA_HC_GERMANY_NEO_G2.1_COS, V3<br>Identification: 2018_2000039565<br>Version: V1.29<br>Publisher: IDEMIA |
| [ASE_STLITE] | Title: SECURITY TARGET LITE IDEMIA_HC_GERMANY_NEO_G2.1_COS, V3<br>Version: V1.29<br>Publisher: IDEMIA |
| [BSI_PP_EHC_G2], [BSI_PP_COS_G2] | Title: Common Criteria Protection Profile – Card Operating System Generation 2 (PP COS G2)<br>Identification: BSI-CC-PP-0082-V4<br>Version: 2.1<br>Publisher: Bundesamt für Sicherheit in der Informationstechnik (BSI) |
| [BSI_PP_IC], [11] | Title: Security IC Platform Protection Profile with Augmentation Packages<br>Identification: BSI-PP-0084-2014<br>Version: 1.0<br>Publisher: Bundesamt für Sicherheit in der Informationstechnik (BSI) |

| Reference | Description |
|---|---|
| [CC] | Title: Common Criteria for Information Technology Security Evaluation, Part 1-3<br>Version: 3.1 Revision 5 |
| [CC_P1] | Title: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model<br>Identification : CCMB-2017-04-001<br>Version : Version 3.1 Revision 5 |
| [DIRECTIVE] | Title: DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a community framework for electronic signatures |
| [EMV´96] | Title: Integrated Circuid Card Specification for Payment Systems<br>Identification: EMV´96<br>Version: 3.1.1<br>Date: 1998-05-31<br>Publisher: Europay International S.A., MasterCard International |
| [EMV2000] | Title: EMV2000 Integrated Circuit Card Specification for Payment Systems<br>Version: Version 4.0<br>Date: 2000-12<br>Author: EMV<br>Publisher: EMV |
| [EXS_BSI_TR_3116_1], [19] | Title: BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung – Teil 1: Telematikinfrastruktur<br>Version: 3.20<br>Publisher: BSI |
| [EXS_BSI_ZK_G2] | Title: Technische Richtlinie BSI TR-3106 – eHealth – Zertifizierungskonzept für Karten der Generation G2<br>Version: 1.2<br>Publisher: BSI |
| [EXS_EHC_COS], [21] | Title: Spezifikation des Card Operating System (COS)<br>Version: 3.12.0<br>Publisher: gematik mbH |

| Reference | Description |
|---|---|
| [EXS_EHC_CRY] | Title: Übergreifende Spezifikation - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur<br>Version: 2.22.0<br>Publisher: gematik mbH |
| [EXS_EHC_EGK], [23], [24] | Title: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem (G2.1)<br>Version: 4.6.0<br>Publisher: gematik mbH<br><br>Title: Spezifikation der Security Module Card SMC-B Objektsystem<br>Version: 5.0.0<br>Publisher: gematik mbH |
| [EXS_EHC_HBA], [22] | Title: Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem<br>Version: 5.2.0<br>Publisher: gematik mbH |
| [EXS_EHC_KFT] | Title: Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1<br>Version: 3.0.0<br>Publisher: gematik mbH |
| [EXS_EHC_OM] | Title: Übergreifende Spezifikation Operations und Maintenance<br>Version: 1.14.0<br>Publisher: gematik mbH |
| [EXS_EHC_PKI] | Title: Übergreifende Spezifikation - Spezifikation PKI<br>Version: 2.12.0<br>Publisher: gematik mbH |
| [EXS_EHC_SDS] | Title: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller<br>Version: 1.3.0<br>Publisher: gematik mbH |
| [EXS_EHC_TLK_COS] | Title: Spezifikation der Testlaborkarte COS / Objektsysteme<br>Version: 2.0.0<br>Publisher: gematik mbH |

| Reference | Description |
|---|---|
| [EXS_JIL_COMP], [8] | Title : Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices<br>Version : 1.5.1<br><br>Publisher : JIL |
| [EXS_NIST_SP800_38A] | Title: NIST Special Publication 800-38A,<br>Recommendation for Block,<br>Cipher Modes of Operation, Methods and Techniques<br>Identification: 800-38A 2001 ED<br><br>Author: Morris Dworkin<br>Publisher: NIST |
| [EXS_WRP_COS], [27] | Title: Spezifikation Wrapper<br>Version: 1.8.0<br><br>Publisher: gematik mbH |
| [GSM11.11] | Title: Digital cellular telecommunications system (Phase 2+);<br>Specification of the Subscriber Identity Module -<br>Mobile Equipment (SIM - ME) interface<br>Identification: ETSI TS 100 977<br>Version: V8.3.0<br><br>Publisher: European Telecommunications Standard Institute (ETSI) |
| [GSM11.12] | Title: Digital cellular telecommunications system (Phase 2);<br>Specification of the 3 Volt Subscriber Identity Module -<br>Module - Mobile Equipment (SIM-ME) interface<br>Identification: ETS 300 641<br>Version: 4.3.1<br><br>Publisher: European Telecommunications Standards Institute (ETSI) |
| [GSM11.17] | Title: Digital cellular telecommunications system (Phase 2+)<br>Subscriber Identity Module (SIM)<br>conformance test specification<br>Identification: ETSI EN 301 086<br>Version: 7.0.2<br><br>Publisher: European Telecommunications Standards Institute (ETSI) |

| Reference | Description |
|---|---|
| [GSM11.18] | Title: ETSI TS 101 116 Digital cellular telecommunication system (Phase 2+); Specification of the 1.8 Volt Subscriber Identity Module - Mobile Equipment (SIM-ME) interface<br>Version: V7.0.1<br>Author: ETSI |
| [HSL_UG] | Title: Hardware Support Library for SLCx2 (HSL) User Guidance<br>Version: v03.12.8812<br>Publisher: Infineon Technologies AG |
| [IC_CL_UG], [ACL_UI] | Title: CL52 Asymmetric Crypto Library for Crypto@2304T, RSA / ECC / Toolbox, 16-bit Security Controller, User Interface<br>Version: 2.9.002<br>Publisher: Infineon Technologies AG |
| [IC_SG] | Title: 16-bit Security Controller – V01, Security Guidelines (SG)<br>Version: 1.01-2596<br>Publisher: Infineon Technologies AG |
| [IC_UG] | Title: 16-bit Security Controller – V01, Hardware Reference Manual<br>Version: Revision 7.0<br>Publisher: Infineon Technologies AG |
| [IC_UG_PP] | Title: Production and Personalization, 16-bit Security Controller in 65 nm<br>Version: 3.6<br>Publisher: Infineon Technologies AG |
| [IC_UG_PR] | Title: 16-bit Security Controller - Programmer's Reference Manual (PRM)<br>Version: 9.14<br>Publisher: Infineon Technologies AG |
| [IFX_PROD_PERSO] | Title: Production and Personalization 16-bit Security Controller in 65nm, Rev. 3.3, |

| Reference | Description |
|---|---|
| [ISO_14443], [30b] | Title: Identification cards – Contactless integrated circuit cards Part 1-4<br>Identification: ISO/IEC 14443<br>Version: Edition 4<br>Publisher: International Organization for Standardization/ International Electrotechnical Commission |
| [ISO_7816_3], [28] | Title: Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocol.<br>Identification: ISO/IEC 7816-3<br>Version: Edition 3<br>Publisher: International Organization for Standardization/ International Electrotechnical Commission |
| [JIL_ADV_ARC1] | Title: Security Architecture Requirements (ADV_ARC) for Smartcards and Similar Devices<br>Version: 2.00<br>Publisher: Joint Interpretation Library |
| [JIL_ADV_ARC2] | Title: Security Architecture Requirements (ADV_ARC) for Smartcards and Similar Devices – Appendix 1<br>Version: 2.00<br>Publisher: Joint Interpretation Library |
| [JIL_ATP_SC] | Title: Application of Attack Potential to Smartcards<br>Version: 3.0<br>Publisher: Joint Interpretation Library |
| [MSSR] | Title: Joint Interpretation Library Minimum Site Security Requirements<br>Version: 2.1 (for trial use) |
| [PP_EIDAS] | Title: Protection profiles for secure signature creation device – Parts 1, 2, 4, 5<br>Identification: DIN EN 419211<br>Publisher: DIN Deutsches Institut für Normung e. V. |

| Reference | Description |
|---|---|
| [SCL_UI] | Title: SCL52-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 DES / AES 16-bit Security Controller, User Interface<br>Version: 2.04.002<br><br>Publisher: Infineon Technologies AG |
| [ST_IC], [100] | Title: Security Target IFX_CCI_000003h IFX_CCI_000005h IFX_CCI_000008h IFX_CCI_00000Ch IFX_CCI_000013h IFX_CCI_000014h IFX_CCI_000015h IFX_CCI_00001Ch IFX_CCI_00001Dh IFX_CCI_000021h IFX_CCI_000022h H13<br>Version: 5.1<br><br>Author: Hans Ulrich Buchmüller<br>Publisher: Infineon Technologies AG |
| [TS 102 221] | Title: Smart Cards; UICC-Terminal interface; Physical and logical characteristics<br>Version: V4.0.0<br><br>Author: ETSI<br>Publisher: ETSI |
| [TS 131 101] | Title: ETSI TS 131 101 Universal Mobile Telecommunication System (UMTS); UICC-Terminal Interface; Physical and Logical Characteristics<br>Version: V3.2.0<br><br>Author: ETSI<br>Publisher: ETSI |
| [TS 131 122] | Title: Universal Mobile Telecommunications Systems (UMTS); USIM Conformance Test Specification;<br>Version: V3.0.0<br><br>Author: ETSI<br>Publisher: ETSI |
| [TS 31.120] | Title: 3rd Generation Partnership Project; Technical Specifiaction Group Terminals; UICC-Terminal Interface; Physical, Electrical and Logical Test Specification<br>Version: V1.0.0 (2000-08)<br><br>Author: 3GPP<br>Publisher: 3GPP |

| Reference | Description |
|---|---|
| [ZKA41] | Title: Schnittstellenspezifikation für die ZKA-Chipkarte<br>Version: 4.1<br><br>Publisher: ZKA |

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

##### 1.1.2.1.1 Common Criteria


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

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017

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

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

[5] AIS20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[6] AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

[9] Joint Interpretation Library – The Application of CC to Integrated Circuits, Version 3.0, February 2009, JIL

[10] Joint Interpretation Library – Guidance for smartcard evaluation, Version 2.0, February 2010, JIL


##### 1.1.2.1.2 Technical Guidelines and Specifications


[16] Technical Guideline BSI TR-03110:

Technical Guideline BSI TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1: eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26 February 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Technical Guideline BSI TR-03110-2: Advanced Security Mechanisms for Machine Readable Travel

Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 21 December 2016, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Technical Guideline BSI TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel

Documents and eIDAS Token – Part 3: Common Specifications, Version 2.21, 21 December 2016, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[17] Technical Guideline BSI TR-03111: Elliptic Curve Cryptography, Version 2.10, 01.06.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[18] Technische Richtlinie BSI TR-03114: Stapelsignatur mit dem Heilberufsausweis, Version 2.0, 22.10.2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[20] Technische Richtlinie BSI TR-03143: eHealth – G2-COS Konsistenz-Prüftool, Version 1.1, 18.05.2017

[25] cf. [26]

[26] Spezifikation gSMC-KT Objektsystem, Version 4.2.0, 15.05.2019, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

#### 1.1.2.1.3 ISO Standards

[29] ISO/IEC 7816-4:2013 (3rd edition), Identification cards – Integrated circuit cards – Part 4: Organisation, security and commands for interchange

[30] ISO/IEC 7816-8:2016 (3rd edition), Identification cards – Integrated circuit cards – Part 8: Commands and mechanisms for security operations

[30a] ISO/IEC 7816-9:2017 (3rd edition), Identification cards – Integrated circuit cards – Part 9: Commands for card management

[200] ISO/IEC 14888-3:2006, Technical Corrigendum 2, published 15.02.2009, Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms

#### 1.1.2.1.4 Cryptography

[31] ISO/IEC 9796-2:2010 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

[33] Federal Information Processing Standards Publication 197 (FIPS PUB 197), ADVANCED ENCRYPTION STANDARD (AES), 26 November 2001, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology (NIST)

[34] PKCS #1, RSA Cryptography Standard, Version 2.2, 27 October 2012, RSA Laboratories

[35] PKCS #3, Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised 1 November 1993, RSA Laboratories

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

[37] Federal Information Processing Standards Publication 180-4 (FIPS PUB 180-4), SECURE HASH STANDARD (SHS), 5 August 2015 (includes updates as of 10-06-2016), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology (NIST)

[39] American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 16 November 2005, ANSI

[40] American National Standard X9.63-2011 (R2017), Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 21 December 2011 (reaffirmed 10 February 2017), ANSI

[41] Elliptic Curve Cryptography (ECC), Brainpool Standard Curves and Curve Generation, RFC 5639, March 2010

[201] IEEE 1363, IEEE Standard Specification for Public key Cryptography, IEEE Standards Board, 30.01.2000

#### 1.1.2.1.5 Other Sources

[42] (shifted to [30b])

[43] VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

[44] DURCHFÜHRUNGSBESCHLUSS (EU) 2016/650 DER KOMMISSION vom 25. April 2016 zur Festlegung von Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten gemäß Artikel 30 Absatz 3 und Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

#### 1.1.2.1.6 Additional references

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

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

[101] Certification Report BSI-DSZ-CC-1110-V3-2020 for Infineon Security Controller IFX_CCI_000003h,000005h, 000008h, 00000Ch, 000013h, 000014h,000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions, Version 1.0, 13.05.2020, Infineon Technologies AG

## 1.2 TOE Overview

### 1.2.1 TOE definition and operational usage

The Target of Evaluation (TOE) addressed by the present Security Target is a smart card platform implementing the Card Operating System (COS) according to [21] without any object system.

The TOE comprises the following components:

- Integrated Circuit (IC) family H13 with Crypto Libraries ACL v2.09.002, SCL v02.04.002 and Hardware Support Library (HSL) v03.12.8812 provided by Infineon Technologies AG
- Smartcard Embedded Software comprising the IDEMIA_HC_Germany_NEO_G2.1_COS, V3 as Card Operating System Card (designed as flash implementation) for the German Health Care System provided by Idemia
- The wrapper for interpretation of exported TSF data
- The associated guidance documentation

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

All components of the TOE will only be used within the German Health Care System and will not be delivered to other parties.

The object system is not part of the TOE. Such the TOE will be configured after production as eHC by Idemia/external personalizer prior to the delivery of the smartcard platform.

The TOE supports contactless communication, whereby the inlay with antenna is not part of the TOE covered by the evaluation.

The guidance documentation describes the security measures provided by the manufacturer and the security measures required for protection of the TOE until reception by the end-user.

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 1.3.4.

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

### 1.2.2 TOE major security features for operational use

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.

### 1.2.3 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].

### 1.2.4 Non-TOE Hardware/Software/Firmware

In order to be powered up and to communicate with the 'external world' the TOE needs a terminal (card reader) with contacts [28] or supporting the contactless communication according to [30b].

### 1.2.5 Options and Packages

The COS specification [21] defines different options which the TOE may implement. The ST takes account of these options by using the so-called Package concept known in the CC and defining corresponding Packages as follows:

| Option in [21] | Package in [BSI_PP_EHC_G2] | Remark | Supported by the TOE |
|---|---|---|---|
| Option_Kryptobox | Crypto Box | Defines additional cryptographic SFRs | NO |
| Option_kontaktlose_Schnittstelle | Contactless | Defines additional SFRs for the support of the contactless interface of the smart card, i.e. PICC part of PACE (see section 7). | YES |
| Option_PACE_PCD | PACE for Proximity Coupling Device | Defines additional SFRs for the support of the contactless interface of the terminal, i.e. PCD part of PACE. | NO |
| Option_logische_Kanäle | Logical Channel | Defines additional SFRs for the support of logical channels (see section 8). | YES |
| Option_USB_Schnittstelle | --- | Defines additional communication support on the lower layers. This option does not contain any security related details and is therefore only listed in this table for the sake of completeness. | NO |
| Option_RSA_CVC | RSA CVC | Defines additional cryptographic SFRs for the support of RSA functionality that is related to CVCs (see section 9). | NO |
| Option_RSA_KeyGeneration | RSA Key Generation | Defines an additional cryptographic SFR for the support of RSA key generation functionality (see section 10). | YES |

**Table 1: Mapping between Options and Packages / Supported Options**

The Common Criteria for IT Security Evaluation [1], [2], [3] define a Package as a set of SFR or SAR. This approach does not necessarily fit for description of extended TSF due to extended functionality of the TOE by means of Packages. Therefore it was decided to provide an extension of the Security Problem Definition, the Security Objectives, and the Security Requirements as well as for the corresponding rationales for each defined Package.

The ST author incorporates the corresponding Package definition with the update of the Security Problem Definition, Security Objectives, and the Security Requirements defined in that Package into this ST. Additionally, all rationales are taken over into this ST.

*Application note 1:* The ST author describes in the section Conformance Claim, section Package claim which Package was chosen and in section Conformance Rationale how these Packages are incorporated in the ST. Note that the chosen Packages may require support of commands or only special variants of the commands, cf. [21] for details.

*Application note 2:* The ST is written from the security point of view. In some cases this can result in different interpretations how security is enforced. For example from the implementation point of view the command ENABLE VERIFICATION REQUIREMENT changes a security state within the memory of the TOE. From the security point of view the change of the security state results in a change of the access rules. The ST describes rather the requirements for the security 28tandard and does not focus on the implementation details claimed by [21]. The user reading this ST should therefore keep in mind that the ST abstracts from the implementation.

The Protection Profile BSI-CC-PP-0084-2014 [11] defines optional Packages which the Security IC Platform may implement and which may be relevant for the TOE. The following table gives an overview of the optional Packages, which Packages are implemented by the Security IC Platform according to [ST_IC] and which Packages are relevant for this TOE:

| Optional Package in [11] | Implemented in [ST_IC] | Relevant for the TOE | Remark |
|---|---|---|---|
| Authentication of the Security IC | YES | YES | The TOE requires unique identification of the TOE |
| Loader 1 | YES | NO | The secure loader functionality of the IC Platform is no longer available after TOE delivery |
| Loader 2 | YES | NO | |
| TDS | YES | NO | Option "Option_DES" is not supported by the TOE |
| AES | YES | YES | The TOE uses secure hardware based cryptographic services for the AES for encryption and decryption |

**Table 2: Relevant optional Packages from BSI-CC-PP-0084-2014 [11]**

In addition to optional packages, the IC Platform Security Target [ST_IC] covers a set of functionalities whereby not all are used by the present TOE. The following table gives an overview of that functionality and if they are used:

| Functionality within [ST_IC] | Used by the TOE |
|---|---|
| ACL v2.09.002: RSA2048 incl. key generation | NO |
| ACL v2.09.002: RSA4096 incl. key generation | YES |
| ACL v2.09.002: EC key generation, ECDSA, ECDH | YES |
| ALC v2.08.007, ACL v2.06.003, ACL v2.07.003 | NO |
| CIPURSE™ | NO |
| TDES | NO |
| SCL v2.04.002: AES, CMAC | YES |
| SCL v2.02.010: AES, CMAC | NO |
| AES by SCP | NO |
| Random number generation: HPRG | YES |

| | |
|---|---|
| Random number generation: DRNG, KSG, TRNG | NO |
| HSL v03.12.8812 | YES |
| HSL v03.11.8339 | NO |
| HSL v02.01.6634 | NO |
| HSL v01.22.4346 | NO |
| NRG Software | NO |

**Table 3: Relevant optional Functionality from the IC Platform Security Target [ST_IC]**

## 1.3 TOE Description

### 1.3.1 Physical Scope of the TOE

#### 1.3.1.1 Contact based communication

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 4 for communication. For details see [IG_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 4: Chip pins**

The Infineon Integrated Circuit family H13 offers a serial communication interface fully compatible with the ISO/IEC 7816-3 standard (T=1).

For details, see [ISO_7816_3].

#### 1.3.1.2 Contactless communication

The contactless interface of the TOE related to the usage as a smart card consists of the use of RF-Interface according to ISO/IEC 14443. For details see [IC_UG].

The Infineon Integrated Circuit family H13 offers a contactless communication interface fully compatible with the ISO/IEC 14443 standard (Transmission protocol Type A).

For details, see [ISO_14443].

### 1.3.2 Logical Scope of the TOE

The following figure provides an overview of the logical structure of the card operating system.

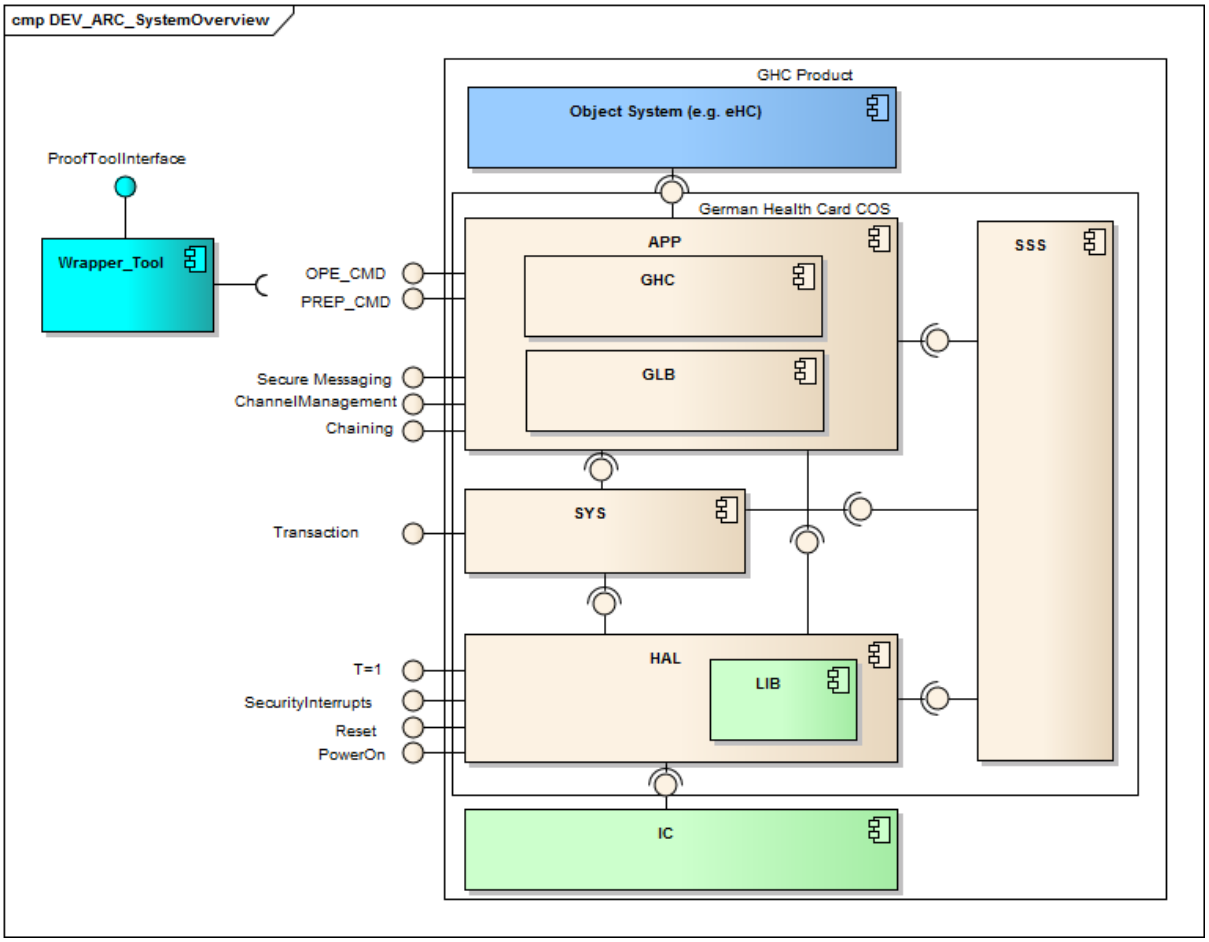



**Figure 1: Logical Structure of the Card Operating System**

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 33tandardized 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 IDEMIA_HC_Germany_NEO_G2.1_COS, V3 implements the 33tandardized 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 resp. of the Type A RF-interface (contactless).

Additionally, the smart card operating system reacts on specific external events, 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.

The operating system is internally decomposed into a set of system elements which form the high-level components of the system. The application layer (APP) implements the product specific functionality which support card products intended to be used in the German Health Care system. This system element is split into the subsystem GHC which is responsible for processing the commands and a supportive subsystem GLB which implements the fundamental system structures like the file system, the system state etc.

The application layer receives support from the system element SYS which implements reusable operating system services. This layer in turn is based on a hardware abstraction layer HAL which is responsible for providing a unique interface to the elementary mechanisms provided by various security ICs. Such mechanisms include an

abstraction for basic memory accesses and other hardware dependent features but also access to elementary cryptographic primitives either accessed to the IC dedicated crypto library or implemented by direct programming of the cryptographic co-processors.

All of the system elements can make use of shared system services provided by the SSS system element.

#### 1.3.2.1 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 Crypto Libraries y ACL and SCL used for cryptographic operations, and including Hardware Support Library HSL) 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].

**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 Libraries ACL v2.09.002, SCL v2.04.002 and Hardware Support Library (HSL) v03.12.8812 provided by Infineon Technologies AG<br><br>Detailed information on the IC Hardware, the IC Dedicated Software (in particular the Crypto Libraries) 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<br><br>Delivery of OS Flashing image<br><br>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 | |
| OS-PrePerso sequence | Command sequence used by the OS Pre-Personalizer to configure the Card Operating System. | SW | |
| Note:<br>A detailed overview of the different procedural variants which are supported by the product can be found in Chapter 1.3.3. | | | |
| IDEMIA_HC_Germany_NEO_G2.1_COS V3–Operational User Guidance | User guidance for the User of the GHC G2 COS V3.0 platform | DOC | Document in paper / electronic form |
| IDEMIA_HC_Germany_NEO_G2.1_COS V3–OS Preparation Guidance<br><br>IDEMIA_HC_Germany_NEO_G2.1_COS V3–Object System 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 |
|---|---|---|---|
| IDEMIA_HC_Germany_NEO_G2.1_COS V3 – 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 |
| IDEMIA_HC_Germany_NEO_G2.1_COS V3 –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<br>Note: The card´s authentication key pair is generated by 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<br>Note: The card´s personalisation key pair is generated by 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 |
| Object System Signature Key | Object System Signature Key, needed for calculation of the Signature over an Object System. | KEY | Document in paper / electronic file |
| OS-PrePersonalizer Master Key | Key for derivation of card individual authentication keys | KEY | Document in paper / electronic file |
| K_OPE_DEC | Key needed for encryption of secrets in Load Application sequences. | KEY | Document in paper / electronic file |
| K_OPE_VERIFICATION | Key needed to calculate a Signature over Load Application sequences. | KEY | Document in paper / electronic file |

**Table 5: Deliverables associated to the TOE**

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.

Note: Additionally a PrePersoScript is shipped to the Product PrePersonaliser. The PrePersoScript is a specific command sequence sent to the card by the Product Pre-Personaliser to create internally the non card individual data.

The PrePersoScript is not part of the TOE, and therefore not listed in the table above.

### 1.3.3 Life Cycle Overview

This chapter describes the details of the life-cycle model of a German Health Card product developed by Idemia. The description is based on a generic life-cycle model used by 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.

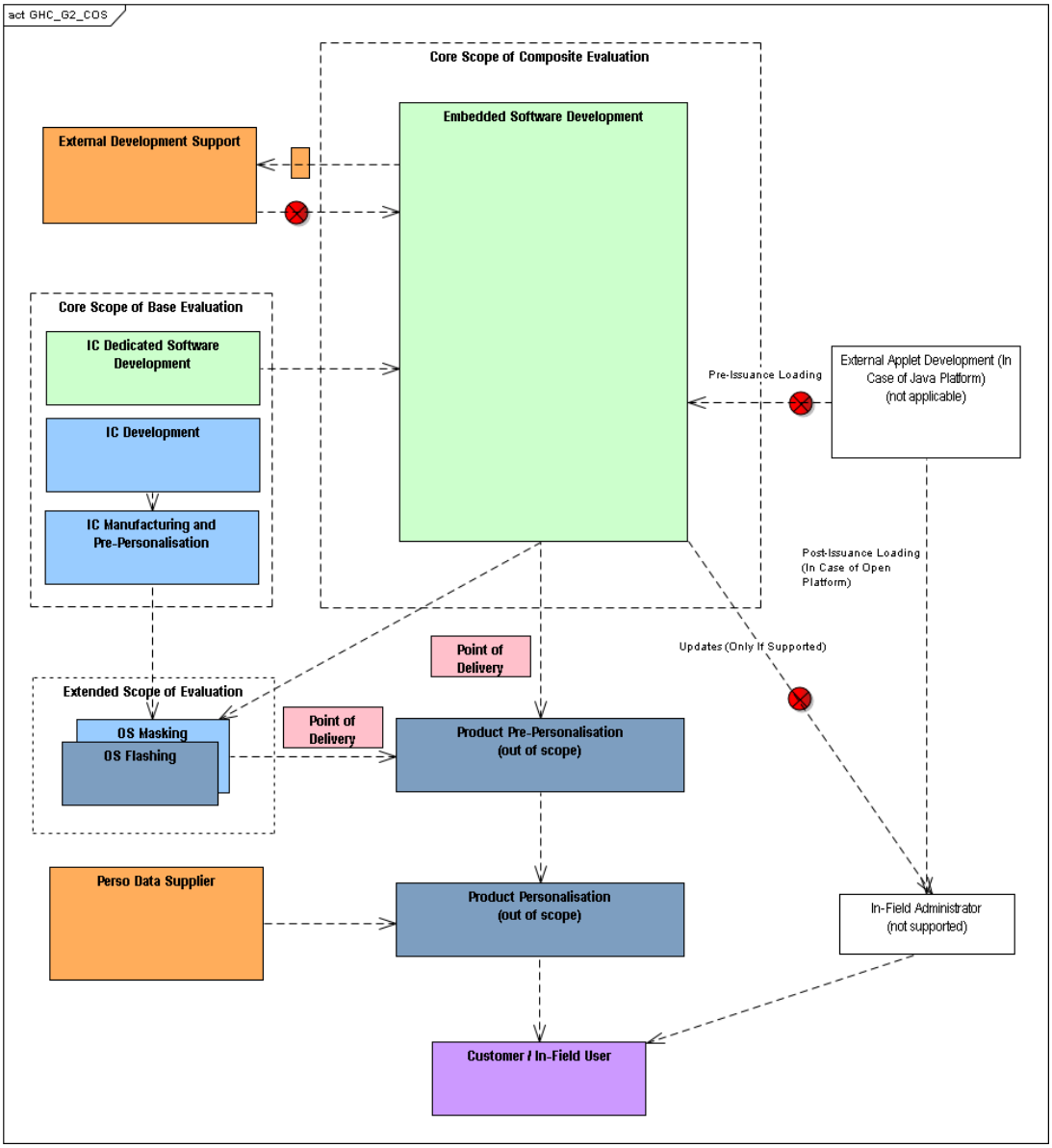



**Figure 2: Life Cycle Overview**

For the IDEMIA_HC_Germany_NEO_G2.1_COS, V3 product the generic 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 and pre-personalisation data from the 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 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 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.
- 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 IDEMIA_HC_Germany_NEO_G2.1_COS, V3 product there are different possible technical and procedural production variants according to the generic life-cycle model.

### 1.3.4 Definition of the Evaluation Scope

The following 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.

### 1.3.5 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 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.
- To IDEMIA Flintbek for inhouse Pre-Personalisation and (optionally) Personalisation as a non-pre-personalised smartcard 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.

In the second case, Idemia may ship the product

- to an external Product Personaliser as pre-personalised smartcard, 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 Idemia conducts the Product Pre-Personalisation, but not the Product 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 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 Idemia.
- The delivery of the OS Flash data from Idemia to Infineon Technologies AG or to Idemia production facilities depending on the responsibilities for flash loading. Additionally, personalisation key data is shipped in this step.

### 1.3.6 TOE Intended Usage

Introducing information on the intended usage of the TOE is given within Chapter 1.2. 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 IDEMIA_HC_Germany_NEO_G2.1_COS, V3 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 IDEMIA_HC_Germany_NEO_G2.1_COS, V3 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 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, 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 functionality)
- 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 IDEMIA_HC_Germany_NEO_G2.1_COS, V3 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 processing)
- 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.

### 1.3.7 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 | Card Product Development |
| Device | OS FlashLoader | OS Flashing |
| Device | OS PrePersonaliser | OS PrePersonalisation<br>(coupled with OS Flashing or Product Pre-Personalisation) |
| Device | OS Personaliser,<br>sub role Product Pre-Personaliser | OS Personalisation,<br>sub step Product Pre-Personalisation |
| Device | OS Personaliser,<br>sub role Product Personaliser | OS Personalisation,<br>sub step Product Personalisation |
| Human User | Card Holder | In Field Usage<br>(no production step) |
| Device | Device for Operational Phase | In Field Usage<br>(no production step) |
| World | User of Wrapper | Verification according to Technical Guidance TR-03143<br>(no production step) |

**Table 6: Role mapping to Production Roles**

# 2 Conformance Claims

## 2.1 CC Conformance Claim

This Security Target claims conformance to

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

as follows

- Part 2 extended,
- Part 3 conformant.

The
Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017, [4]
is taken into account.

## 2.2 PP Claim

This Security Target claims strict conformance to the Protection Profile BSI-CC-PP-0082-V4 [BSI_PP_EHC_G2].

## 2.3 Package Claim

The TOE includes the following optional packages described in Chapter 1.2.5 of the PP [BSI_PP_EHC_G2]:

- Package “Contactless”, section 7
- Package “Logical Channel”, section 8
- Package “RSA Key Generation”, section 9

The ST 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 [3].

## 2.4 Conformance Claim Rationale

This ST claims strict conformance to [BSI_PP_EHC_G2] which claims strict conformance to BSI-CC-PP-0084-2014 [11]. The IC Platform Security Target [ST_IC] claims strict conformance to BSI-CC-PP-0084-2014 [11].

From the Security Problem Definition (see section 3 "Security Problem Definition" [11]) of BSI-CC-PP-0084-2014 the Threats (see section 3.2 "Threats" [11]) and the Organisational Security Policies (see section 3.3 "Organisational Security Policies" [11]) are taken over into this Security Target. Namely the following Threats are taken over: T.Leak-Inherent, T.Phys-Probing, T.Malfunction, T.Phys-Manipulation, T.Leak-Forced, T.Abuse-Func, T.RND. The OSP P.Process-TOE is also taken over from BSI-CC-PP-0084-2014. In this ST all Threats and all OSPs are taken over from [BSI_PP_EHC_G2]. See section 3.2 and 3.3 for more details.

The Assumptions A.Process-Sec-IC and A.Resp-Appl defined in BSI-CC-PP-0084-2014 [11] address the operational environment of the Security IC Platform, i.e. the COS part of the present TOE and the operational environment of the present TOE. The aspects of these Assumptions are relevant for the COS part of the present TOE, address the development process of the COS and are evaluated according to the composite evaluation approach [8]. Therefore these Assumptions are now refined in order to address the Assumptions about the operational environment of the present TOE. In this ST all Assumptions are taken over from [BSI_PP_EHC_G2]. See section 3.4 for more details.

The Security Objectives for the Security IC Platform as defined in BSI-CC-PP-0084-2014 O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced, O.Abuse-Func, O.Identification, O.RND are included as Security Objectives for the present TOE. The Security Objective for the Operational Environment OE.Resp-Appl defined in BSI-CC-PP-0084-2014 is split into the Security Objective O.Resp-COS for the COS part of the TOE and the Security Objectives OE.Plat-COS and OE.Resp-ObjS for the object system in the operational environment of the TOE. In addition, the aspects relevant for the COS part of the present TOE are fulfilled in the development process of the COS and evaluated according to the composite evaluation approach [8]. The Security Objective for the Operational Environment OE.Process-Sec-IC defined in BSI-CC-PP-0084-2014 is completely ensured by the assurance class ALC of the TOE up to Phase 5 and addressed by OE.Process-Card. In this ST all Security Objectives for the

TOE and all Security Objectives for the Operational Environment of the TOE are taken over from [BSI_PP_EHC_G2]. See section 4 for more details.

The Security IC Platform makes use of optional Packages in BSI-CC-PP-0084-2014. The following packages are relevant for the present TOE: "Authentication of the Security IC" and "AES".

Therefore the following Threats, Organisational Security Policies, Security Objectives for the TOE and Security Objectives for the Operational Environment are taken over from BSI-CC-PP-0084-2014 [11]:

- T.Masquerade_TOE (see section 4.1 in [ST_IC] and section 7.2 in [11]),
- P.Crypto-Service (see section 4.2 in [ST_IC] and sections 7.3, 7.4 in [11]),
- O.Authentication and O.AES (see section 5.1 in [ST_IC] and sections 7.2, 7.3, 7.4 in [11], and
- OE.TOE_Auth (section 5.2 in [ST_IC] and 7.2, 7.3 in [11]).

Due to the augmentation of [11], the IC Platform Security Target [ST_IC] defines additional Threats, Organisational Security Policies, Assumptions and Security Objectives for the TOE:

- T.Mem-Access is taken over into this ST (see section 4.1 in [ST_IC]),
- P.Add-Functions is taken over into this ST (see section 4.2 in [ST_IC]),
- A.Key-Function is covered for this TOE by the Threats T.Leak-Inherent and T.Leak-Forced (see section 4.3 in [ST_IC]),
- O.Add-Functions, O.Mem-Access are taken over into this ST (see section 5.1 in [ST_IC]).

All Security Functional Requirements with existing refinements from BSI-CC-PP-0084-2014 [11] that are taken over into [BSI_PP_EHC_G2] by iterations indicated by "/SICP" are taken over into the present ST. Thereby the used optional packages in [11] are considered. Additionally, the augmentation of [11] in the IC Platform Security Target [ST_IC] is considered. See section 7.1 in [ST_IC]. Section 6.1.3 lists all Security Functional Requirements from [ST_IC] and which are taken over into this ST.

The Assurance Package claim is EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. For rationale of the augmantations see section 6.3.3.

The refinements of the Security Assurance Requirements made in BSI-CC-PP-0082-V4 [BSI_PP_EHC_G2] (which takes over the Security Assurance Requirements from BSI-CC-PP-0084-2014 [11]) are taken over into this Security Target.

According to section 1.2.5, the TOE makes use of optional Packages in the COS specification [21], by using the Package concept. The following Packages are supported by the TOE: "Contactless", "Logical Channel" and "RSA Key Generation".

All Threats, Organisational Security Policies, Assumptions, Security Objectives and Security Functional Requirements concerning the supported Packages are taken over from [BSI_PP_EHC_G2] into this ST. For Package “Contactless” see section 7, for Package “Logical Channel” see section 8 and for Package “RSA Key Generation” see section 9.

As all important parts (i.e. parts from SPD, objectives, SFRs, SARs) of BSI-CC-PP-0082-V4 [BSI_PP_EHC_G2], BSI-CC-PP-0084-2014 [11] and the IC Platform Security Target [ST_IC] that are relevant for this Security Target are referred in a way that these are part of this Security Target the rationales still hold. Please refer to sections 4.3, 6.3, 7.5, 8.5 and 9.5 for further details. Therefore the strict conformance with BSI-CC-PP-0082-V4 [BSI_PP_EHC_G2] and BSI-CC-PP-0084-2014 [11] is fulfilled by this Security Target.

# 3 Security Problem Definition

## 3.1 Assets and External Entities

As defined in section 1.2.1 the TOE is a smart card platform implementing the Card Operating System (COS) according to [21] without any object system. In sense of BSI-CC-PP-0082-V4 [BSI_PP_EHC_G2] and BSI-CC-PP-0084-2014 [11] the COS is User Data and Security IC Embedded Software.

In section 3.1 "Description of Assets" in BSI-CC-PP-0084-2014 a high level description (in sense of this ST) of the assets (related to standard functionality) is given. Please refer there for a long description. Namely these assets are

- the User Data,
- the Security IC Embedded Software, stored and in operation,
- the security services provided by the TOE for the Security IC Embedded Software, and
- the random numbers produced by the IC platform.

In this Security Target these assets and the protection requirements of these assets are refined because

- the User Data defined in BSI-CC-PP-0084-2014 are User Data or TSF Data in the context of the present ST,
- Security IC Embedded Software is part of the present TOE,
- the security services provided by the TOE for the Security IC Embedded Software are part of the present TSF and
- the random numbers produced by the IC platform are internally used by the TSF.

The primary assets are User Data to be protected by the COS as long as they are in scope of the TOE and the security services provided by the TOE.

| Asset | Definition |
|---|---|
| User Data 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. |

**Table 7: Data objects to be protected by the TOE as primary assets**

Note: Elementary files (EF) may be stored in the MF, any Dedicated File (DF), Application or Application Dedicated File (ADF). The place of an EF in the file hierarchy defines features of the User Data stored in the EF. User Data do not affect the operation of the TSF (cf. CC Part 1, para 100). Cryptographic keys used by the TSF to verify authentication attempts of external entities (i.e. authentication reference data) including the verification of Card Verifiable Certificates (CVC) or authenticate itself to external entities by generation of authentication verification data in a cryptographic protocol are TSF Data (cf. Table 13, Table 14 and Table 17)

This Security Target considers the following external entities:

| External entity | Definition |
|---|---|
| World | Any user independent on identification or successful authentication.[1] |
| Human User | A person authenticated by password or PUC. |
| Device | An external device authenticated by cryptographic operation. |

**Table 8: External entities[2]**

## 3.2 Threats

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

[1] The user World corresponds to the access condition ALWAYS in [21]. An authenticated Human User or Device is allowed to use the right assigned for World.

[2] This table defines external entities and subjects in the sense of [1]. Subjects can be recognised by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entity – an 'image' inside and 'works' then with this TOE internal image (also called subject in [1]). From this point of view, the TOE itself perceives only 'subjects' and, for them, does not differ between 'subjects' and 'external entities'. There is no dedicated subject with the role 'attacker' within the present security policy, whereby an attacker might 'capture' any subject role recognised by the TOE.

The following Threats are defined in BSI-CC-PP-0084-2014 [11]: T.Leak-Inherent, T.Phys-Probing, T.Malfunction, T.Phys-Manipulation, T.Leak-Forced, T.Abuse-Func, T.RND.

According to [ST_IC], the Security IC Platform makes use of optional Packages in BSI-CC-PP-0084-2014 [11]. The following Threat is defined in BSI-CC-PP-0084-2014 [11] for the optional package "Authentication of the Security IC" which is relevant for the present TOE: T.Masquerade_TOE.

Furthermore, the IC Platform Security Target [ST_IC] defines an additional Threat: T.Mem-Access.

All Threats are part of the aforementioned Protection Profile or IC Platform Security Target and are taken over into this ST for the present TOE. Please refer to BSI-CC-PP-0084-2014 and [ST_IC] for further descriptions and details. Table 9 lists all Threats taken over with the corresponding reference to [11].

| **Threat name** | **Reference to paragraph in [11] and section in [ST_IC]** | **Short description** |
|---|---|---|
| T.Leak-Inherent | [11], 82; [ST_IC], 4.1 | Inherent Information Leakage |
| T.Phys-Probing | [11], 83; [ST_IC], 4.1 | Physical Probing |
| T.Malfunction | [11], 84; [ST_IC], 4.1 | Malfunction due to Environmental Stress |
| T.Phys-Manipulation | [11], 85; [ST_IC], 4.1 | Physical Manipulation |
| T.Leak-Forced | [11], 86; [ST_IC], 4.1 | Forced Information Leakage |
| T.Abuse-Func | [11], 87; [ST_IC], 4.1 | Abuse of Functionality |
| T.RND | [11], 88; [ST_IC], 4.1 | Deficiency of Random Numbers |
| T.Masquerade_TOE | [11], 328; [ST_IC], 4.1 | Masquerade of the TOE |
| T.Mem-Access | [ST_IC], 4.1.1 | Memory Access Violation (Hardware) |

**Table 9: Overview of Threats defined in BSI-CC-PP-0084-2014 [11] and [ST_IC] and taken over into this ST**

Additionally, the following Threats for the TOE are defined:

The TOE shall avert the Threat "Forge of User or TSF Data (T.Forge_Internal_Data)" as specified below.

| | |
|---|---|
| **T.Forge_Internal_Data** | **Forge of User or TSF Data**<br><br>An attacker with high attack potential tries to forge internal User Data or TSF Data.<br><br>This Threat comprises several attack scenarios of smart card forgery. The attacker may try to alter the User Data e.g. to add User Data in elementary files. The attacker may misuse the TSF management function to change the user authentication data to a known value. |

The TOE shall avert the Threat "Compromise of confidential User or TSF Data (T.Compromise_Internal_Data)" as specified below.

| | |
|---|---|
| **T.Compromise_Internal_Data** | **Compromise of confidential User or TSF Data**<br><br>An attacker with high attack potential tries to compromise confidential User Data or TSF Data through the communication interface of the TOE.<br><br>This Threat comprises several attack scenarios e.g. guessing of the user authentication data (password) or reconstruction the private decipher key using the response code for chosen cipher texts (like Bleichenbacher attack for the SSL protocol implementation), e.g. to add keys for decipherment. The attacker may misuse the TSF management function to change the user authentication data to a known value. |

The TOE shall avert the Threat "Misuse of TOE functions (T.Misuse)" as specified below.

| | |
|---|---|
| **T.Misuse** | **Misuse of TOE functions**<br><br>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 authorisation. |

This Threat comprises several attack scenarios e.g. the attacker may try circumvent the user authentication to use signing functionality without authorisation. The attacker may try to alter the TSF Data e.g. to extend the user rights after successful authentication.

The TOE shall avert the Threat "Malicious Application (T.Malicious_Application)" as specified below.

| | |
|---|---|
| **T.Malicious_Application** | **Malicious Application**<br><br>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. |

The TOE shall avert the Threat "Cryptographic attack against the implementation (T.Crypto)" as specified below.

| | |
|---|---|
| **T.Crypto** | **Cryptographic attack against the implementation**<br><br>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.<br><br>This Threat comprises several attack scenarios e.g. an attacker may try to foresee the output of a random number generator in order to get a session key. An attacker may try to use leakage during cryptographic operation in order to use SPA, DPA, DFA or EMA techniques in order to compromise the keys or to get knowledge of other sensitive TSF or User Data. Furthermore an attacker could try guessing the key by using a brute-force attack. |

The TOE shall avert the Threat "Interception of Communication (T.Intercept)" as specified below.

| | |
|---|---|
| **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.

This Threat comprises several attack scenarios. An attacker may try to read or forge data during transmission in order to add data to a record or to gain access to authentication data.

The TOE shall avert the Threat "Wrong Access Rights for User Data or TSF Data (T.WrongRights)" as specified below.

**T.WrongRights** **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.

## 3.3 Organisational Security Policies

The TOE and/or its environment shall comply with the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operation.

The following OSP is originally defined in BSI-CC-PP-0084-2014 [11]: P.Process-TOE.

According to [ST_IC], the Security IC Platform makes use of optional Packages in BSI-CC-PP-0084-2014 [11]. The following OSP is defined in BSI-CC-PP-0084-2014 [11] for the optional package "AES" which is relevant for the present TOE: P.Crypto-Service.

Furthermore, the IC Platform Security Target [ST_IC] defines an additional OSP: P.Add-Functions.

The OSPs are part of the aforementioned Protection Profile or IC Platform Security Target and are taken over into this ST for the present TOE.

Note that the present ST includes the embedded software which is not part of the TOE defined in BSI-CC-PP-0084-2014 [11]. Hence, the OSPs are extended on content level in comparison to BSI-CC-PP-0084-2014 and [ST_IC]. Please refer to BSI-CC-PP-0084-

2014 and [ST_IC] for further descriptions and details. Table 10 lists all OSPs taken over with the corresponding reference to [11] or [ST_IC].

| OSP name | Short description | Reference to paragraph in [11] and section in [ST_IC] |
|---|---|---|
| P.Process-TOE | Identification during TOE Development and Production | [11], 90; [ST_IC], 4.2 |
| P.Crypto-Service | Cryptographic services of the TOE | [11], 374; [ST_IC], 4.2.1 |
| P.Add-Functions | Additional Specific Security Functionality | [ST_IC], 4.2.1 |

**Table 10: Overview of OSP defined in BSI-CC-PP-0084-2014 [11] and [ST_IC] and taken over into this ST**

## 3.4 Assumptions

The Assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

The Assumptions defined in BSI-CC-PP-0084-2014 [11] and [ST_IC] address the operational environment of the Security IC Platform, i.e. the COS part of the present TOE and the operational environment of the present TOE. The aspects of these Assumptions which are relevant for the COS part of the present TOE address the development process of the present TOE and are evaluated according to the composite evaluation approach [8]. Therefore, these Assumptions are now appropriately re-defined in order to address the Assumptions for the operational environment of the present TOE. Table 11 lists and maps these Assumptions for the operational environment with the corresponding reference to [11] or [ST_IC].

| Assumptions defined in [11] | Reference to paragraph in [11] or section in [ST_IC] | Re-defined Assumptions for the operational environment of the present TOE | Rationale of the changes |
|---|---|---|---|
| A.Process-Sec-IC | [11], 95 | A.Process-Sec-SC | While the TOE of BSI-CC-PP-0084-2014 is delivered after Phase 3 'IC Manufacturing' or Phase 4 'IC Packaging' the present TOE is delivered after Phase 5 'Composite |

| | | | |
|---|---|---|---|
| | | | Product Integration' / 'Smart Card Product Finishing' before Phase 6 'Personalisation' / 'Smart Card Personalisation'. The protection during Phase 4 may and during Phase 5 shall be addressed by appropriate security of the development environment and process of the present TOE. Only protection during Phase 6 'Personalisation' / 'Smart Card Personalisation' is in responsibility of the operational environment. |
| A.Resp-Appl | [11], 99 | A.Resp-ObjS | The User Data of the TOE of BSI-CC-PP-0084-2014 are the Security IC Embedded Software, i.e. the COS part of the TOE, the TSF Data of the present 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 present TOE. |
| A.Key-Function | [ST_IC], 4.3.1 | - | This Assumption is not overtaken into this ST because it focusses onto Key-dependent funtions within the Smartcard Embedded Software which have to be implemented in a way that they are not susceptible to leakage attacks. The Smartcard Embedded Software is part of this TOE, and therefore A.Key-Function is covered by T.Leak-Inherent and T.Leak-Forced in this ST. |

**Table 11: Overview of Assumptions defined in BSI-CC-PP-0084-2014 [11] and [ST_IC] and implemented by the TOE**

The following Assumptions for the TOE and its operational environment are defined:

The developer of applications that are intended to run on the COS must ensure the appropriate "Usage of COS (A.Plat-COS)" while developing the application.

**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,

including TOE related application notes, usage requirements, recommendations and restrictions, and (ii) certification report including TOE related usage requirements, recommendations, restrictions and findings resulting from the TOE's evaluation and certification.

The developer of applications that are intended to run on the COS must ensure the appropriate "Treatment of User Data and TSF Data by the Object System (A.Resp-ObjS)" while developing the application.

| | |
|---|---|
| **A.Resp-ObjS** | **Treatment of User Data and TSF Data by the Object System**<br><br>All User Data and TSF Data of the TOE are treated in the object system as defined for its specific intended application context. |

The developer of applications that are intended to run on the COS must ensure the appropriate "Protection during Personalisation (A.Process-Sec-SC)" after delivery of the TOE.

| | |
|---|---|
| **A.Process-Sec-SC** | **Protection during Personalisation**<br><br>It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to the delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data with the goal to prevent any possible copy, modification, retention, theft or unauthorised use. |

# 4 Security Objectives

This section describes the Security Objectives for the TOE and the Security Objectives for the Operational Environment of the TOE.

## 4.1 Security Objectives for the TOE

The following Security Objectives for the TOE address the protection to be provided by the TOE.

The following Security Objectives for the TOE are defined in BSI-CC-PP-0084-2014 [11].

According to [ST_IC], the Security IC Platform makes use of optional Packages in BSI-CC-PP-0084-2014 [11]. The following Security Objectives for the TOE are defined in BSI-CC-PP-0084-2014 [11] for the optional packages "Authentication of the Security IC" and "AES" which are all relevant for the present TOE: O.Authentication and O.AES.

Furthermore, the IC Platform Security Target [ST_IC] defines additional Security Objectives for the TOE: O.Add-Functions, O.Mem-Access.

All Security Objectives for the TOE are part of the aforementioned Protection Profile or IC Platform Security Target and are taken over into this ST for the present TOE.

Please refer to BSI-CC-PP-0084-2014 and [ST_IC] for further descriptions and details. Table 12 lists all Security Objectives taken over with the corresponding reference to [11].

| Security Objectives name | Short description | Reference to paragraph in [11] and [ST_IC] |
|---|---|---|
| O.Leak-Inherent | Protection against Inherent Information Leakage | [11], 105 |
| O.Phys-Probing | Protection against Physical Probing | [11], 107 |
| O.Malfunction | Protection against Malfunctions | [11], 108 |
| O.Phys-Manipulation | Protection against Physical Manipulation | [11], 109 |
| O.Leak-Forced | Protection against Forced Information Leakage | [11], 111 |
| O.Abuse-Func | Protection against Abuse of Functionality | [11], 112 |
| O.Identification | TOE Identification | [11], 113 |

| | | |
|---|---|---|
| O.RND | Random Numbers | [11], 114 |
| O.Authentication | Authentication to external entities | [11], 330;<br>[ST_IC], 5.1 |
| O.AES | Cryptographic service AES | [11], 385;<br>[ST_IC], 5.1 |
| O.Add-Functions | Additional Specific Security Functionality | [ST_IC], 5.1 |
| O.Mem-Access | Area based Memory Access Control | [ST_IC], 5.1 |

**Table 12: Overview of Security Objectives for the TOE defined in BSI-CC-PP-0084-2014 [11] and [ST_IC] and taken over into this ST**

Additionally, the following Security Objectives for the TOE are defined:

The TOE shall fulfil the Security Objective "Integrity of internal data (O.Integrity)" as specified below.

**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.

The TOE shall fulfil the Security Objective "Confidentiality of internal data (O.Confidentiality)" as specified below.

**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.

The TOE shall fulfil the Security Objective "Treatment of User and TSF Data (O.Resp-COS)" as specified below.

**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.

The TOE shall fulfil the Security Objective "Support of TSF Data export (O.TSFDataExport)" as specified below.

| | |
|---|---|
| **O.TSFDataExport** | **Support of TSF Data export**<br><br>The TOE must provide correct export of TSF Data of the object system excluding confidential TSF Data for external review. |

The TOE shall fulfil the Security Objective "Access Control for Objects (O.AccessControl)" as specified below.

| | |
|---|---|
| **O.AccessControl** | **Access Control for Objects**<br><br>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. |

The TOE shall fulfil the Security Objective "Generation and import of keys (O.KeyManagement)" as specified below.

| | |
|---|---|
| **O.KeyManagement** | **Generation and import of keys**<br><br>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. |

The TOE shall fulfil the Security Objective "Cryptographic functions (O.Crypto)" as specified below.

| | |
|---|---|
| **O.Crypto** | **Cryptographic functions**<br><br>The TOE must provide cryptographic services by implementation of secure cryptographic algorithms for random number generation, 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. |

The TOE shall fulfil the Security Objective "Secure messaging (O.SecureMessaging)" as specified below.

| | |
|---|---|
| **O.SecureMessaging** | **Secure messaging**<br><br>The TOE supports secure messaging for protection of the confidentiality and the integrity of the commands received from successfully 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. |

## 4.2 Security Objectives for the Operational Environment of the TOE

This section describes the Security Objectives for the Operational Environment of the TOE.

The following Security Objectives for the Operational Environment of the Security IC Platform are defined in BSI-CC-PP-0084-2014 [11]. The operational environment of the Security IC Platform as TOE in BSI-CC-PP-0084-2014 comprises the COS part of the present TOE and the operational environment of the present TOE. Therefore these Security Objectives for the Operational Environment are appropriately split and re-defined. The aspects relevant for the COS part of the present TOE shall be fulfilled in the development process of the COS and evaluated according to the composite evaluation approach [8]. The remaining aspects of the Security Objectives for the Operational Environment defined in BSI-CC-PP-0084-2014 are addressed in new Security Objectives for the Operational Environment of the present ST. In particular, the Security Objective for the Operational Environment OE.Resp-Appl defined in BSI-CC-PP-0084-2014 is split into the Security Objective O.Resp-COS (see definition in section 4.1) for the COS part of the TOE and the Security Objectives OE.Plat-COS and OE.Resp-ObjS for the object system in the operational environment of the TOE.

According to [ST_IC], the Security IC Platform makes use of optional Packages in BSI-CC-PP-0084-2014 [11]. The following Security Objective for the Operational Environment is defined in BSI-CC-PP-0084-2014 [11] for the optional package "Authentication of the Security IC" which is relevant for the present TOE: OE.TOE_Auth.

These Security Objectives for the Operational Environment are taken over unmodified into this ST for the present TOE.

Table 13 lists and maps these Security Objectives for the Operational Environment with the corresponding reference to [11].

| Security Objectives for the Operational Environment defined in [11] | Reference to paragraph in [11] | Re-defined Security Objectives for the Operational Environment of the present TOE | Rationale of the changes or short description |
|---|---|---|---|
| OE.Resp-Appl | 117 | OE.Resp-ObjS<br>OE.Plat-COS | 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 | 118 | OE.Process-Card | The Security Objective defined for the environment of the Security IC Platform is appropriately re-defined for the present TOE. |
| OE.TOE_AUTH | 331 | OE.TOE_AUTH (taken over from [11]) | Authentication to external entities |

**Table 13: Overview of Security Objectives for the Operational Environment defined in BSI-CC-PP-0084-2014 [11] and taken over into this ST**

Additionally, the following Security Objectives for the Operational Environment of the TOE are defined:

The operational environment of the TOE shall fulfil the Security Objective "Usage of COS (OE.Plat-COS)" as specified below.

**OE.Plat-COS** **Usage of COS**

To ensure that the TOE is used in a secure manner the object system shall be designed such that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the user guidance, including TOE related application notes, usage

| | |
|---|---|
| | requirements, recommendations and restrictions, and (ii) certification report including TOE related usage requirements, recommendations, restrictions and findings resulting from the TOE's evaluation and certification. |

The operational environment of the TOE shall fulfil the Security Objective "Treatment of User Data and TSF Data by the Object System (OE.Resp-ObjS)" as specified below.

| | |
|---|---|
| **OE.Resp-ObjS** | **Treatment of User Data and TSF Data by the Object System**<br><br>All User Data and TSF Data of the object system are defined as required by the security needs of the specific application context. |

The operational environment of the TOE shall fulfil the Security Objective "Protection during Personalisation (OE.Process-Card)" as specified below.

| | |
|---|---|
| **OE.Process-Card** | **Protection during Personalisation**<br><br>Security procedures shall be used after delivery of the TOE during Phase 6 'Personalisation' up to the delivery of the smart card to the end-user in order to maintain confidentiality and integrity of the TOE and to prevent any theft, unauthorised personalisation or unauthorised use. |

## 4.3 Security Objectives Rationale

The following tables provide an overview for the coverage of the defined security problem by the Security Objectives for the TOE and its environment. The tables address the security problem definition as outlined in BSI-CC-PP-0084-2014 and [ST_IC] and taken over to the present ST as well as the Threats, Organisational Security Policies and Assumptions that are additionally defined or redefined in the present ST. The tables show that all Threats and OSPs are addressed by the Security Objectives for the TOE and for the TOE environment. The tables also show that all Assumptions are addressed by the Security Objectives for the TOE environment.

Table 1 in BSI-CC-PP-0084-2014 [11], Section 4.4 "Security Objectives Rationale" gives an overview, how the Assumptions, Threats and Organisational Security Policies that are taken over in the present ST are addressed by the respective Security Objectives.

Please refer for the further details to the related justification provided in BSI-CC-PP-0084-2014 [11]. In addition, in view of the present ST the following considerations hold:

| | (SAR ALC for IC part of the TOE) | OE.Process-Card | (SAR for COS part of the TOE) | OE.Resp-ObjS | OE.TOE_Auth | O.Identification | O.Leak-Inherent | O.Phys-Probing | O.Malfunction | O.Phys-Manipulation | O.Leak-Forced | O.Abuse-Func | O.RND | O.Authentication | O.Mem-Access | O.AES | O.Add-Functions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (A.Process-Sec-IC[3]) | (X) | (X) | | | | | | | | | | | | | | | |
| A.Process-Sec-SC | | X | | | | | | | | | | | | | | | |
| (A.Resp-Appl[4]) | | | (X) | (X) | | | | | | | | | | | | | |
| A.Resp-ObjS | | | | X | | | | | | | | | | | | | |
| P.Process-TOE | | | | | | X | | | | | | | | | | | |
| P.Crypto_Service | | | | | | | | | | | | | | | | X | |
| P.Add-Functions | | | | | | | | | | | | | | | | | X |
| T.Leak-Inherent | | | | | | | X | | | | | | | | | | |
| T.Phys-Probing | | | | | | | | X | | | | | | | | | |
| T.Malfunction | | | | | | | | | X | | | | | | | | |
| T.Phys-Manipulation | | | | | | | | | | X | | | | | | | |
| T.Leak-Forced | | | | | | | | | | | X | | | | | | |
| T.Abuse-Func | | | | | | | | | | | | X | | | | | |

[3] Re-defined Assumption, see section 3.4
[4] Re-defined Assumption, see section 3.4

| | (SAR ALC for IC part of the TOE) | OE.Process-Card | (SAR for COS part of the TOE) | OE.Resp-ObjS | OE.TOE_Auth | O.Identification | O.Leak-Inherent | O.Phys-Probing | O.Malfunction | O.Phys-Manipulation | O.Leak-Forced | O.Abuse-Func | O.RND | O.Authentication | O.Mem-Access | O.AES | O.Add-Functions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T.RND | | | | | | | | | | | | | X | | | | |
| T.Masquerade_TOE | | | | | X | | | | | | | | | X | | | |
| T.Mem-Access | | | | | | | | | | | | | | | X | | |

**Table 14: Security Objective Rationale related to the IC platform**

The Assumption **A.Process-Sec-IC** assumes and the Security Objective **OE.Process-Sec-IC** requires that security procedures are used after delivery of the IC by the IC Manufacturer up to the 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). Development and production of the Security IC Platform is part of the development and production of the present TOE because it includes the Security IC Platform. The Assumption **A.Process-Sec-SC** as appropriate re-definition of **A.Process-Sec-IC** assumes and the Security Objective **OE.Process-Card** as appropriate re-definition of **OE.Process-Sec-IC** requires security procedures during Phase 6 'Personalisation' up to the delivery of the smart card to the end-user. More precisely, the smart card life cycle according to [10] (cf. also to BSI-CC-PP-0084-2014 [11]) is covered as follows:

- 'IC Development' (Phase 2) and 'IC Manufacturing' (Phase 3) are covered as development and manufacturing of the Security IC Platform and therefore of the TOE as well.
- 'IC Packaging' (Phase 4) may be part of the development and manufacturing environment or the operational environment of the Security IC Platform. Even if it is part of the operational environment of the Security IC Platform addressed by OE.Process-Sec-IC it will be part of the development and manufacturing environment of the present TOE and covered by the SAR ALC_DVS.2.
- 'Composite Product Integration' / 'Smart Card Product Finishing' (Phase 5) is addressed by OE.Process-Sec-IC but it is part of the development and

manufacturing environment of the present TOE and covered by the SAR ALC_DVS.2.

- 'Personalisation' / 'Smart Card Personalisation' (Phase 6) up to the delivery of the smart card to the end-user is addressed by A.Process-Sec-IC and A.Process-Sec-SC and covered by OE.Process-Sec-SC.

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 the SFRs of the present ST 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-ObjS** requires the object system to be defined as required by the security needs of the specific application context.

The OSPs **P.Process-TOE** and **P.Crypto_Service** and the Threats **T.Leak-Inherent**, **T.Phys-Probing**, **T.Malfunction**, **T.Phys-Manipulation**, **T.Leak-Forced**, **T.Abuse-Func, T.RND** and **T.Masquerade_TOE** are covered by the Security Objectives as described in BSI-CC-PP-0084-2014, including the relevant optional packages "Authentication of the Security IC" and "AES". As stated in section 2.4, the present ST claims strict conformance to BSI-CC-PP-0084-2014 [11].

The OSP **P.Add-Functions** and the Threat **T.Mem-Access** are additionally defined in the IC Platform Security Target [ST_IC] and taken over into this ST. As stated in section 2.4, the IC Platform Security Target [ST_IC] claims strict conformance to BSI-CC-PP-0084-2014 [11].

The Security Objectives, Assumptions, Organisational Security Policies (OSPs) and Threats as used in Table 14 are defined and handled in [11] or [ST_IC]. Hence, the rationale for these items and their correlation with Table 14 is given in [11] and [ST_IC] resp., and not repeated here. The present ST defines new Threats and Assumptions for the TOE in comparison to the Security IC Platform as TOE defined in BSI-CC-PP-0084-2014 and IC Platform Security Target and extends the OSP P.Process-TOE to the present TOE.

| | O.Integrity | O.Confidentiality | O.Resp-COS | O.TSFDataExport | O.Authentication | O.AccessControl | O.KeyManagement | O.Crypto | O.SecureMessaging | OE.Plat-COS | OE.Resp-ObjS | OE.Process-Card |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T.Forge_Internal_Data | X | | X | | | | | | | | | |
| T.Compromise_Internal_Data | | X | X | | | | X | | | | | |
| T.Misuse | | | | | X | X | | | | | | |
| T.Malicious_Application | | | | X | X | X | | | | | | |
| T.Crypto | | | | | | | | X | | | | |
| T.Intercept | | | | | | | | | X | | | |
| T.WrongRights | | | X | | | | | | | | | |
| A.Plat-COS | | | | | | | | | | X | | |
| A.Resp-ObjS | | | | | | | | | | | X | |
| A.Process-Sec-SC | | | | | | | | | | | | X |
| P.Process-TOE | | | | | | | | | | | | X |

**Table 15: Security Objective Rationale for the COS part of the TOE**

A detailed justification required for suitability of the Security Objectives to coup with the security problem definition is given below.

The Threat **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 Threat because the User Data and TSF Data are treated by the TOE as defined by the TSF Data of the object system.

The Threat **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.

The Threat **T.Misuse** addresses the usage of access control protected assets by an attacker without knowledge of user authentication data or by any implicit authorisation. 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.

The Threat **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.

The Threat **T.Crypto** addresses a cryptographic attack to the implementation of cryptographic algorithms or the guessing of keys using brute force attacks. This threat is directly covered by the Security Objective O.Crypto which requires a secure implementation of cryptographic algorithms.

The Threat **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 Threat 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.

The Threat **T.WrongRights** addresses the compromising or manipulation of sensitive User Data or TSF Data by using undocumented or inappropriate access rights defined in the object system. This Threat 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.

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.

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.

The Assumption **A.Process-Sec-SC** covers the secure use of the TOE after TOE delivery in Phase 6 and is directly addressed by the Security Objective for the Operational Environment OE.Procress-Card.

The OSP **P.Process-TOE** addresses the protection during TOE development and production as defined in BSI-CC-PP-0084-2014 [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.

# 5 Extended Component Definition

This Security Target uses components defined as extensions to Common Criteria Part 2 [2]. The following extensions are taken from BSI-CC-PP-0084-2014 [11], section 5 "Extended Components Definition" and are part of this Security Target:

- Definition of the Family FMT_LIM,
- Definition of the Family FAU_SAS,
- Definition of the Family FDP_SDC, and
- Definition of the Family FCS_RNG.

The following extension is taken from [ST_IC], section 6 "Extended Components Definition" and is part of this Security Target:

- Definition of the Component FPT_TST.2.

The families FIA_API, FPT_EMS and FPT_ITE are defined in the document on hand.

## 5.1 Definition of the Family FIA_API Authentication Proof of Identity

To describe the IT Security Functional Requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

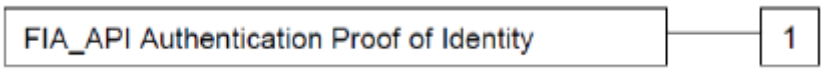
*Application note 3:* The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the extended family FIA_API from point of view of a TOE proving its identity.

**FIA_API Authentication Proof of Identity**

**Family Behaviour**

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.

**Component levelling**




FIA_API.1 Authentication Proof of Identity, provides prove of the identity of the TOE to an external entity.

| | |
|---|---|
| Management: | The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity. |
| Audit: | There are no actions defined to be auditable. |
| **FIA_API.1** | **Authentication Proof of Identity** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_API.1.1 | The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment:object, authorised user or role] to an external entity. |

## 5.2 Definition of the Family FPT_EMS TOE emanation

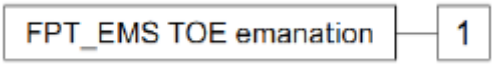
The family FPT_EMS (TOE emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT Security Functional Requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena 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].

**FPT_EMS TOE emanation**

**Family Behaviour**

This family defines requirements to mitigate intelligible emanations.

**Component levelling**



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

| | |
|---|---|
| FPT_EMS.1.1 | Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data |
| FPT_EMS.1.2 | Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data |
| Management: | There are no management activities foreseen. |
| Audit: | There are no actions defined to be auditable. |
| **FPT_EMS.1** | **Emanation of TSF and User data** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_EMS.1.1 | The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*]. |
| FPT_EMS.1.2 | The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*]. |

## 5.3 Definition of the Family FPT_ITE TSF image export

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 the export of TOE implementation fingerprints and of TSF Data in order to allow the verification of the correct implementation of the IC Dedicated Software and the COS of the TOE and the TSF Data of the smart card.

A fingerprint of the TOE implementation covers (beside a value randomly chosen by the external world) all implemented executable code including related configuration data and may e.g. be realised as a keyed hash value over all these implementation items. Refer to the COS specification [21] for technical details concerning the command FINGERPRINT. Such TOE implementation fingerprint serves for the identification as well as for the verification of the integrity and authenticity of the TOE and its implementation. The export of a fingerprint of the TOE implementation provides the ability to compare the provided TOE implementation with the known intended TOE implementation that is subject of the TOE's evaluation and certification on base of the ST on hand.

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 an object system specification. The exported data 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 the export of TOE implementation fingerprints and for the unprotected export of TSF Data not being addressed by any other component of CC Part 2 [2].

**FPT_ITE TSF image export**

**Family Behaviour**

This family defines requirements for the export of the TOE implementation fingerprint and of TSF data.

**Component levelling**


FPT_ITE.1 Export of TOE implementation fingerprint, provides the ability to export the TOE implementation fingerprint without protection of confidentiality or integrity.

FPT_ITE.2 Export of TSF data, provides the ability to export the TSF data without protection of confidentiality or integrity.

| | |
|---|---|
| Management FPT_ITE.1, FPT_ITE.2: | There are no management activities foreseen. |
| Audit FPT_ITE.1, FPT_ITE.2: | There are no actions defined to be auditable. |

| | |
|---|---|
| **FPT_ITE.1** | **Export of TOE implementation fingerprint** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_ITE.1.1 | The TOE shall export fingerprint of TOE 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. |
| **FPT_ITE.2** | **Export of TSF data** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| 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. |

# 6 Security Requirements

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

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. Each of these operations is used in this ST.

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

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the ST author are denoted as underlined text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the ST author are denoted by showing as underlined text.

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.

Application Notes of the PP are respected by the ST author in the way indicated in **bold text**.

Some SFRs (including the potential exiting refinement) were taken over from the IC Platform Security Target. A list of all SFRs taken from [ST_IC] can be found in section 6.1.3.

## 6.1 Security Functional Requirements for the TOE

In order to define the Security Functional Requirements Part 2 of the Common Criteria [2] was used. However, some Security Functional Requirements have been refined. The refinements are described below the associated SFR.

### 6.1.1 Overview

In order to give an overview of the Security Functional Requirements in the context of the security services offered by the TOE, the author of the ST defined the following security functional groups and allocated the Security Functional Requirements described in the following sections to them:

| Security Functional Groups | Security Functional Requirements concerned |
|---|---|
| Protection against Malfunctions | FRU_FLT.2/SICP, FPT_FLS.1/SICP |
| Protection against Abuse of Functionality | FMT_LIM.1/SICP, FMT_LIM.2/SICP, FAU_SAS.1/SICP |
| Protection against Physical Manipulation and Probing | FDP_SDC.1/SICP, FDP_SDI.2/SICP, FPT_PHP.3/SICP |
| Protection against Leakage | FDP_ITT.1/SICP, FPT_ITT.1/SICP, FDP_IFC.1/SICP |
| Generation of Random Numbers | FCS_RNG.1/HPRG_SICP |
| General Protection of User Data and TSF Data | FPT_TST.2/SICP |
| Authentication | FIA_API.1/SICP |
| Access Control | FDP_ACC.1/SICP , FDP_ACF.1/SICP, FMT_MSA.3/SICP, FMT_MSA.1/SICP, FMT_SMF.1/SICP |
| Cryptographic Functions | FCS_CKM.1/RSA-0_SICP, FCS_CKM.1/EC-0_SICP, FCS_CKM.4/AES-SCL-1_SICP, FCS_COP.1/AES-SCL-1_SICP, FCS_COP.1/RSA-0_SICP, FCS_COP.1/ECDSA-0_SICP, FCS_COP.1/ECDH-0_SICP |

**Table 16: Security functional groups vs. SFRs related to the Security IC Platform**

| Security Functional Groups | Security Functional Requirements concerned |
|---|---|
| General Protection of User Data and TSF Data (section 6.1.4) | FDP_RIP.1, FDP_SDI.2, FPT_FLS.1, FPT_EMS.1, FPT_TDC.1, FPT_ITE.1, FPT_ITE.2, FPT_TST.1 |
| Authentication (section 6.1.5) | FIA_AFL.1/PIN, FIA_AFL.1/PUC, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UID.1, FIA_API.1, FMT_SMR.1, FIA_USB.1 |
| Access Control (section 6.1.6) | FDP_ACC.1/EF, FDP_ACF.1/EF, FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF, FDP_ACC.1/TEF, FDP_ACF.1/TEF, |

| Security Functional Groups | Security Functional Requirements concerned |
|---|---|
| | FDP_ACC.1/SEF, FDP_ACF.1/SEF, FDP_ACC.1/KEY, FDP_ACF.1/KEY, 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 |
| Cryptographic Functions (section 6.1.7) | FCS_RNG.1, FCS_RNG.1/GR, FCS_COP.1/SHA, FCS_COP.1/COS.AES, FCS_COP.1/COS.CMAC, FCS_CKM.1/AES.SM, FCS_CKM.1/ELC, FCS_COP.1/COS.RSA.S, FCS_COP.1/COS.ECDSA.V, FCS_COP.1/COS.ECDSA.S, FCS_COP.1/COS.RSA, FCS_COP.1/COS.ELC, FCS_CKM.4 |
| Protection of communication (section 6.1.8) | FTP_ITC.1/TC |

**Table 17: Security functional groups vs. SFRs**

The following TSF Data are defined for the IC part of the TOE.

| TSF Data | Definition |
|---|---|
| TOE pre-personalisation data | Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer.1 |
| TOE initialisation data | Initialisation Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC Platform's production and further life-cycle phases are considered as belonging to the TSF Data. |

**Table 18: TSF Data defined for the IC part**

### 6.1.2 Users, subjects and objects

The security attributes of human users are stored in password objects (cf. [21] for details). The human user selects the password object by *pwIdentifier* and therefore the role gained by the subject acting for this human user after successful authentication. The role is a set of access rights defined by the access control rules of the objects containing this *pwIdentifier*. The *secret* is used to verify the authentication attempt of the human user providing the authentication verification data. The security attributes *transportStatus, lifeCycleStatus* and *flagEnabled* stored in the password object define the status of the role associated with the password. E.g. if the *transportStatus* is equal

to *Leer-PIN* or *Transport-PIN* the user is enforced to define his or her own password and making this password and this role effective (by changing the *transportStatus* to *regularPassword*). The multi-reference password shares the *secret* with the password identified by *pwReference.* It allows enforcing re-authentication for access and limitation of authentication state to specific objects and makes password management easier by using the same secret for different roles. The security attributes *interfaceDependentAccessRules, startRetryCounter, retryCounter, minimumLength* and *maximumLength* are defined for the *secret*. The PUC defined for the *secret* is intended for password management and the authorisation gained by successful authentication is limited to the command RESET RETRY COUNTER for reset of the *retryCounter* and setting a new *secret.*

The following table provides an overview of the authentication reference data and security attributes of human users and the security attributes of the authentication reference data as TSF Data.

| **User type** | **Authentication reference data and security attributes** | **Comments** |
|---|---|---|
| Human user | **Password**<br>Authentication reference data<br>*secret*<br>Security attributes of the user role<br>*pwIdentifier*<br>*transportStatus*<br>*lifeCycleStatus*<br>*flagEnabled*<br>*startSsecList*<br>Security attributes of the secret<br>*interfaceDependentAccessRules*<br>*startRetryCounter*<br>*retryCounter*<br>*minimumLength*<br>*maximumLength* | The following command is used by the TOE to authenticate the human user and to reset the security attribute *retryCounter* by PIN: VERIFY.<br>The following command is used by the TOE to manage the authentication reference data *secret* and the security attribute *retryCounter* with authentication of the human user by PIN: CHANGE REFERENCE DATA (P1=’00’).<br>The following commands are used by the TOE to manage the authentication reference data *secret* without authentication of the human user: CHANGE REFERENCE DATA (P1=’01’) and RESET RETRY COUNTER (P1=’02’).<br>The following command is used by the TOE to manage the security attribute *retryCounter* of the authentication reference data PIN without authentication of |

| User type | Authentication reference data and security attributes | Comments |
|---|---|---|
| | | the human user: RESET RETRY COUNTER (P1=’03’).<br>The command GET PIN STATUS is used to query the security attribute *retryCounter* of the authentication reference data PIN with password object specific access control rules.<br>The following commands are used by the TOE to manage the security attribute *flagEnabled* of the authentication reference data with human user authentication by PIN: ENABLE VERIFICATION REQUIREMENT (P1=’00’), DISABLE VERIFICATION REQUIREMENT (P1=’00’).<br>The following commands are used by the TOE to manage the security attribute *flagEnabled* of the authentication reference data without human user authentication: ENABLE VERIFICATION REQUIREMENT (P1=’01’), DISABLE VERIFICATION REQUIREMENT (P1=’01’).<br>The commands ACTIVATE, DEACTIVATE and TERMINATE are used to manage the security attribute *lifeCycleStatus* of the authentication reference data password with password object specific access control rules.<br>The command DELETE is used to delete the authentication reference data password with password object specific access control rules. |
| Human user | **Multi-Reference password** | The commands used by the TOE to authenticate the |

| User type | Authentication reference data and security attributes | Comments |
|---|---|---|
| | Authentication reference data<br>*Secret* is shared with the password identified by *pwReference*.<br>Security attributes of the user role<br>*pwIdentifier*<br>*lifeCycleStatus*<br>*transportStatus*<br>*flagEnabled*<br>*startSsecList*<br>Security attributes of the secret<br>The security attributes *interfaceDependentAccessRules, minimumLength, maximumLength, startRetryCounter* and *retryCounter* are shared with password identified by *pwReference*. | human user and to manage the authentication reference Multi-Reference password data are the same as for password. |
| Human user | **Personal unblock code (PUC)**<br>Authentication reference data<br>*PUK*<br>Security attributes<br>*pwIdentifier* of the password[5]<br>*pukUsage* | The following command is used by the TOE to manage the authentication reference data *secret* and the security attribute *retryCounter* of the authentication reference data PIN with authentication of the human user by PUC: RESET RETRY COUNTER (P1='00').<br>The following command is used by the TOE to manage the security attribute *retryCounter* of the authentication reference data PIN with authentication of the human user by PUC: RESET RETRY COUNTER (P1='01'). |

[5] The PUC is part of the password object as authentication reference data for the RESET RETRY COUNTER command for this password.

**Table 19: Authentication reference data of the human user and security attributes**

The security attributes of devices depend on the authentication mechanism and the authentication reference data. A device may be associated with a symmetric cryptographic authentication key with a specific *keyIdentifier* and therefore the role gained by the subject acting for this device after successful authentication. The role is defined by the access control rules of the objects containing this *keyIdentifier*. A device may be also associated with a certificate containing the public key as authentication reference data and the card holder authorisation (*CHA*) in case of RSA-based CVC (if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE) or the card holder authorisation template (*CHAT*) in case of ELC-based CVC. The authentication protocol comprise the verification of the certificate by means of the root public key and command PSO VERIFY CERTIFICATE and by means of the public key contained in the successful verified certificate and the command EXTERNAL AUTHENTICATE. The subject acting for this device gets the role of the *CHA* (if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE) or *CHAT* which is referenced in the access control rules of the objects. The security attribute *lifeCycleStatus* is defined for persistently stored keys only. **Option_RSA_CVC is not supported by the TOE.**

| User type | Authentication reference data and security attributes | Comments |
|---|---|---|
| Device | **Symmetric authentication key**<br>Authentication reference data<br>*macKey*[6]<br>Security attributes of the Authentication reference data<br>*keyIdentifier*<br>*interfaceDependentAccessRules*<br>*lifeCycleStatus*<br>*algorithmIdentifier*<br>*numberScenario* | The following commands are used by the TOE to authenticate a device: EXTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE and GENERAL AUTHENTICATE.<br>The following commands are used by the TOE to manage the authentication reference data: ACTIVATE, DEACTIVATE, DELETE and TERMINATE. |
| Device | **Asymmetric authentication key** | The following command is used by the TOE to authenticate a |

[6] The symmetric authentication object contains encryption key encKey and a message authentication key macKey.

| User type | Authentication reference data and security attributes | Comments |
|---|---|---|
| | Authentication reference data<br>*Root Public Key*<br>*Certificate containing the public key* of the device[7]<br>*persistentCache*<br>*applicationPublicKeyList*[8]<br>Security attributes of the user<br>*Certificate Holder Reference (CHR)*<br>*lifeCycleStatus*<br>*interfaceDependentAccessRules*<br>~~*Certificate Holder Authorisation (CHA)* for RSA keys~~ (~~if~~ the RSA-based CVC functionality according to Option_RSA_CVC in [21] is **not** supported by the TOE) ~~or~~ *Certificate Holder Authorisation Template (CHAT)* for ECC keys<br>Security attributes in the certificate<br>*Certificate Profile Identifier (CPI)*<br>*Certification Authority Reference (CAR)*<br>*Object Identifier (OID)* | device: EXTERNAL AUTHENTICATE with ~~*algID* equal to *rsaRoleCheck*~~ (~~if~~ the RSA-based CVC functionality according to Option_RSA_CVC in [21] is **not** supported by the TOE) ~~or~~ *elcRoleCheck*.<br>The following commands are used by the TOE to manage the authentication reference data: PSO VERIFY CERTIFICATE, ACTIVATE, DEACTIVATE, DELETE and TERMINATE. |
| Device | **Secure messaging channel key**<br>Authentication reference data<br>MAC session key SK4SM | The TOE authenticates the sender of a received command using secure messaging. |

[7] The certificate of the device may be only end of a certificate chain going up to the root public key.

[8] The command PSO VERIFY CERTIFICATE may store the successful verified public key temporarily in the *volatileCache* or persistently in the *applicationPublicKeyList* or the *persistentCache*. Public keys in the *applicationPublicKeyList* may be used like root public keys. The wrapper specification [27] and COS specification [21] define the attribute *persistentPublicKeyList* as superset of all persistently stored public key in the *applicationPublicKeyList* and the *persistentCache*.

| User type | Authentication reference data and security attributes | Comments |
|---|---|---|
| | Security attributes of SK4SM<br>*flagSessionEnabled* (equal SK4SM)<br>*Kmac* and *SSCmac*<br>*negotiationKeyInformation* | |

**Table 20: Authentication reference data of the devices and security attributes**

The following table defines the authentication verification data used by the TSF itself for authentication by external entities (cf. FIA_API.1).

| Subject type | Authentication verification data and security attributes | Operations |
|---|---|---|
| TSF | **Private authentication key**<br>Authentication verification data<br>*privateKey*<br>Security attributes<br>*keyIdentifier*<br>*setAlgorithmIdentifier with algorithmIdentifier*<br>*lifeCycleStatus* | The following commands are used by the TOE to authenticate themselves to an external device: INTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE. |
| TSF | **Secure messaging channel key**<br>Authentication verification data<br>MAC session key SK4SM<br>Security attributes<br>*flagSessionEnabled* (equal SK4SM)<br>*macKey* and *SSCmac*<br>*encKey* and *SSCenc*<br>*flagCmdEnc* and *flagRspEnc* | Responses using secure messaging. The session keys are linked to the folder of the keys used to them. |

**Table 21: Authentication verification data of the TSF and security attributes**

The COS specification associates a subject with a *logical channel* and its *channelContext* (cf. [21], section 12). The TOE may support one subject respective logical channel or more than one independent subject or logical channel respectively, cf. section 10

Package Logical Channel. The *channelContext* comprises security attributes of the subject summarized in the following table.

| Security attribute | Elements | Comments |
|---|---|---|
| *interface* | | The TOE detects whether the communication uses contact-based interface (value set to *kontaktbehaftet*), or contactless interface (value set to *kontaktlos*)[9]. If the TOE does not support contactless communication the TOE shall behave as *interfaceDependentAccess* Rules is permanently set to "*kontaktbehaftet*". |
| *currentFolder* | | Identifier of the (unique) current folder. |
| | *seIdentifier* | Security environment selected by means of the command MANAGE SECURITY ENVIRONMENT[10]. If no security environment is explicitly selected the default security environment #1 is assumed. |
| *keyReferenceList* | | The list contains elements which may be empty or may contain one pair (*keyReference, algorithmIdentifier*). |
| | *externalAuthenticate* | *keyReference* and *algorithmIdentifier* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for device authentication by means of the commands EXTERNAL AUTHENTICATE and MUTUAL AUTHENTICATE. |

[9] Note the COS specification [21] describes this security attribute in the context of access control rules in section 8.1.4 only. If the TOE does not support contactless communication the document in hand shall be read assuming that this attribute is equal to "kontaktbehaftet".

[10] Note the COS specification [21] describes this security attribute in the informative section 8.8. The object system specification of the eHCP uses this security attribute for access control rules of batch signature creation.

| Security attribute | Elements | Comments |
|---|---|---|
| | *internalAuthenticate* | *keyReference* and *algorithmIdentifier* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for authentication of the TSF itself by means of the command INTERNAL AUTHENTICATE. |
| | *verifyCertificate* | *keyReference* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for PSO VERIFY CERTIFICATE. |
| | *signatureCreation* | *keyReference* and *algorithmIdentifier* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for PSO COMPUTE DIGITAL SIGNATURE. |
| | *dataDecipher* | *keyReference* and *algorithmIdentifier* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for PSO DECIPHER or PSO TRANSCIPHER. |
| | *dataEncipher* | *keyReference* and *algorithmIdentifier* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for PSO ENCIPHER. |
| | ~~*macCalculation*~~[11] | ~~*keyReference* and *algorithmIdentifier* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for PSO COMPUTE CRYPTOGRAPHIC CHECKSUM and PSO VERIFY CRYPTOGRAPHIC CHECKSUM (if the Package Crypto Box is supported by the TOE).~~ |

[11] Package Crypto Box **is not** supported by the TOE

| Security attribute | Elements | Comments |
|---|---|---|
| *SessionkeyContext* | | This list contains security attributes associated with secure messaging and trusted channels. |
| | *flagSessionEnabled* | Value *noSK* indicates no session key established.<br>Value *SK4SM* indicates session keys established for receiving commands and sending responses.<br>~~Value *SK4TC* indicates session keys established for PSO ENCIPHER and PSO DECIPHER and PSO COMPUTE CRYPTOGRAPHIC CHECKSUM, PSO VERIFY CRYPTOGRAPHIC CHECKSUM (if the Package Crypto Box is supported by the TOE).~~[12] |
| | *encKey* and *SSCenc* | Key for encryption and decryption and its sequence counter. |
| | *macKey* and *SSCmac* | Key for MAC calculation and verification and its sequence counter. |
| | *flagCmdEnc* and *flagRspEnc* | Flags indicating encryption of data in commands respective responses. |
| | *negotiationKeyInformation* | *keyIdentifier* of the key used to generate the session keys and if asymmetric key was used the *accessRight* associated with this key. The *keyIdentifier* may reference to the authentication reference data used for PACE[13] (~~if~~ PACE is supported by the TOE). |
| | *accessRulesSessionkeys* | Access control rules associated with trusted channel support. |

[12] Package Crypto Box **is not** supported by the TOE

[13] The *keyIdentifier* generated by successful authentication with PACE protocol is named "Kartenverbindungsobjekt" in the COS specification [21].

| Security attribute | Elements | Comments |
|---|---|---|
| *globalPasswordList* | *(pwReference, securityStatusEvaluation-Counter)* | List of 0, 1, 2, 3 or 4 elements containing results of successful human user authentication with password in MF: *pwReference* and *securityStatusEvaluationCounter*. |
| *dfSpecificPasswordList* | *(pwReference, securityStatusEvaluation-Counter)* | List of 0, 1, 2, 3 or 4 elements containing results of successful human user authentication with password for each DF: *pwReference* and *securityStatusEvaluationCounter*. |
| *globalSecurityList* | ~~*CHA* or~~ *keyIdentifier* | List of 0, 1, 2 or 3 elements containing results of successful device authentication with authentication reference data in MF: ~~CHA as reference to the role gained by authentication based on certificate~~ (~~if~~ the RSA-based CVC functionality according to Option_RSA_CVC in [21] is **not** supported by the TOE) ~~or~~ *keyIdentifier* as reference to the used symmetric authentication key or *keyIdentifier* generated by successful authentication with PACE protocol (~~if~~ PACE is supported by the TOE). |
| *dfSpecificSecurityList* | ~~*CHA* or~~ *keyIdentifier* | List of 0, 1, 2 or 3 elements containing results of successful device authentication with authentication reference data for each DF: ~~*CHA* as reference to the role gained by authentication based on certificate~~ (~~if~~ the RSA-based CVC functionality according to Option_RSA_CVC in [21] is **not** supported by the TOE) ~~or~~ *keyIdentifier* as reference to symmetric authentication key or *keyIdentifier* generated by successful authentication with PACE protocol (~~if~~ PACE is supported by the TOE). |
| *bitSecurityList* | | List of CHAT gained by successful authentication with CVC based on ECC. The effective access rights are the intersection of access rights defined in CVC of the CVC chain up to the root. |

| Security attribute | Elements | Comments |
|---|---|---|
| *Current* | | Identifier of the (unique) current file from *currentFolder.children*. |
| *securityStatus-EvaluationCounter* | *startSsec* | Must contain all values of *startSsec* and may be *empty*. |

**Table 22: Security attributes of a subject**

The following table provides an overview of the objects, operations and security attributes defined in the present PP (including the Packages). All references in the table refer to the technical specification of the Card Operating System [21]. The security attribute *lifeCycleStatus* is defined for persistently stored keys only.

| Object type | Elements | Comments |
|---|---|---|
| Object system | *applicationPublicKeyList*<br>*persistentCache*<br>*pointInTime* | PSO VERIFY CERTIFICATE |
| Folder<br>(8.3.1) | *accessRules:*<br>*lifeCycleStatus*<br>*shareable*[14]<br>*interfaceDependentAccessRules*<br>*children* | SELECT<br>ACTIVATE<br>DEACTIVATE<br>DELETE<br>FINGERPRINT<br>GET RANDOM<br>LOAD APPLICATION<br>TERMINATE DF |
| Dedicated File<br>(8.3.1.2) | Additionally for Folder:<br>*fileIdentifier* | Identical to Folder |
| Application<br>(8.3.1.1) | Additionally for Folder:<br>*applicationIdentifier* | Identical to Folder |
| Application Dedicated File<br>(8.3.1.3) | Additionally for Folder: | Identical to Folder |

[14] Available with Package Logical Channel

| Object type | Elements | Comments |
|---|---|---|
| | *fileIdentifier*<br>*applicationIdentifier*<br>*children* | |
| Elementary File<br>(8.3.2) | *fileIdentifier*<br>*list of shortFileIdentifier*<br>*lifeCycleStatus*<br>*shareable*[15]<br>*accessRules:*<br>*interfaceDependentAccessRules*<br>*flagTransactionMode*<br>*flagChecksum* | SELECT<br>ACTIVATE<br>DEACTIVATE<br>DELETE<br>TERMINATE |
| Transparent EF<br>(8.3.2.1) | Additionally for Elementary File:<br>*numberOfOctet*<br>*positionLogicalEndOfFile*<br>*body* | Additionally for Elementary File:<br>ERASE BINARY<br>READ BINARY<br>UPDATE BINARY<br>WRITE BINARY |
| Structured EF<br>(8.3.2.2) | Additionally for Elementary File:<br>*recordList*<br>*maximumNumberOfRecords*<br>*maximumRecordLength*<br>*flagRecordLifeCycleStatus* | Additionally for Elementary File:<br>ACTIVATE RECORD<br>APPEND RECORD<br>DELETE RECORD<br>DEACTIVATE RECORD<br>ERASE RECORD<br>READ RECORD<br>SEARCH RECORD<br>SET LOGICAL EOF<br>UPDATE RECORD |
| Regular Password (PIN)<br>(8.4) | *lifeCycleStatus*<br>*pwdIdentifier*<br>*accessRules:*<br>*interfaceDependentAccessRules*<br>*secret: PIN*<br>*minimumLength*<br>*maximumLength*<br>*startRetryCounter*<br>*retryCounter*<br>*transportStatus*<br>*flagEnabled*<br>*startSsecList* | ACTIVATE<br>DEACTIVATE<br>DELETE<br>TERMINATE<br>CHANGE REFERENCE DATA<br>DISABLE VERIFICATION REQUIREMENT<br>ENABLE VERIFICATION REQUIREMENT<br>GET PIN STATUS |

[15] Available with Package Logical Channel

| Object type | Elements | Comments |
|---|---|---|
| | *PUC*<br>*pukUsage*<br>channel specific:<br>*securityStatusEvaluationCounter* | RESET RETRY COUNTER<br>VERIFY |
| Multi-reference Password<br>(MR-PIN)<br>(8.5) | *lifeCycleStatus*<br>*pwdIdentifier*<br>*accessRules:*<br>*interfaceDependentAccessRules*<br>*startSsecList*<br>*flagEnabled*<br>*passwordReference*<br>Attributes used together with *referred password (PIN)*:<br>*secret: PIN*<br>*minimumLength*<br>*maximumLength*<br>*startRetryCounter*<br>*retryCounter*<br>*transportStatus*<br>*PUC*<br>*pukUsage*<br>channel specific:<br>*securityStatusEvaluationCounter* | Identical to Regular Password |
| PUC | *type pin*<br>*pukUsage* | RESET RETRY COUNTER |
| Symmetric Key<br>(8.6.1) | *lifeCycleStatus*<br>*keyIdentifier*<br>*accessRules:*<br>*interfaceDependentAccessRules*<br>*encKey*<br>*macKey*<br>*numberScenario*<br>*algorithmIdentifier*<br>*accessRulesSessionkeys:*<br>*interfaceDependentAccessRules* | ACTIVATE<br>DEACTIVATE<br>DELETE<br>TERMINATE<br>EXTERNAL AUTHENTICATE<br>GENERAL AUTHENTICATE<br>INTERNAL AUTHENTICATE<br>MUTUAL AUTHENTICATE |
| Private Asymmetric Key<br>(8.6.4) | *lifeCycleStatus*<br>*keyIdentifier*<br>*accessRules:*<br>*interfaceDependentAccessRules*<br>*privateKey*<br>*listAlgorithmIdentifier*<br>*accessRulesSessionkeys:*<br>*interfaceDependentAccessRules* | ACTIVATE<br>DEACTIVATE<br>DELETE<br>TERMINATE<br>GENERATE ASYMMETRIC KEY PAIR or key import<br>EXTERNAL AUTHENTICATE<br>GENERAL AUTHENTICATE<br>INTERNAL AUTHENTICATE |

| Object type | Elements | Comments |
|---|---|---|
| | *algorithmIdentifier*<br>*keyAvailable* | PSO COMPUTE DIGITAL SIGNATURE<br>PSO DECIPHER<br>PSO TRANSCIPHER |
| Public Asymmetric Key<br>(8.6.4) | *lifeCycleStatus*<br>*keyIdentifier*<br>*oid*<br>*accessRules:*<br>*interfaceDependentAccessRules* | ACTIVATE<br>DEACTIVATE<br>DELETE<br>TERMINATE |
| Public Asymmetric Key for signature verification<br>(8.6.4.2) | Additionally for Public Asymmetric Key:<br>*publicRsaKey: oid* or<br>*publicElcKey: oid*<br>*CHAT*<br>*expirationDate: date* | Additionally for Public Asymmetric Key:<br>PSO VERIFY CERTIFICATE,<br>PSO VERIFY DIGITAL SIGNATURE |
| Public Asymmetric Key for authentication<br>(8.6.4.3) | Additionally for Public Asymmetric Key:<br>*publicRsaKey: oid* or<br>*publicElcKey: oid*<br>*CHA (if applicable for the TOE) / CHAT*<br>*expirationDate: date* | Additionally for Public Asymmetric Key:<br>EXTERNAL AUTHENTICATE<br>GENERAL AUTHENTICATE<br>INTERNAL AUTHENTICATE |
| Public Asymmetric Key for encryption<br>(8.6.4.4) | Additionally for Public Asymmetric Key:<br>*publicRsaKey: oid*<br>*publicElcKey: oid* | Additionally for Public Asymmetric Key:<br>PSO ENCIPHER |
| Card verifiable certificate (CVC)<br>(7.1, 7.2) | *Certificate Profile Identifier (CPI)*<br>*Certification Authority Reference (CAR)*<br>*Certificate Holder Reference (CHR)*<br>*Certificate Holder Authorisation (~~CHA (if applicable for the TOE)~~ / CHAT)*<br>*Object Identifier (OID)*<br>*signature* | |

**Table 23: Subjects, objects, operations and security attributes (for the references refer to [21])**

The TOE must support Access control lists for

- *lifeCycleStatus* values "*Operational state (active)*", "*Operational state (deactivated)*" and "*Termination state*",
- *security environments* with value *seIdentifier* selected for the folder,
- *interfaceDependentAccessRules* for contact-based communication,

and may support Access control lists for

- *interfaceDependentAccessRules* for contactless communication (cf. section 8 Package Contactless).

If the user communicates with the TOE through the contact-based interface the security attribute "*interface*" of the subject is set to the value "*kontaktbehaftet*" and the *interfaceDependentAccessRules* for contact-based communication shall apply. If the user communicates with the TOE through the contactless interface the security attribute "*interface*" of the subject is set to the value "*kontaktlos*" and the *interfaceDependentAccessRules* for contactless communication shall apply. If the TOE does not support the contactless communication it behaves in respect to access control like a TOE defining all *interfaceDependentAccessRules* "*kontaktlos*" set to *NEVER* in the object system.

The user may set the *seIdentifier* value of the *security environments* for the folder by means of the command MANAGE SECURITY ENVIRONMENT. This may be seen as selection of a specific set of access control rules for the folder and the objects in this folder.[16]

The TOE access control rule contains

- command defined by CLA, 0 or 1 parameter P1, and 0 or 1 parameter P2,
- values of the *lifeCycleStatus* and *interfaceDependentAccessRules* indicating the set of access control rules to be applied,
- access control condition defined as Boolean expression with Boolean operators AND and OR of Boolean elements of the following types *ALWAYS*, *NEVER*, PWD(pwIdentifier), *AUT(keyReference)*, ~~*AUT(CHA)*~~ (~~if~~ the RSA-based CVC functionality according to Option_RSA_CVC in [21] is **not** supported by the TOE), *AUT(CHAT)* and secure messaging conditions (cf. [21], section 10.2 for details).

[16] This approach is used e.g. for signature creation with eHPC: the signatory selects security environment #1 for single signature, and security environment #2 for batch signature creation requirering additional authentication of the signature creation application.

Note that AUT(CHAT) is true if the access right bit necessary for the object and the command is 1 in the effective access rights calculated as bitwise-AND of all CHAT in the CVC chain verified successfully by PSO VERIFY DIGITAL SIGNATURE command executions.

The Boolean element ALWAYS provides the Boolean value TRUE. The Boolean element NEVER provides the Boolean value FALSE. The other Boolean elements provide the Boolean value TRUE if the value in the access control list match its corresponding security attribute of the subject and provides the Boolean value FALSE is they do not match.

The following table gives an overview of the commands the COS has to implement and the related SFRs. Please note that commands or special variants of commands may be required only if a specific Package is supported by the TOE. Some commands may be or may be not implemented by the COS as defined in [21] and therefore are not addressed by SFRs in this ST.

| **Operation** | **SFR** | **Section** |
|---|---|---|
| ACTIVATE | FMT_SMF.1, FMT_MSA.1/Life | 14.2.1 |
| ACTIVATE RECORD | FMT_SMF.1, FMT_MSA.1/SEF | 14.4.1 |
| APPEND RECORD | FDP_ACC.1/SEF, FDP_ACF.1/SEF | 14.4.2 |
| CHANGE REFERENCE DATA | FIA_UAU.5, FIA_USB.1, FMT_SMF.1, FMT_MTD.1/PIN, FMT_MSA.1/PIN, FIA_AFL.1/PIN**, FIA_SOS.1, FDP_SDI.2, FIA_ATD.1** | 14.6.1 |
| CREATE | **This optional command is not supported by the TOE.** | 14.2.2 |
| DEACTIVATE | FMT_SMF.1, FMT_MSA.1/**Life** | 14.2.3 |
| DEACTIVATE RECORD | FMT_SMF.1, FMT_MSA.1/SEF | 14.4.3 |
| DELETE | FIA_USB.1, FDP_ACC.1/MF_DF, FDP_ACF.1/ MF_DF, FDP_ACC.1/EF, FDP_ACF.1/EF, FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3, | 14.2.4 |

| Operation | SFR | Section |
|---|---|---|
| | FMT_SMF.1, FMT_MSA.1/Life, FCS_CKM.4, FIA_USB.1/LC[17], **FIA_ATD.1** | |
| DELETE RECORD | FDP_ACC.1/SEF, FDP_ACF.1/SEF, FMT_MSA.1/SEF, **FDP_RIP.1** | 14.4.4 |
| DISABLE VERIFICATION REQUIREMENT | FMT_SMF.1, FMT_MSA.1/PIN, FIA_AFL.1/PIN, FIA_USB.1, **FIA_ATD.1, FDP_SDI.2** | 14.6.2 |
| ENABLE VERIFICATION REQUIREMENT | FMT_SMF.1, FMT_MSA.1/PIN, FIA_AFL.1/PIN, FIA_USB.1, **FIA_ATD.1, FDP_SDI.2** | 14.6.3 |
| ENVELOPE | **This optional command is not supported by the TOE.** | 14.9.1 |
| ERASE BINARY | FDP_ACC.1/TEF, FDP_ACF.1/TEF, **FDP_RIP.1** | 14.3.1 |
| ERASE RECORD | FDP_ACC.1/SEF, FDP_ACF.1/SEF, ~~FMT_MSA.1/SEF~~, **FDP_RIP.1** | 14.4.5 |
| EXTERNAL AUTHENTICATE | FIA_UAU.4, FIA_UAU.5, **FIA_UAU.6**, FIA_USB.1, FCS_RNG.1, FCS_CKM.1/AES.SM, FCS_COP.1/COS.ECDSA.V, ~~FCS_COP.1/RSA.CVC.V~~[18], ~~FCS_COP.1/CB.AES, FCS_COP.1/CB.CMAC~~[19], **FDP_SDI.2, FIA_ATD.1, FDP_RIP.1** | 14.7.1 |
| FINGERPRINT | FPT_ITE.1, **FDP_ACC.1/MF_DF**, FDP_ACF.1/MF_DF | 14.9.2 |
| GENERAL AUTHENTICATE | FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_API.1, FIA_USB.1, FCS_RNG.1, FCS_COP.1/COS.AES, ~~FCS_CKM.1/AES.SM~~[20], **FCS_COP.1/COS.CMAC**, **FCS_COP.1/COS.ECDSA.V, FCS_COP.1/SHA, FDP_SDI.2, FCS_RNG.1/PACE, FCS_CKM.1/DH.PACE.PICC, FIA_UID.1/PACE, FIA_UAU.4/PACE.PICC,** FIA_UAU.5/PACE**.PICC**, FIA_UAU.6/PACE**.PICC**, | 14.7.2 |

[17] Package Logical Channel **is** supported by the TOE
[18] Package RSA CVC **is not** supported by the TOE
[19] Package Crypto Box **is not** supported by the TOE
[20] Package Crypto Box **is not** supported by the TOE

| Operation | SFR | Section |
|---|---|---|
| | FIA_USB.1/PACE**.PICC, FDP_RIP.1/PACE.PICC, FDP_UCT.1/PACE, FDP_UIT.1/PACE** [21]**, FIA_ATD.1/PACE** | |
| GENERATE ASYMMETRIC KEY PAIR | FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3, FMT_SMF.1, FCS_CKM.1/RSA[22], FCS_CKM.1/ELC, **FDP_SDI.2** | 14.9.3 |
| GET ATTRIBUTE[23] | **FMT_MTD.1/NE, FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF, FPT_ITE.2, FPT_ITE.2/PACE**[24] | - |
| GET CHALLENGE | FCS_RNG.1**, FIA_UAU.1, FIA_UID.1, FDP_ACC.1/MF_DF**, **FDP_ACF.1/MF_DF** | 14.9.4 |
| GET DATA | **FPT_ITE.2, FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF, FIA_UAU.1, FIA_UID.1, FMT_MTD.1/NE, FPT_ITE.2/PACE**[25] | 14.5.1 |
| GET PIN STATUS | FMT_SMF.1, FMT_MSA.1/PIN, **FDP_SDI.2, FPT_ITE.2, FPT_ITE.2/PACE**[26] | 14.6.4 |
| GET RANDOM | FCS_RNG.1/GR | 14.9.5 |
| GET RESPONSE | **This optional command is not supported by the TOE.** | 14.9.6 |
| GET SECURITY STATUS KEY | FMT_SMF.1, FMT_MSA.1/Auth | 14.7.3 |
| INTERNAL AUTHENTICATE | FIA_API.1, ~~FCS_CKM.1/AES.SM~~[27], FCS_COP.1/COS.RSA.S, FCS_COP.1/COS.ECDSA.S, | 14.7.4 |

[21] Package Contactless **is** supported by the TOE
[22] Package RSA Key Generation **is** supported by the TOE
[23] Proprietary Idemia command to retrieve information of objects on the card needed by the Wrapper.
[24] Package Contactless **is** supported by the TOE
[25] Package Contactless **is** supported by the TOE
[26] Package Contactless **is** supported by the TOE
[27] Package Crypto Box **is not** supported by the TOE

| Operation | SFR | Section |
|---|---|---|
| | ~~FCS_COP.1/RSA.CVC.S~~[28], ~~FCS_COP.1/CB.AES,~~ ~~FCS_COP.1/CB.CMAC~~[29], **FDP_SDI.2, FCS_RNG.1, FCS_COP.1/SHA** | |
| LOAD APPLICATION | FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF, FMT_SMF.1, FMT_MSA.1/Life, **FMT_MSA.3, FMT_MTD.1/Auth, FDP_RIP.1**, **FCS_COP.1/COS.ECDSA.V**[30] | 14.2.5 |
| LIST PUBLIC KEY | FPT_ITE.2, FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF, **FIA_UAU.1, FIA_UID.1, FMT_MTD.1/NE, FDP_SDI.2, FPT_ITE.2/PACE**[31] | 14.9.7 |
| MANAGE CHANNEL | FIA_UID.1, FIA_UAU.1, FIA_USB.1/LC[32], FMT_MSA.3, **FIA_ATD.1, FIA_ATD.1/PACE**[33] | 14.9.8 |
| MANAGE SECURITY ENVIRONMENT | FIA_USB.1, FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3**, FIA_UAU.1, FIA_UID.1, FIA_ATD.1, FMT_MTD.1/Auth** | 14.9.9 |
| MUTUAL AUTHENTICATE | FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_API.1, FIA_USB.1, FCS_RNG.1, FCS_CKM.1/AES.SM, FCS_COP.1/COS.AES, FCS_COP.1/COS.CMAC, **FDP_SDI.2, FIA_ATD.1, FDP_RIP.1** | 14.7.1 |
| PSO COMPUTE CRYPTOGRAPHIC CHECKSUM[34] | ~~FDP_ACC.1/KEY, FDP_ACF.1/KEY, FIA_API.1/CB, FCS_COP.1/CB.CMAC, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_USB.1/PACE~~ **This Crypto Box command is not supported by the TOE.** | 14.8.1 |

[28] Package RSA CVC **is not** supported by the TOE
[29] Package Crypto Box **is not** supported by the TOE
[30] Digital signature verification for object system import in phase 6 (Product Pre-Personalisation)
[31] Package Contactless **is** supported by the TOE
[32] Package Logical Channel **is** supported by the TOE
[33] Package Logical Channel **is** supported by the TOE
[34] Package Crypto Box **is not** supported by the TOE

| Operation | SFR | Section |
|---|---|---|
| PSO COMPUTE DIGITAL SIGNATURE, WITHOUT "RECOVERY" | FDP_ACC.1/KEY, FDP_ACF.1/KEY, ~~FMT_MSA.3~~, FCS_COP.1/COS.RSA.S, FCS_COP.1/COS.ECDSA.S, **FCS_COP.1/SHA**, **FDP_SDI.2** | 14.8.2.1 |
| PSO COMPUTE DIGITAL SIGNATURE, WITH "RECOVERY" | FDP_ACC.1/KEY, FDP_ACF.1/KEY, ~~FMT_MSA.3~~, FCS_COP.1/COS.~~ECDSA~~**RSA**.S, **FDP_SDI.2** | 14.8.2.2 |
| PSO DECIPHER | ~~FIA_USB.1,~~ FDP_ACC.1/KEY, FDP_ACF.1/KEY, ~~FMT_MSA.3~~, FCS_COP.1/COS.RSA, FCS_COP.1/COS.ELC, ~~FCS_COP.1/CB.AES~~[35], ~~FIA_UAU.5/PACE~~**~~.PICC~~**, ~~FIA_UAU.6/PACE~~**~~.PICC~~**, ~~FIA_USB.1/PACE~~**~~.PICC~~**[36], **FCS_COP.1/SHA, FDP_SDI.2** | 14.8.3 |
| PSO ENCIPHER | ~~FIA_API.1~~[37], FDP_ACC.1/KEY, FDP_ACF.1/KEY, ~~FMT_MSA.3~~[38], FCS_COP.1/COS.RSA, FCS_COP.1/COS.ELC, ~~FCS_COP.1/CB.AES, FCS_COP.1/CB.RSA, FCS_COP.1/CB.ELC~~[39], **FCS_COP.1/SHA, FDP_SDI.2** | 14.8.4 |
| PSO HASH, [ISO/IEC 7816–8] | **This optional command is not supported by the TOE.** | 14.8.5 |
| PSO TRANSCIPHER USING RSA | FDP_ACC.1/KEY, FDP_ACF.1/KEY, ~~FMT_MSA.3~~[40], FCS_COP.1/COS.RSA, **FCS_COP.1/SHA**, FCS_COP.1/COS.ELC, **FDP_SDI.2** | 14.8.6.1, 14.8.6.2, 14.8.6.4 |

[35] Package Crypto Box **is not** supported by the TOE

[36] Package Contactless **is** supported, but package Crypto Box is not supported by the TOE, so that symmetric decryption using session keys is not supported. Thus, FIA_UAU.5/PACE.PICC, FIA_UAU.6/PACE.PICC, FIA_USB.1/PACE.PICC and FIA_USB.1 are not relevant for PSO DECIPHER.

[37] FIA_API.1 refers to the authentication means offered by the product which do not play a role for PSO ENCIPHER.

[38] FMT_MSA.3 refers to setting restrictive default values for security attributes which does not relates to PSO ENCIPHER.

[39] Package Crypto Box **is not** supported by the TOE

[40] FMT_MSA.3 refers to setting restrictive default values for security attributes which does not relates to PSO TRANSCIPHER.

| Operation | SFR | Section |
|---|---|---|
| PSO TRANSCIPHER USING ELC | FDP_ACC.1/KEY, FDP_ACF.1/KEY, ~~FMT_MSA.3~~[41], FCS_COP.1/COS.RSA, **FCS_COP.1/SHA**, FCS_COP.1/COS.ELC, **FDP_SDI.2** | 14.8.6.2, 14.8.6.3, 14.8.6.4 |
| PSO VERIFY CERTIFICATE | FMT_SMF.1, FMT_MTD.1/Auth, FCS_COP.1/COS.ECDSA.V**, FCS_COP.1/SHA**, FDP_ACC.1/KEY, FDP_ACF.1/KEY, ~~FCS_COP.1/RSA.CVC.V~~[42], **FDP_SDI.2, FPT_TDC.1** | 14.8.7 |
| PSO VERIFY CRYPTOGRAPHIC CHECKSUM[43] | ~~FDP_ACC.1/KEY, FDP_ACF.1/KEY, FIA_USB.1/CB, FCS_COP.1/CB.CMAC~~ **This Crypto Box command is not supported by the TOE.** | 14.8.8 |
| PSO VERIFY DIGITAL SIGNATURE | FDP_ACC.1/KEY, FDP_ACF.1/KEY, ~~FMT_MSA.3~~[44], FCS_COP.1/COS.ECDSA.V, **FDP_SDI.2** | 14.8.9 |
| PUT DATA[45] | **FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF, FIA_UAU.1, FIA_UID.1, FMT_SMF.1** | 14.5.2 |
| READ BINARY | FDP_ACC.1/TEF, FDP_ACF.1/TEF | 14.3.2 |
| READ RECORD | FDP_ACC.1/SEF, FDP_ACF.1/SEF | 14.4.6 |
| REINIT[46] | **FMT_SMF.1, FMT_MSA.1/Life, FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF** | - |

[41] FMT_MSA.3 refers to setting restrictive default values for security attributes which does not relates to PSO TRANSCIPHER.

[42] Package RSA CVC **is not** supported by the TOE

[43] Package Crypto Box **is not** supported by the TOE

[44] FMT_MSA.3 refers to setting restrictive default values for security attributes which does not relates to PSO VERIFY DIGITAL SIGNATURE.

[45] PUT DATA is only supported in preparation phases, but not supported in phase 7 (Operational Use)

[46] Proprietary Idemia command to perform a re-initialisation of the card. This command is only available, if the card is configured as Testcard. The command is effectively blocked for all operational cards.

| Operation | SFR | Section |
|---|---|---|
| RESET RETRY COUNTER | FIA_AFL.1/PUC, FIA_UAU.5, FMT_SMF.1, FMT_MTD.1/PIN, FMT_MSA.1/PIN, **FIA_AFL.1/PIN, FIA_ATD.1, FDP_SDI.2** | 14.6.5 |
| SEARCH BINARY | **This optional command is not supported by the TOE.** | 14.3.3 |
| SEARCH RECORD | FDP_ACC.1/SEF, FDP_ACF.1/SEF | 14.4.7 |
| SELECT | FIA_USB.1, FDP_ACC.1/MF_DF, FDP_ACF.1/ MF_DF, FDP_ACC.1/EF, FDP_ACF.1/EF, **FIA_UAU.1, FIA_UID.1, FMT_MSA.1/Life, FDP_RIP.1, FIA_ATD.1** | 14.2.6 |
| SET LOGICAL EOF | FDP_ACC.1/TEF, FDP_ACF.1/TEF, **FDP_RIP.1** | 14.3.4 |
| TERMINATE | FMT_SMF.1, FMT_MSA.1/Life | 14.2.9 |
| TERMINATE CARD USAGE | FMT_SMF.1, FMT_MSA.1/Life | 14.2.7 |
| TERMINATE DF | FMT_SMF.1, FMT_MSA.1/Life | 14.2.8 |
| UPDATE BINARY | FDP_ACC.1/TEF, FDP_ACF.1/TEF | 14.3.5 |
| UPDATE RECORD | FDP_ACC.1/SEF, FDP_ACF.1/SEF | 14.4.8 |
| VERIFY | FIA_AFL.1/PIN, FIA_UAU.5, FIA_USB.1, FMT_SMF.1, FMT_MSA.1/PIN, **FDP_SDI.2, FIA_ATD.1** | 14.6.6 |
| WRITE BINARY | FDP_ACC.1/TEF, FDP_ACF.1/TEF | 14.3.6 |
| WRITE RECORD | **This optional command is not supported by the TOE.** | 14.4.9 |

**Table 24: Mapping between commands described in COS specification [21] and the SFRs**

*Application note 4*: An implementation has to support the data types and the limits for the data types given in [21] exactly. If an implementation of COS supports additional values / types or extends limits it must be guaranteed that no Security Objective can be undermined. A justification for each additional difference and why it does not undermine a Security Objective has to be given from the developer. **(The TOE does not support additional values / types or extended limits)**

*Application note 5*: If an implementation of COS accepts objects that do not follow defined rules it must be guaranteed that no Security Objective can be undermined. A justification for each accepted object and why it does not undermine a Security Objective has to be given from the developer. **(The TOE does not accept objects that do not follow the defined rules)**

*Application note 6*: If an implementation of COS implements additional functionality not described in [21] it must be guaranteed that the additional functionality cannot undermined any Security Objective. A justification for added additional functionality and why it does not undermine any Security Objective has to be given from the developer (cf. SAR ADV_ARC.1). If the additional functionality implements further TSF with cryptographic mechanisms the SFR component FCS_COP has to be iterated corresponding to the new introduced cryptographic functionality. **(FCS_COP has been iterated by the IC Platform Security Target [ST_IC] according section 6.1.3)**

### 6.1.3 Security Functional Requirements for the TOE taken over from the IC Platform Security Target

From section 7 in the IC Platform Security Target [ST_IC] SFRs are part of this ST. On each SFR of [ST_IC] an iteration operation is performed. For the iteration operation, the suffix "/SICP" (short for: Secure Integrated Chip Platform) is added to the respective SFR name in [ST_IC]. In case of already iterated SFRs in [ST_IC], this ST adds the suffix "_SICP".

The complete list of the SFRs from [ST_IC] and which are taken over follows. For further descriptions, details, and interpretations refer to section 7 in [ST_IC].

| SFR name | Description | Taken over as | Comment |
|---|---|---|---|
| By the ACLs | | | |
| FCS_CKM.1/RSA-0 | Cryptographic key generation-RSA by ACL-0 | FCS_CKM.1/RSA-0_SICP | RSA by ACL v2.09.002 used |
| FCS_CKM.1/RSA-1 | Cryptographic key generation-RSA by ACL-1 | - | ACL v2.08.007 not used |
| FCS_CKM.1/RSA-2 | Cryptographic key generation-RSA by ACL-2 | - | ACL v2.07.003 not used |
| FCS_CKM.1/RSA-3 | Cryptographic key generation-RSA by ACL-3 | - | ACL v2.06.003 not used |

| SFR name | Description | Taken over as | Comment |
|---|---|---|---|
| FCS_CKM.1/EC-0 | Cryptographic key generation-EC by ACL-1 | FCS_CKM.1/EC-0_SICP | EC by ACL v2.09.002 used |
| FCS_CKM.1/EC-1 | Cryptographic key generation-EC by ACL-0 | - | ACL v2.08.007 not used |
| FCS_CKM.1/EC-2 | Cryptographic key generation-EC by ACL-2 | - | ACL v2.07.003 not used |
| FCS_CKM.1/EC-3 | Cryptographic key generation-EC by ACL-3 | - | ACL v2.06.003 not used |
| FCS_COP.1/RSA-0 | Cryptographic operation – RSA by ACL-0 | FCS_COP.1/RSA-0_SICP | ACL v2.09.002 used |
| FCS_COP.1/RSA-1 | Cryptographic operation – RSA by ACL-1 | - | ACL v2.08.007 not used |
| FCS_COP.1/RSA-2 | Cryptographic operation – RSA by ACL-2 | - | ACL v2.07.003 not used |
| FCS_COP.1/RSA-3 | Cryptographic operation – RSA by ACL-3 | - | ACL v2.06.003 not used |
| FCS_COP.1/ECDSA-0 | Cryptographic operation – ECDSA by ACL-0 | FCS_COP.1/ECDSA-0_SICP | ACL v2.09.002 used |
| FCS_COP.1/ECDSA-1 | Cryptographic operation – ECDSA by ACL-1 | - | ACL v2.08.007 used |
| FCS_COP.1/ECDSA-2 | Cryptographic operation – ECDSA by ACL-2 | - | ACL v2.07.003 not used |
| FCS_COP.1/ECDSA-3 | Cryptographic operation – ECDSA by ACL-3 | - | ACL v2.06.003 not used |
| FCS_COP.1/ECDH-0 | Cryptographic operation – ECDH by ACL-0 | FCS_COP.1/ECDH-0_SICP | ACL v2.09.002 used |
| FCS_COP.1/ECDH-1 | Cryptographic operation – ECDH by ACL-1 | - | ACL v2.08.007 not used |
| FCS_COP.1/ECDH-2 | Cryptographic operation – ECDH by ACL-2 | - | ACL v2.07.003 not used |
| FCS_COP.1/ECDH-3 | Cryptographic operation – ECDH by ACL-3 | - | ACL v2.06.003 not used |
| By the SCLs | | | |

| SFR name | Description | Taken over as | Comment |
|---|---|---|---|
| FCS_COP.1/TDES-SCL-1 | Cryptographic operation – TDES by SCL-1 | - | TDES not used |
| FCS_CKM.4/TDES-SCL-1 | Cryptographic key destruction – TDES by SCL-1 | - | TDES not used |
| FCS_COP.1/AES-SCL-1 | Cryptographic operation – AES by SCL-1 | FCS_COP.1/AES-SCL-1_SICP | AES by SCL v02.04.002 used |
| FCS_CKM.4/AES-SCL-1 | Cryptographic key destruction – AES by SCL-1 | FCS_CKM.4/AES-SCL-1_SICP | AES by SCL used |
| FCS_COP.1/CMAC-SCL-1 | Cryptographic operation CMAC by SCL-1 | - | CMAC by SCL not used, last block of AES by SCL-1 in CBC mode used as CMAC |
| FCS_CKM.4/CMAC-SCL-1 | Cryptographic key destruction CMAC by SCL-1 | - | CMAC by SCL not used, last block of AES by SCL-1 in CBC mode used as CMAC |
| FCS_COP.1/TDES-SCL-2 | Cryptographic operation – TDES by SCL-2 | - | TDES not used |
| FCS_CKM.4/TDES-SCL-2 | Cryptographic key destruction – TDES by SCL-2 | - | TDES not used |
| FCS_COP.1/AES-SCL-2 | Cryptographic operation – AES by SCL-2 | - | SCL v02.02.010 not used |
| FCS_CKM.4/AES-SCL-2 | Cryptographic key destruction – AES by SCL-2 | - | SCL v02.02.010 not used |
| By the CIPURSE™ CLs | | | |
| FCS_CKM.1/CCL | Cryptographic key generation - CIPURSE™ CL by CCL | - | CIPURSE™ not used |
| FCS_CKM.4/CCL | Cryptographic key destruction CIPURSE™ CL by CCL | - | CIPURSE™ not used |
| FCS_COP.1/CCL | Cryptographic operation – CIPURSE™ CL Trusted Channel by CCL | - | CIPURSE™ not used |
| By Hardware, Firmware and the HSLs | | | |

| SFR name | Description | Taken over as | Comment |
|---|---|---|---|
| FCS_CKM.4/AES | Cryptographic key destruction – AES by SCP | - | AES by SCP not used |
| FCS_COP.1/AES | Cryptographic operation – AES by SCP | - | AES by SCP not used |
| FCS_CKM.4/TDES | Cryptographic key destruction – TDES by SCP | - | TDES not used |
| FCS_COP.1/TDES | Cryptographic operation – TDES by SCP | - | TDES not used |
| FAU_SAS.1 | Audit data storage | FAU_SAS.1/SICP | Mandatory SFR |
| FCS_RNG.1/DRNG | Generation of Random Numbers – DRNG | - | DRNG not used |
| FCS_RNG.1/HPRG | Random number generation – HPRG | FCS_RNG.1/HPRG _SICP | HPRG used |
| FCS_RNG.1/KSG | Random number generation – KSG | - | KSG not used |
| FCS_RNG.1/TRNG | Random number generation – TRNG | - | TRNG not used |
| FDP_ACC.1 | Subset access control | FDP_ACC.1/SICP | Mandatory SFR |
| FDP_ACC.1/Loader | Subset access control – Loader | - | Secure Loader blocked |
| FDP_ACF.1 | Security attribute based access control | FDP_ACF.1/SICP | Mandatory SFR |
| FDP_ACF.1/Loader | Security attribute based access control – Loader | - | Secure Loader blocked |
| FDP_IFC.1 | Subset information flow control | FDP_IFC.1/SICP | Mandatory SFR |
| FDP_ITT.1 | Basic internal transfer protection | FDP_ITT.1/SICP | Mandatory SFR |
| FDP_SDC.1 | Stored data confidentiality | FDP_SDC.1/SICP | Mandatory SFR |
| FDP_SDI.2 | Stored data integrity monitoring and action | FDP_SDI.2/SICP | Mandatory SFR |
| FDP_UCT.1 | Basic data exchange confidentiality | - | Secure Loader blocked |

| SFR name | Description | Taken over as | Comment |
|---|---|---|---|
| FDP_UIT.1 | Data exchange integrity | - | Secure Loader blocked |
| FIA_API.1 | Authentication Proof of Identity | FIA_API.1/SICP | Authentication of the Security IC used |
| FMT_LIM.1 | Limited capabilities | FMT_LIM.1/SICP | Mandatory SFR |
| FMT_LIM.1/Loader | Limited capabilities | - | Secure Loader blocked |
| FMT_LIM.2 | Limited availability | FMT_LIM.2/SICP | Mandatory SFR |
| FMT_LIM.2/Loader | Limited availability | - | Secure Loader blocked |
| FMT_MSA.1 | Management of security attributes | FMT_MSA.1/SICP | Mandatory SFR |
| FMT_MSA.3 | Static attribute initialization | FMT_MSA.3/SICP | Mandatory SFR |
| FMT_SMF.1 | Specification of Management functions | FMT_SMF.1/SICP | Mandatory SFR |
| FPT_FLS.1 | Failure with preservation of secure state | FPT_FLS.1/SICP | Mandatory SFR |
| FTP_ITC.1 | Inter-TSF trusted channel – Loader | - | Secure Loader blocked |
| FPT_ITT.1 | Basic internal TSF data transfer protection | FPT_ITT.1/SICP | Mandatory SFR |
| FPT_PHP.3 | Resistance to physical attack | FPT_PHP.3/SICP | Mandatory SFR |
| FPT_TST.2 | TOE security testing | FPT_TST.2/SICP | Mandatory SFR |
| FRU_FLT.2 | Limited fault tolerance | FRU_FLT.2/SICP | Mandatory SFR |

**Table 25: SFRs from the IC Platform Security Target [ST_IC] and which are taken over**

In some cases Security Functional Requirements have been added or refined in BSI-CC-PP-0084-2014 [11] and in the IC Platform Security Target [ST_IC]. In view of refinements specified for Security Assurance Requirements refer to section 6.2.

Note that the Security IC Platform makes use of optional Packages in BSI-CC-PP-0084-2014 [11]. An overview of the usage of optional Packages and which are relevant for the present TOE is given in section 1.2.5. The ST author incorporated the respective SFRs of the relevant Packages in this ST and adapted the related rationale and dependency analysis accordingly.

### 6.1.4 General Protection of User Data and TSF Data

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

| | |
|---|---|
| **FDP_RIP.1** | Subset residual information protection |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FDP_RIP.1.1 | The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[47] the following objects: password objects, secret cryptographic keys, private cryptographic keys, session keys, and data in all files[48] [49]. |

*Application note 7:* The author 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.**

[47] [selection: *allocation of the resource to, deallocation of the resource from*]
[48] [assignment: *other data objects*]
[49] [assignment: *list of objects*]

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

| | |
|---|---|
| **FDP_SDI.2** | Stored data integrity monitoring and action |
| Hierarchical to: | FDP_SDI.1 Stored data integrity monitoring |
| Dependencies: | No dependencies. |
| FDP_SDI.2.1 | The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors[50] on all objects, based on the following attributes:<br>(1) key objects,<br>(2) PIN objects,<br>(3) *affectedObject.flagTransactionMode=TRUE*,<br>(4) user data in protected files,<br>(5) external input data for digital signature.[51] [52]. |
| FDP_SDI.2.2 | Upon detection of a data integrity error, the TSF shall prevent the usage of the altered data[53]. |

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

| | |
|---|---|
| **FPT_FLS.1** | Failure with preservation of secure state |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_FLS.1.1 | The TSF shall preserve a secure state when the following types of failures occur:<br>(1) exposure to operating conditions where therefore a malfunction could occur,<br>(2) failure detected by TSF according to FPT_TST.1.[54] |

[50] [assignment: *integrity errors*]
[51] [assignment: *other user data attributes*]
[52] [assignment: *user data attributes*]
[53] [assignment: *action to be taken*]
[54] [assignment: *list of types of failures in the TSF*]

The TOE shall meet the requirement "Emanation of TSF and User data (FPT_EMS.1)" as specified below (CC Part 2 extended).

| | |
|---|---|
| **FPT_EMS.1** | Emanation of TSF and User data |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_EMS.1.1 | The TOE shall not emit information on IC power consumption, information on command execution time, information on electromagnetic emanations[55] in excess of non-useful information[56] enabling access to the following TSF data<br>(1) Regular password,<br>(2) Multi-Reference password,<br>(3) PUC,<br>(4) Session keys,<br>(5) Symmetric authentication keys,<br>(6) Private authentication keys,<br>(7) no other TSF data[57] [58]<br>and the following user data<br>(1) Private asymmetric keys,<br>(2) Symmetric keys,<br>(3) no other user data[59] [60]. |
| FPT_EMS.1.2 | The TSF shall ensure any user[61] are unable to use the following interface circuit interfaces[62] to gain access to the following TSF data<br>(1) Regular password,<br>(2) Multi-Reference password,<br>(3) PUC, |

[55] [assignment: *types of emissions*]
[56] [assignment: *specified limits*]
[57] [assignment: *list of additional types of TSF data*]
[58] [assignment: *list of types of TSF data*]
[59] [assignment: *list of additional types of user data*]
[60] [assignment: *list of types of user data*]
[61] [assignment: *type of users*]
[62] [assignment: *type of connection*]

(4) Session keys,
(5) Symmetric authentication keys,
(6) Private authentication keys,
(7) no other TSF data[63] [64]
and the following user data
(1) Private asymmetric keys,
(2) Symmetric keys,
(3) no other user data[65] [66].

The TOE shall meet the requirement "Inter-TSF basic TSF data consistency (FPT_TDC.1)" as specified below.

| | |
|---|---|
| **FPT_TDC.1** | Inter-TSF basic TSF data consistency |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_TDC.1.1 | The TSF shall provide the capability to consistently interpret Card Verifiable Certificate (CVC)[67] when shared between the TSF and another trusted IT product. |
| FPT_TDC.1.2 | The TSF shall use ~~[21], section 7.1 "CV-Certificates for RSA keys" (if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE),~~[68] [21], section 7.2 "CV-Certificates for ELC keys"[69] when interpreting the TSF data from another trusted IT product. |

[63] [assignment: *list of additional types of TSF data*]
[64] [assignment: *list of types of TSF data*]
[65] [assignment: *list of additional types of user data*]
[66] [assignment: *list of types of user data*]
[67] [assignment: *list of TSF data types*]
[68] Refinement: Option_RSA_CVC **is not** supported by the TOE
[69] [assignment: *list of interpretation rules to be applied by the TSF*]

The TOE shall meet the requirement "Export of TOE implementation fingerprint (FPT_ITE.1)" as specified below.

| | |
|---|---|
| **FPT_ITE.1** | Export of TOE implementation fingerprint |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_ITE.1.1 | The TOE shall export fingerprint of TOE implementation given the following conditions execution of the command FINGERPRINT [21][70]. |
| FPT_ITE.1.2 | The TSF shall use SHA-256 based fingerprint of the TOE implementation[71] for the exported data. |

*Application note 8*: The command FINGERPRINT calculates a hash value or CMAC based fingerprint over the complete executable code actually implemented by the TOE including related configuration data. The TOE implementation includes the IC Dedicated Support Software, the Card Operating System, application specific code loaded on the smart card by the command LOAD CODE or any other means as well as all TOE implementation related configuration data. The hash function or the CMAC respectively based calculation uses the prefix sent in the command FINGERPRINT for "fresh" fingerprints over all executable code (including related configuration data), i.e. no precomputed values over fixed parts of the TOE implementation only. For more details on the intention of the export of TOE implementation fingerprints refer to section 5.3.

[70] [assignment: *conditions for export*]

[71] [selection: *SHA-256 based fingerprint of the TOE implementation, SHA-384 based fingerprint of the TOE implementation, SHA-512 based fingerprint of the TOE implementation, CMAC based fingerprint of the TOE implementation using [selection: AES-128, AES-192, AES-256] with cryptographic key size [selection: 128 bit, 192 bit, 256 bit] that meet the following standard [selection: FIPS180-4 [37], NIST SP800-38B [36]]*]

The TOE shall meet the requirement "Export of TSF data (FPT_ITE.2)" as specified below.

| | |
|---|---|
| **FPT_ITE.2** | Export of TSF data |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_ITE.2.1 | The TOE shall export<br>(1) all public authentication reference data,<br>(2) all security attributes of the object system and for all objects of the object system for all commands,<br>(3) none[72] [73]<br>given the following conditions<br>(1) no export of secret data,<br>(2) no export of private keys,<br>(3) no export of secure messaging keys,<br>(4) no export of passwords and PUC[74]. |
| FPT_ITE.2.2 | The TSF shall use Idemia proprietary encoding rules that meet the requirements of the Technical Guideline BSI TR-03143 [20] (so that the exported data can be transformed by the Idemia wrapper implementation into the specified coding format of the Gematik)[75] for the exported data. |

*Application note 9*: 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], *applicationPublicKeyList* 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

[72] [assignment: *list of all TOE specific security attributes not described in COS specification [21]*]
[73] [assignment: *list of types of TSF data*]
[74] [assignment: *conditions for export*]
[75] [assignment: *list of encoding rules to be applied by TSF*]

of object types listed in Table 23 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 that 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 that 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 the wrapper to allow interpretation of the TSF Data. The encoding rules shall meet the requirements of the Technical Guideline BSI TR-03143 [20] describing the verification tool used for examination of the object system against the specification of the object system **(the wrapper encodes accordingly)**.

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

| | |
|---|---|
| **FPT_TST.1** | TSF testing |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_TST.1.1 | The TSF shall run a suite of self tests during initial start-up[76] to demonstrate the correct operation of the TSF[77]. |
| FPT_TST.1.2 | The TSF shall provide authorised users with the capability to verify the integrity of TSF data[78]. |
| FPT_TST.1.3 | The TSF shall provide authorised users with the capability to verify the integrity of TSF[79]. |

[76] [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]*]

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

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

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

### 6.1.5 Authentication

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

| | |
|---|---|
| **FIA_SOS.1** | Verification of secrets |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_SOS.1.1 | The TSF shall provide a mechanism to verify that secrets provided by the user for password objects meet the quality metric: length not lower than *minimumLength* and not greater than *maximumLength*[80]. |

The TOE shall meet the requirement "Authentication failure handling (FIA_AFL.1/PIN)" as specified below.

| | |
|---|---|
| **FIA_AFL.1/PIN** | Authentication failure handling |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UAU.1 Timing of authentication |
| FIA_AFL.1.1/PIN | The TSF shall detect when ~~an administrator~~ configurable positive integer within 1 to 15[81] 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[82]. |
| FIA_AFL.1.2/PIN | When the defined number of unsuccessful authentication attempts has been met[83], the TSF shall block the password for authentication until successful unblock using command RESET RETRY COUNTER<br>(1) P1='00' or P1='01' with presenting unblocking code PUC of this password object,<br>(2) P1='02' or P1='03' without presenting unblocking code PUC of this password object[84]. |

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

[81] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

*Application note 10:* 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.

The TOE shall meet the requirement “Authentication failure handling (FIA_AFL.1/PUC)” as specified below.

[82] [assignment: *list of authentication events*]
[83] [selection: *met, surpassed*]
[84] [assignment: *list of actions*]

| | |
|---|---|
| **FIA_AFL.1/PUC** | Authentication failure handling |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UAU.1 Timing of authentication |
| FIA_AFL.1.1/PUC | The TSF shall detect when ~~an administrator~~ configurable positive integer within 1 to 15[85] ~~unsuccessful~~[86] authentication attempts occur related to usage of a password unblocking code using the RESET RETRY COUNTER command[87]. |
| FIA_AFL.1.2/PUC | When the defined number of ~~unsuccessful~~[88] authentication attempts has been met[89], the TSF shall<br>(1) warn the entity connected<br>(2) not unblock the referenced blocked PIN<br>(3) 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.[90]. |

*Application note 11:* 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.

*Application note 12:* 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.

---

[85] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

[86] Refinement: not only unsuccessful but all attempts shall be counted here – obviously this refinement is valid, because the original requirement is still fulfilled.

[87] [assignment: *list of authentication events*]

[88] Refinement: not only unsuccessful but all attempts shall be counted here – obviously this refinement is valid, because the original requirement is still fulfilled.

[89] [selection: *met, surpassed*]

[90] [assignment: *list of actions, which at least includes: block the password unblocking code*]

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

| | |
|---|---|
| **FIA_ATD.1** | User attribute definition |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_ATD.1.1 | The TSF shall maintain the following list of security attributes belonging to individual users:<br>(1) for Human User: authentication state gained<br>a. with password: *pwdIdentifier* in *globalPasswordList* and *pwdIdentifier* in *dfSpecificPasswordList*,<br>b. with Multi-Reference password: *pwIdentifier* in *globalPasswordList* and *pwIdentifier* in *dfSpecificPasswordList*,<br>(2) for Device: authentication state gained<br>a. ~~if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE: by CVC with CHA in *globalSecurityList* if CVC is stored in MF and *dfSpecificSecurityList* if CVC is stored in a DF,~~[91]<br>b. by CVC with CHAT in *bitSecurityList*,<br>c. with symmetric authentication key: *keyIdentity* of the key,<br>d. with secure messaging keys: *keyIdentity* of the key used for establishing the session key[92]. |

[91] Refinement: Option_RSA_CVC **is not** supported by the TOE

[92] [assignment: *list of security attributes*]

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

| | |
|---|---|
| **FIA_UAU.1** | Timing of authentication |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UID.1 Timing of identification |
| FIA_UAU.1.1 | The TSF shall allow<br>(1) reading the ATR,<br>(2) GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT and SELECT[93],<br>(3) commands with access control rule ALWAYS for the current life cycle status and depending on the interface,<br>(4) LIST PUBLIC KEY, GET DATA, PUT DATA[94] [95]<br>on behalf of the user to be performed before the user is authenticated. |
| FIA_UAU.1.2 | The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. |

Application note 13: 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 then 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)** .

[93] [selection: *GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, SELECT*]
[94] [assignment: *list of additional TSF mediated actions*]
[95] [assignment: *list of TSF mediated actions*]

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

| | |
|---|---|
| **FIA_UAU.4** | Single-use authentication mechanisms |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_UAU.4 .1 | The TSF shall prevent reuse of authentication data related to<br>(1) external device authentication by means of executing the command EXTERNAL AUTHENTICATE with symmetric or asymmetric key,<br>(2) external device authentication by means of executing the command MUTUAL AUTHENTICATE with symmetric or asymmetric key,<br>(3) external device authentication by means of executing the command GENERAL AUTHENTICATE with symmetric or asymmetric key,<br>(4) none[96] [97]. |

[96] [assignment: *additional identified authentication mechanism(s)*]
[97] [assignment: *identified authentication mechanism(s)*]

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

| | |
|---|---|
| **FIA_UAU.5** | Multiple authentication mechanisms |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_UAU.5.1 | The TSF shall provide<br>(1) the execution of the VERIFY command,<br>(2) the execution of the CHANGE REFERENCE DATA command,<br>(3) the execution of the RESET RETRY COUNTER command,<br>(4) the execution of the EXTERNAL AUTHENTICATE command,<br>(5) the execution of the MUTUAL AUTHENTICATE command,<br>(6) the execution of the GENERAL AUTHENTICATE command,<br>(7) a secure messaging channel,<br>(8) a trusted channel[98]<br>to support user authentication. |
| FIA_UAU.5.2 | The TSF shall authenticate any user's claimed identity according to the following rules:<br>(1) password based authentication shall be used for authenticating a human user by means of the commands VERIFY, CHANGE REFERENCE DATA and RESET RETRY COUNTER,<br>(2) key based authentication mechanisms shall be used for authenticating of devices by means of the commands EXTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE and GENERAL AUTHENTICATE,<br>(3) none[99] [100]. |

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

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

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

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below.

| | |
|---|---|
| **FIA_UAU.6** | Re-authenticating |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_UAU.6.1 | The TSF shall re-authenticate the ~~user~~ **sender of a message**[101] under the conditions<br>(1) each command sent to the TOE after establishing the secure messaging by successful authentication after 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[102]. |

*Application note 14*: 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. section 7 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)

[101] Refinement: identifying the concrete user

[102] [assignment: *list of conditions under which re-authentication is required*]

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) 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.

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

| | |
|---|---|
| **FIA_UID.1** | Timing of identification |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_UID.1.1 | The TSF shall allow<br>(1) reading the ATR,<br>(2) GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, SELECT[103],<br>(3) commands with access control rule ALWAYS for the current life cycle status and depending on the interface,<br>(4) LIST PUBLIC KEY, GET DATA, PUT DATA [104]<br>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. |

*Application note 15:* 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

[103] [selection: *GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, SELECT*]

[104] [assignment: *list of TSF mediated actions*]

FIA_UID.1.1 **(no TOE specific access control rules defined, all these commands are listed in FIA_UID.1.1)**.

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2 extended (see section 5.1)).

| | |
|---|---|
| **FIA_API.1** | Authentication Proof of Identity |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_API.1.1 | The TSF shall provide ~~a~~<br>(1) INTERNAL AUTHENTICATE,<br>(2) MUTUAL AUTHENTICATE,<br>(3) GENERAL AUTHENTICATE[105]<br>to prove the identity of the TSF itself[106] to an external entity. |

[105] [assignment: *authentication mechanism*]
[106] [assignment: *object, authorised user or rule*].

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

| | |
|---|---|
| **FMT_SMR.1** | Security roles |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UID.1 Timing of identification |
| FMT_SMR.1.1 | The TSF shall maintain the roles<br>(1) World as unauthenticated user without authentication reference data,<br>(2) Human User authenticated by password in the role defined for this password,<br>(3) Human User authenticated by PUC as holder of the corresponding password,<br>(4) Device authenticated by means of symmetric key in the role defined for this key,<br>(5) Device authenticated by means of asymmetric key in the role defined by the Certificate Holder Authorisation in the CVC,<br>(6) none[107] [108]. |
| FMT_SMR.1.2 | The TSF shall be able to associate users with roles. |

*Application note 16*: The Protection Profile BSI-CC-PP-0084-2014 does not explicitly define role because roles are linked to life cycle of the chip not addressed by SFR. Therefore the present 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 **(no additional roles added)**.

*Application note 17*: 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 authorisation with a password is defined in the security attributes of the objects and related to identified commands. The authorisation 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

[107] [assignment: *additional authorised identified roles*]
[108] [assignment: *object, authorised identified roles*]

assign additional role like the role defined for authentication by means of PACE protocol (if PACE is supported by the TOE) or "none" **(additional roles for PACE protocol is specified by FMT_SMR.1/PACE.PICC)**.

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

| | |
|---|---|
| **FIA_USB.1** | User-subject binding |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_ATD.1 User attribute definition |
| FIA_USB.1.1 | The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:<br>(1) for Human User authenticated with password: *pwIdentifier* and Authentication Context *globalPasswordList* and *dfSpecificPasswordList*,<br>(2) for Human User authenticated with PUC: *pwIdentifier* of corresponding password,<br>(3) ~~for Device the Role authenticated by RSA-based CVC, if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE: the Certificate Holder Authorisation (CHA) in the CVC,~~[109]<br>(4) for Device the Role authenticated by ECC-based CVC: the Certificate Holder Authorisation Template (CHAT),<br>(5) for Device the Role authenticated by symmetric key: *keyIdentifier* and Authentication Context[110]. |
| FIA_USB.1.2 | The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:<br>(1) If the logical channel is reset by the 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*).<br>(2) If the command SELECT is executed and the newFile is a folder the initial authentication state of the selected folder inherits the authentication state of the folder above up the root[111]. |

[109] Refinement: Option_RSA_CVC **is not** supported by the TOE
[110] [assignment: *list of user security attributes*]
[111] [assignment: *rules for the initial association of attributes*]

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

(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

entries 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), **GENERAL AUTHENTICATE**.

(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 has 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 state of the device in the current context has to be set to "not authenticated" (i.e. the element in *globalSecurityList* respective in *dfSpecificSecurityList* and the used SK4SM are deleted).

(9) none[112] [113].

*Application note 18:* Note that 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 the 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)).

### 6.1.6 Access Control

*Application note 19:* 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,

[112] [assignment: *further rules for the changing of attributes*]
[113] [assignment: *rules for the changing of attributes*]

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~~ (~~if~~ the RSA-based CVC functionality according to Option_RSA_CVC in [21] is **not** supported by the TOE), 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.

The TOE shall meet the requirement "Subset access control (FDP_ACC.1/MF_DF)" as specified below.

| | |
|---|---|
| **FDP_ACC.1/MF_DF** | Subset access control |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACF.1 Security attribute based access control |
| FDP_ACC.1.1/ MF_DF | The TSF shall enforce the access control MF_DF SFP[114] on<br>(1) the subjects logical channel bind to users<br>a. World,<br>b. Human User,<br>c. Device,<br>d. Human User and Device,<br>e. none[115],<br>(2) the objects<br>a. all executable code implemented by the TOE,<br>b. MF,<br>c. Application,<br>d. Dedicated File,<br>e. Application Dedicated File,<br>f. persistent stored public keys,<br>g. none[116],<br>(3) the operation by the following commands<br>a. command SELECT,<br>b. create objects with command LOAD APPLICATION with and without command chaining,<br>c. delete objects with command DELETE,<br>d. read fingerprint with command FINGERPRINT,<br>e. command LIST PUBLIC KEY,<br>f. retrieve a challenge from the card with GET_CHALLENGE, export data with the command GET DATA, import data with the command PUT DATA, retrieves information of objects on card with the command GET ATTRIBUTE, re-initialization of the card with command REINIT (only for Testcards, always blocked for operational cards)[117] [118]. |

*Application note 20*: Note that 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 smart card by command LOAD CODE or any other means (including related configuration data).

[114] [assignment: *access control SFP*]
[115] [assignment: *list of further subjects*]
[116] [assignment: *list of further objects*]
[117] [assignment: *all other operations applicable to MF and DF*]
[118] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1/ MF_DF)” as specified below.

| | |
|---|---|
| **FDP_ACF.1/ MF_DF** | Security attribute based access control |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACC.1 Subset access control<br>FMT_MSA.3 Static attribute initialisation |
| FDP_ACF.1.1/ MF_DF | The TSF shall enforce the access control MF_DF SFP[119] to objects based on the following<br>(1) the subjects *logical channel* with security attributes<br>a. *interface,*<br>b. *globalPasswordList,*<br>c. *globalSecurityList,*<br>d. *dfSpecificPasswordList,*<br>e. *dfSpecificSecurityList,*<br>f. *bitSecurityList,*<br>g. *SessionkeyContext,*<br>h. none[120],<br>(2) the objects<br>a. all executable code implemented by the TOE,<br>b. MF with security attributes *lifeCycleStatus, seIdentifier* and *interfaceDependentAccessRules,*<br>c. DF with security attributes *lifeCycleStatus, seIdentifier* and *interfaceDependentAccessRules,*<br>d. Application with security attributes *lifeCycleStatus, seIdentifier* and *interfaceDependentAccessRules,*<br>e. Application Dedicated File with security attributes *lifeCycleStatus, seIdentifier* and *interfaceDependentAccessRules,*<br>f. persistent stored public keys,<br>g. none[121] [122]. |

[119] [assignment: *access control SFP*]
[120] [assignment: *further subjects listed in FDP_ACC.1.1/MF_DF with their security attributes*]
[121] [assignment: *list of further objects listed in FDP_ACC.1.1/MF_DF with their security attributes*]

[122] [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*]

| | |
|---|---|
| FDP_ACF.1.2/ MF_DF | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:<br>(1) SELECT is ALWAYS allowed[123].<br>(2) GET CHALLENGE is ALWAYS allowed[124].<br>(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*.<br>(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*.<br>(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*.<br>(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*.<br>(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*.<br>(8) All subjects are allowed to execute command LIST PUBLIC KEY to export all persistent stored public keys. |

(9) A subject is allowed to execute command GET ATTRIBUTE if the security attributes interface, globalPasswordList, globalSecurityList and SessionkeyContext of the subject meet the access rules for the command GET ATTRIBUTE dependent on lifeCycleStatus, seIdentifier and interfaceDependentAccessRules.

(10) GET DATA is ALWAYS allowed; PUT DATA is ALWAYS allowed in preparation phases, but NEVER allowed in phase 7 (Operational Use).

(11) A subject is allowed to execute command REINIT if the security attributes interface, globalPasswordList, globalSecurityList and SessionkeyContext of the subject meet the access rules for the command REINIT dependent on lifeCycleStatus, seIdentifier and interfaceDependentAccessRules (REINIT is only available for Testcards, always blocked for operational cards)[125] [126].

| | |
|---|---|
| FDP_ACF.1.3/ MF_DF | The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[127]. |
| FDP_ACF.1.4/ MF_DF | 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[128]. |

*Application note 21:* 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 the command MANAGE SECURITY ENVIRONMENT. The command SELECT

[123] [selection: *ALWAYS allowed, [assignment: supported access control rules]*]

[124] [selection: *ALWAYS allowed, [assignment: supported access control rules]*]

[125] [assignment: *further list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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

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

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

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 that the command FINGERPRINT processes 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 author shall describe the TOE specific access control rules for these commands **(Access control rules for SELECT and FINGERPRINT described)**. The ST author shall perform the open operations whereby "none" is allowed **(all operations performed – added GET DATA and PUT DATA, see following application note)**.

The TOE shall meet the requirement "Subset access control (FDP_ACC.1/EF)" as specified below.

| | |
|---|---|
| **FDP_ACC.1/EF** | Subset access control |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACF.1 Security attribute based access control |
| FDP_ACC.1.1/EF | The TSF shall enforce the access control EF SFP[129] on<br>(1) the subjects *logical channel* bind to users<br>a. World,<br>b. Human User,<br>c. Device,<br>d. Human User and Device,<br>e. none[130],<br>(2) the objects<br>a. EF,<br>b. Transparent EF,<br>c. Structured EF,<br>d. none[131],<br>(3) the operation by the following commands<br>a. SELECT,<br>b. DELETE of the current file,<br>c. none[132] [133]. |

*Application note 22*: Note that 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 these commands is 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

[129] [assignment: *access control SFP*]
[130] [assignment: *list of further subjects*]
[131] [assignment: *list of further objects*]
[132] [assignment: *further operations*]
[133] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

corresponding FDP_ACC.1 and FDP_ACF.1 SFR **(CREATE and GET RESPONSE are not implemented. GET DATA and PUT DATA was added to FDP_ACC.1/MF_DF and FDP_ACF.1/MF_DF)**. 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.

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

| | |
|---|---|
| **FDP_ACF.1/EF** | Security attribute based access control |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACC.1 Subset access control<br>FMT_MSA.3 Static attribute initialisation |
| FDP_ACF.1.1/EF | The TSF shall enforce the access control EF SFP[134] to objects based on the following<br>(1) the subjects *logical channel* with security attributes<br>a. *interface,*<br>b. *globalPasswordList,*<br>c. *globalSecurityList,*<br>d. *dfSpecificPasswordList,*<br>e. *dfSpecificSecurityList,*<br>f. *bitSecurityList,*<br>g. *SessionkeyContext,*<br>h. none[135],<br>(2) the objects<br>a. EF with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules* of the EF, and transaction mode, checksum[136],<br>b. none[137] [138]. |

[134] [assignment: *access control SFP*]
[135] [assignment: *further subjects listed in FDP_ACC.1.1/EF*]
[136] [selection: *transaction mode, checksum*]
[137] [assignment: *list of further objects listed in FDP_ACC.1.1/EF with their security attributes*]
[138] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

| | |
|---|---|
| FDP_ACF.1.2/EF | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:<br>(1) SELECT is ALWAYS allowed[139].<br>(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.<br>(3) none[140] [141]. |
| FDP_ACF.1.3/EF | The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[142]. |
| FDP_ACF.1.4/EF | 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[143]. |

*Application note 23*: 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 mode" (*flagTransactionMode*) and "checksum" (*flagChecksum*) may be empty because they are optional in the COS specification [21] **(transaction mode and checksum selected)**.

[139] [selection: *ALWAYS allowed, [assignment: supported access control rules]*]
[140] [assignment: *further list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[141] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[142] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[143] [assignment*: rules, based on security attributes, that explicitly deny access of subjects to objects*]

The TOE shall meet the requirement "Subset access control (FDP_ACC.1/TEF)" as specified below.

| | |
|---|---|
| **FDP_ACC.1/TEF** | Subset access control |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACF.1 Security attribute based access control |
| FDP_ACC.1.1/TEF | The TSF shall enforce the access rule TEF SFP[144] on<br>(1) the subjects *logical channel* bind to users<br>a. World,<br>b. Human User,<br>c. Device,<br>d. Human User and Device,<br>e. none[145],<br>(2) the objects<br>a. Transparent EF,<br>b. none[146],<br>(3) the operation by the following commands<br>a. ERASE BINARY,<br>b. READ BINARY,<br>c. SET LOGICAL EOF,<br>d. UPDATE BINARY,<br>e. WRITE BINARY,<br>f. none[147] [148]. |

[144] [assignment: *access control SFP*]
[145] [assignment: *further subjects*]
[146] [assignment: *list of further objects*]
[147] [assignment: *further operation*]
[148] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1/TEF)” as specified below.

| | |
|---|---|
| **FDP_ACF.1/TEF** | Security attribute based access control |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACC.1 Subset access control<br>FMT_MSA.3 Static attribute initialisation |
| FDP_ACF.1.1/TEF | The TSF shall enforce the access rule TEF SFP[149] to objects based on the following<br>(1) the subjects *logical channel* with security attributes<br>a. *interface,*<br>b. *globalPasswordList,*<br>c. *globalSecurityList,*<br>d. *dfSpecificPasswordList,*<br>e. *dfSpecificSecurityList,*<br>f. *bitSecurityList,*<br>g. *SessionkeyContext,*<br>h. none[150],<br>(2) the objects<br>a. with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules* of the current Transparent EF, and transaction mode **and** checksum[151],<br>b. none[152] [153]. |
| FDP_ACF.1.2/TEF | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:<br>(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, globalPasswordList, globalSecurityList, 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.<br>(2) none[154] [155]. |
| FDP_ACF.1.3/TEF | The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[156]. |

| | |
|---|---|
| FDP_ACF.1.4/TEF | 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[157] [158]. |

*Application note 24*: The selection of "transaction mode" (*flagTransactionMode*) and "checksum" (*flagChecksum*) may be empty because they are optional in the COS specification [21] **(transaction 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.

[149] [assignment: *access control SFP*]
[150] [assignment: *further subjects listed in FDP_ACC.1.1/TEF*]
[151] [selection: *transaction mode, checksum*]
[152] [assignment: *list of further objects listed in FDP_ACC.1.1/TEF*]
[153] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[154] [assignment: *further list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[155] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[156] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[157] [assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*]
[158] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

The TOE shall meet the requirement "Subset access control (FDP_ACC.1/SEF)" as specified below.

| | |
|---|---|
| **FDP_ACC.1/SEF** | Subset access control |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACF.1 Security attribute based access control |
| FDP_ACC.1.1/ SEF | The TSF shall enforce the access rule SEF SFP[159] on<br>(1) the subjects *logical channel* bind to users<br>a. World,<br>b. Human User<br>c. Device<br>d. Human User and Device,<br>e. none[160],<br>(2) the objects<br>a. record in Structured EF<br>b. none[161],<br>(3) the operation by the following commands<br>a. APPEND RECORD,<br>b. ERASE RECORD,<br>c. DELETE RECORD,<br>d. READ RECORD,<br>e. SEARCH RECORD,<br>f. UPDATE RECORD,<br>g. none[162] [163]. |

[159] [assignment: *access control SFP*]
[160] [assignment: *further subjects*]
[161] [assignment: *list of further objects*]
[162] [assignment: *further operation*]
[163] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

*Application note 25*: The command WRITE RECORD is optional. If implemented by the TOE this command shall be added to the corresponding FDP_ACC.1/SEF and FDP_ACF.1/SEF SFR.

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1/SEF)” as specified below.

| | |
|---|---|
| **FDP_ACF.1/SEF** | Security attribute based access control |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACC.1 Subset access control<br>FMT_MSA.3 Static attribute initialisation |
| FDP_ACF.1.1/SEF | The TSF shall enforce the access rule SEF SFP[164] to objects based on the following<br>(1) the subjects *logical channel* with security attributes<br>a. *interface,*<br>b. *globalPasswordList,*<br>c. *globalSecurityList,*<br>d. *dfSpecificPasswordList,*<br>e. *dfSpecificSecurityList,*<br>f. *bitSecurityList,*<br>g. *SessionkeyContext,*<br>h. none[165],<br>(2) the objects<br>a. with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules* of the current Structured EF, and *lifeCycleStatus* of the record,<br>b. none[166] [167]. |
| FDP_ACF.1.2/SEF | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:<br>(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, globalPasswordList, globalSecurityList, 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.<br>(2) none[168] [169]. |
| FDP_ACF.1.3/SEF | The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[170]. |

| | |
|---|---|
| FDP_ACF.1.4/SEF | 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[171] [172]. |

*Application note 26*: 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)**.

*Application note 27*: 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.

---

[164] [assignment: *access control SFP*]
[165] [assignment: *further subjects listed in FDP_ACC.1.1/SEF*]
[166] [assignment: *list of further objects listed in FDP_ACC.1.1/SEF*]
[167] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[168] [assignment: *further list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[169] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[170] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[171] [assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*]
[172] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

The TOE shall meet the requirement "Subset access control (FDP_ACC.1/KEY)" as specified below.

| | |
|---|---|
| **FDP_ACC.1/KEY** | Subset access control |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACF.1 Security attribute based access control |
| FDP_ACC.1.1/KEY | The TSF shall enforce the access control key SFP[173] on |

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

(1) the subjects *logical channel* bind to users
   a. World,
   b. Human User
   c. Device
   d. Human User and Device,
   e. none[174],
(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[175],
(3) the operation by the following commands
   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,
   h. PSO DECIPHER,
   i. PSO TRANSCIPHER,
   j. ~~PSO COMPUTE CRYPTOGRAPHIC CHECKSUM if supported by the TOE,~~
   k. ~~PSO VERIFY CRYPTOGRAPHIC CHECKSUM if supported by the TOE,~~[176]
   l. none[177] [178].

[174] [assignment: *further subjects*]
[175] [assignment: *list of further objects*]
[176] Not supported because Package Crypto Box is not supported by the TOE
[177] [assignment: *further operation*]

[178] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1/KEY)” as specified below.

| | |
|---|---|
| **FDP_ACF.1/KEY** | Security attribute based access control |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACC.1 Subset access control<br>FMT_MSA.3 Static attribute initialisation |
| FDP_ACF.1.1/KEY | The TSF shall enforce the access control key SFP[179] to objects based on the following<br>(1) the subjects *logical channel* with security attributes<br>a. *interface,*<br>b. *globalPasswordList,*<br>c. *globalSecurityList,*<br>d. *dfSpecificPasswordList,*<br>e. *dfSpecificSecurityList,*<br>f. *bitSecurityList,*<br>g. *SessionkeyContext,*<br>h. none[180],<br>(2) the objects<br>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,<br>b. private asymmetric key used for user data with security attributes *seIdentifier* of the current folder, *lifeCycleStatus*, *keyAvailable* and *interfaceDependentAccessRules,*<br>c. public asymmetric key for signature verification used for user data with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules,*<br>d. public asymmetric key for encryption used for user data with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules,*<br>e. CVC with security attributes *certificate content* and *signature,*<br>f. ephemeral keys used during Diffie-Hellman key exchange,<br>g. none[181] [182]. |

[179] [assignment: *access control SFP*]
[180] [assignment: *further subjects listed in FDP_ACC.1.1/KEY*]
[181] [assignment: *list of further objects listed in FDP_ACC.1.1/KEY*]
[182] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

FDP_ACF.1.2/KEY 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[183] 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

[183] [selection: *ALWAYS allowed, [assignment: supported access control rules]*]

*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 to 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 to 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 to 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 then 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 then 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[184] [185].

FDP_ACF.1.3/KEY The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[186].

FDP_ACF.1.4/KEY 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[187].

[184] [assignment: *further list of subjects, objects, and operations among subjects and objects covered by the SFP*]

[185] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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

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

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

| | |
|---|---|
| **FMT_SMF.1** | Specification of Management Functions |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FMT_SMF.1.1 | The TSF shall be capable of performing the following management functions:<br>(1) Initialisation,<br>(2) Personalisation,<br>(3) Life Cycle Management by means of the commands GENERATE ASYMMETRIC KEY PAIR, DELETE, LOAD APPLICATION, TERMINATE, TERMINATE DF, TERMINATE CARD USAGE, none[188],<br>(4) Management of access control security attributes by means of the commands ACTIVATE, DEACTIVATE, ACTIVATE RECORD, DEACTIVATE RECORD, ENABLE VERIFICATION REQUIREMENT, DISABLE VERIFICATION REQUIREMENT, LOAD APPLICATION,<br>(5) Management of password objects attributes by means of the commands CHANGE REFERENCE DATA, RESET RETRY COUNTER, GET PIN STATUS, VERIFY, LOAD APPLICATION,<br>(6) Management of device authentication reference data by means of the commands PSO VERIFY CERTIFICATE, GET SECURITY STATUS KEY, LOAD APPLICATION,<br>(7) Initialization by means of command LOAD APPLICATION, Personalization by means of command LOAD APPLICATION, import of CPLC data by PUT DATA, activation/deactivation of contactless interface by PUT DATA, re-initialization by means of command REINIT (only for Testcards, always blocked for operational cards)[189] [190]. |

[188] [assignment: *list of further management functions to be provided by the TSF*]
[189] [assignment: *list of further management functions to be provided by the TSF*]
[190] [assignment: *list of management functions to be provided by the TSF*]

*Application note 28*: The Protection Profile BSI-CC-PP-0084-2014 [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.**

*Application note 29*: 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 author 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.**

The TOE shall meet the requirement "Management of security attributes (FMT_MSA.1/Life)" as specified below.

| | |
|---|---|
| **FMT_MSA.1/Life** | Management of security attributes |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |
| FMT_MSA.1.1/Life | 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[191] to restrict the ability to |

[191] [assignment: *access control SFP(s), information flow control SFP(s)*]

(1) create[192] **all** ~~the~~ security attributes of the new object DF, Application, Application Dedicated File, EF, TEF and SEF[193] to subjects allowed to execute the command LOAD APPLICATION for the MF, DF, Application, Application Dedicated File where the new object is created[194],

(2) **change[195] the security attributes of the object MF, DF, Application, Application Dedicated File, EF, TEF and SEF[196] by means of the command LOAD APPLICATION to none[197] [198],**

(3) **change[199] the security attributes *lifeCycleStatus* to *„Operational state (active)"*[200] to subjects allowed to execute the command ACTIVATE for the selected object[201],**

(4) **change[202] the security attributes *lifeCycleStatus* to *„Operational state (deactivated)"*[203] to subjects allowed to execute the command DEACTIVATE for the selected object[204],**

(5) **change[205] the security attributes *lifeCycleStatus* to *„Termination state"*[206] to subjects allowed to execute the command TERMINATE for the selected EF, the key object or the password object[207],**

(6) **change[208] the security attributes *lifeCycleStatus* to *„Termination state"*[209] to subjects allowed to execute the command TERMINATE DF for the selected DF, Application or Application Dedicated File[210],**

(7) **change[211] the security attributes *lifeCycleStatus* to *„Termination state"*[212] to subjects allowed to execute the command TERMINATE CARD USAGE[213],**

(8) **query[214] the security attributes *lifeCycleStatus* by means of the command SELECT[215] to ALWAYS allowed[216] [217],**

(9) **delete[218] all security attributes of the selected object[219] to subjects allowed to execute the command DELETE for the selected object[220] to none[221],**

(10) **change[222] the security attributes *lifeCycleStatus* to *„preparative state"*[223] to subjects allowed to execute the command REINIT (only for Testcards, not available for operational cards)[224].**

**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.**

[192] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[193] [assignment: *list of security attributes*]
[194] [assignment: *the authorised identified roles*]
[195] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[196] [assignment: *list of security attributes*]
[197] [selection: *none, subjects allowed to execute the command LOAD APPLICATION for the MF, DF, Application, Application Dedicated File where the object is updated*]
[198] [assignment: *the authorised identified roles*]
[199] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[200] [assignment: *list of security attributes*]
[201] [assignment: *the authorised identified roles*]
[202] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[203] [assignment: *list of security attributes*]
[204] [assignment: *the authorised identified roles*]
[205] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[206] [assignment: *list of security attributes*]
[207] [assignment: *the authorised identified roles*]
[208] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[209] [assignment: *list of security attributes*]
[210] [assignment: *the authorised identified roles*]
[211] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[212] [assignment: *list of security attributes*]
[213] [assignment: *the authorised identified roles*]
[214] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[215] [assignment: *list of security attributes*]
[216] [selection: *ALWAYS allowed, [assignment: supported access control rules]*]
[217] [assignment: *the authorised identified roles*]
[218] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[219] [assignment: *list of security attributes*]
[220] [assignment: *the authorised identified roles*]
[221] [assignment: *list of further security attributes with the authorised identified roles*]
[222] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[223] [assignment: *list of security attributes*]
[224] [assignment: *the authorised identified roles*]

*Application note 30*: 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 author 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. **The selection performed taking into account the consequences of LOAD APPLICATION.**

The TOE shall meet the requirement "Management of security attributes (FMT_MSA.1/SEF)" as specified below.

| | |
|---|---|
| **FMT_MSA.1/SEF** | Management of security attributes |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |
| FMT_MSA.1.1/SEF | The TSF shall enforce the access rule SEF SFP[225] to restrict the ability to<br>(1) change[226] the security attributes *lifeCycleStatus* of the selected record to „*Operational state (active)*"[227] to subjects allowed to execute the command ACTIVATE RECORD[228],<br>(2) **change[229] the security attributes *lifeCycleStatus* of the selected record to „*Operational state (deactivated)*"[230] to subjects allowed to execute the command DEACTIVATE RECORD[231],**<br>(3) **delete[232] all security attributes of the selected record[233] to subjects allowed to execute the command DELETE RECORD[234],**<br>(4) **none[235]**.<br>**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.** |

[225] [assignment: *access control SFP(s), information flow control SFP(s)*]
[226] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[227] [assignment: *list of security attributes*]
[228] [assignment: *the authorised identified roles*]
[229] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[230] [assignment: *list of security attributes*]
[231] [assignment: *the authorised identified roles*]

*Application note 31*: 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.

The TOE shall meet the requirement "Static attribute initialisation (FMT_MSA.3)" as specified below.

[232] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[233] [assignment: *list of security attributes*]
[234] [assignment: *the authorised identified roles*]
[235] [assignment: *list of further security attributes with the authorised identified roles*]

| | |
|---|---|
| **FMT_MSA.3** | Static attribute initialisation |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_MSA.1 Management of security attributes<br>FMT_SMR.1 Security roles |
| FMT_MSA.3.1 | 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[236] to provide restrictive[237] default values for security attributes that are used to enforce the SFP.<br>**After reset the security attributes of the subject are set as follows:**<br>**(1) *currentFolder* is *root*,**<br>**(2) *keyReferenceList, globalSecurityList, globalPasswordList, dfSpecificSecurityList, dfSpecificPasswordList* and *bitSecurityList* are empty,**<br>**(3) *SessionkeyContext.flagSessionEnabled* is set to *noSK*,**<br>**(4) *seIdentifier* is #1,**<br>**(5) *currentFile* is undefined.** |
| FMT_MSA.3.2 | The TSF shall allow the subjects allowed to execute the command LOAD APPLICATION[238] to specify alternative initial values to override the default values when an object or information is created. |

*Application note 32*: The refinements provide rules for setting restrictive security attributes after reset.

[236] [assignment: *access control SFP, information flow control SFP*]
[237] [selection, *choose one of: restrictive, permissive, [assignment: other property]*]
[238] [assignment: *the authorised identified roles*]

The TOE shall meet the requirement "Management of TSF data - PIN (FMT_MTD.1/PIN)" as specified below.

| | |
|---|---|
| **FMT_MTD.1/PIN** | Management of TSF data – PIN |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |
| FMT_MTD.1.1/PIN | The TSF shall restrict the ability to<br>(1) set new *secret* of the password objects by means of the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[239] [240] to subjects successfully authenticated with the old *secret* of this password object[241],<br>(2) **set new *secret* and change *transportStatus* to *regularPassword* of the password objects with *transportStatus* equal to Leer-PIN[242] [243] to subjects allowed to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01)[244],**<br>(3) **set new *secret* of the password objects by means of the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,00)[245] [246] to subjects successfully authenticated with the PUC of this password object[247],**<br>(4) **set new *secret* of the password objects by means of the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02)[248] [249] to subjects allowed to execute the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02)[250].** |

[239] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[240] [assignment: *other operations*]
[241] [assignment: *the authorised identified roles*]
[242] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[243] [assignment: *other operations*]
[244] [assignment: *the authorised identified roles*]
[245] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

*Application note 33*: 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)**.

[246] [assignment: *other operations*]
[247] [assignment: *the authorised identified roles*]
[248] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[249] [assignment: *other operations*]
[250] [assignment: *the authorised identified roles*]

The TOE shall meet the requirement “Management of security attributes - PIN (FMT_MSA.1/PIN)” as specified below.

| | |
|---|---|
| **FMT_MSA.1/PIN** | Management of security attributes – PIN |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |

FMT_MSA.1.1/PIN 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[251] to restrict the ability to

(1) reset by means of the command VERIFY[252] [253] the security attributes retry counter of password objects[254] to subjects successfully authenticated with the secret of this password object[255],

(2) **reset by means of the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[256] [257] the security attributes retry counter of password objects[258] to subjects successfully authenticated with the old secret of this password object[259],**

(3) **change by means of the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[260] [261] the security attributes *transportStatus* from Transport-PIN to regularPassword[262] to subjects allowed to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[263],**

(4) **change by means of the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01)[264] [265] the security attributes transportStatus from Leer-PIN to regularPassword[266] to subjects allowed to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01)[267],**

(5) **reset by means of the command DISABLE VERIFICATION REQUIREMENT with (CLA,INS,P1)=(00,26,00)[268] [269] the security attributes retry counter of password objects[270] to subjects successfully authenticated with the old secret of this password object[271],**

(6) **reset by means of the command ENABLE VERIFICATION REQUIREMENT with (CLA,INS,P1)=(00,28,00)[272] [273] the security attributes retry counter of password objects[274] to subjects successfully authenticated with the old secret of this password object[275],**

(7) **reset by means of the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,00) or (CLA,INS,P1)=(00,2C,01)[276] [277] the security attributes retry counter of password objects[278] to**

[251] [assignment: *access control SFP(s), information flow control SFP(s)*]
[252] [assignment: *other operations*]
[253] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[254] [assignment: *list of security attributes*]
[255] [assignment: *the authorised identified roles*]
[256] [assignment: *other operations*]
[257] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[258] [assignment: *list of security attributes*]
[259] [assignment: *the authorised identified roles*]
[260] [assignment: *other operations*]
[261] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[262] [assignment: *list of security attributes*]
[263] [assignment: *the authorised identified roles*]
[264] [assignment: *other operations*]
[265] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[266] [assignment: *list of security attributes*]
[267] [assignment: *the authorised identified roles*]
[268] [assignment: *other operations*]
[269] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[270] [assignment: *list of security attributes*]
[271] [assignment: *the authorised identified roles*]
[272] [assignment: *other operations*]
[273] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[274] [assignment: *list of security attributes*]
[275] [assignment: *the authorised identified roles*]
[276] [assignment: *other operations*]
[277] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[278] [assignment: *list of security attributes*]

**subjects successfully authenticated with the PUC of this password object**[279]**,**

(8) **reset by means of the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or (CLA,INS,P1)=(00,2C,03)**[280] [281] **the security attributes retry counter of password objects**[282] **to subjects allowed to execute the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or (CLA,INS,P1)=(00,2C,03)**[283]**,**

(9) **query by means of the command GET PIN STATUS**[284] [285] **the security attributes *flagEnabled, retry counter, transportStatus***[286] **to World**[287]**,**

(10) **enable**[288] **the security attributes *flagEnabled* requiring authentication with the selected password**[289] **to subjects authenticated with password and allowed to execute the command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00'28,00)**[290]**,**

(11) **enable**[291] **the security attributes *flagEnabled* requiring authentication with the selected password**[292] **to subjects allowed to execute the command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,28,01)**[293]**,**

(12) **disable**[294] **the security attributes *flagEnabled* requiring authentication with the selected password**[295] **to subjects authenticated with password and allowed to execute the command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,00)**[296]**,**

(13) **disable**[297] **the security attributes *flagEnabled* requiring authentication with the selected password**[298] **to subjects allowed to execute the command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,01)**[299]**.**

*Application note 34*: 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)**.

---

279 [assignment: *the authorised identified roles*]
280 [assignment: *other operations*]
281 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
282 [assignment: *list of security attributes*]
283 [assignment: *the authorised identified roles*]
284 [assignment: *other operations*]
285 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
286 [assignment: *list of security attributes*]
287 [assignment: *the authorised identified roles*]
288 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
289 [assignment: *list of security attributes*]
290 [assignment: *the authorised identified roles*]
291 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
292 [assignment: *list of security attributes*]
293 [assignment: *the authorised identified roles*]
294 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
295 [assignment: *list of security attributes*]
296 [assignment: *the authorised identified roles*]
297 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
298 [assignment: *list of security attributes*]
299 [assignment: *the authorised identified roles*]

The TOE shall meet the requirement "Management of TSF data – Authentication data (FMT_MTD.1/Auth)" as specified below.

| | |
|---|---|
| **FMT_MTD.1/Auth** | Management of TSF data – Authentication data |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |
| FMT_MTD.1.1/Auth | The TSF shall restrict the ability to<br>(1) import by means of the command LOAD APPLICATION[300] the root public keys[301] to roles authorised to execute this command[302],<br>(2) **import by means of the command PSO VERIFY CERTIFICATE[303] the root public keys[304] to roles authorised to execute this command[305],**<br>(3) **import by means of the command PSO VERIFY CERTIFICATE[306] the certificates as device authentication reference data[307] to roles authorised to execute this command[308],**<br>(4) **select by means of the command MANAGE SECURITY ENVIRONMENT[309] the device authentication reference data[310] to World[311] [312].**<br>**The subject *logical channel* is allowed to execute a command if the security attributes *interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList, dfSpecificSecurityList* and *bitSecurityList SessionkeyContext* of the subject meet the security attributes *lifeCycleStatus, seIdentifier* and *interfaceDependentAccessRules* of the affected object.** |

*Application note 35*: 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

[300] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[301] [assignment: *list of TSF data*]
[302] [assignment: *the authorised identified roles*]
[303] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[304] [assignment: *list of TSF data*]
[305] [assignment: *the authorised identified roles*]

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.

The TOE shall meet the requirement "Management of security attributes (FMT_MSA.1/Auth)" as specified below.

| | |
|---|---|
| **FMT_MSA.1/Auth** | Management of security attributes |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |
| FMT_MSA.1.1/ Auth | The TSF shall enforce the access control key SFP[313] to restrict the ability to query[314] [315] the security attributes access control rights set for the key[316] to meet the access rules of command GET SECURITY STATUS KEY of the object dependent on *lifeCycleStatus, seIdentifier* and *interfaceDependentAccessRules*[317]. |

The TOE shall meet the requirement "Management of TSF data – No export (FMT_MTD.1/NE)" as specified below.

[306] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[307] [assignment: *list of TSF data*]
[308] [assignment: *the authorised identified roles*]
[309] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[310] [assignment: *list of TSF data*]
[311] [selection: *World, roles authorised to execute this command*]
[312] [assignment: *the authorised identified roles*]
[313] [assignment: *access control SFP(s), information flow control SFP(s)*]
[314] [assignment: *other operations*]
[315] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[316] [assignment: *list of security attributes*]
[317] [assignment: *the authorised identified roles*]

| | |
|---|---|
| **FMT_MTD.1/NE** | Management of TSF data – No export |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |
| FMT_MTD.1.1/NE | The TSF shall restrict the ability to<br>(1) export TSF data according to FPT_ITE.2[318] the<br>a. public authentication reference data,<br>b. security attributes for objects of the object system<br>to<br>a. in case of public authentication reference data: all security attributes without restrictions,<br>b. in case of security attributes for objects of the object system: the security attributes interface, globalPasswordList, globalSecurityList and SessionkeyContext of the subject that meet the access rules for the command GET ATTRIBUTE dependent on lifeCycleStatus, seIdentifier and interfaceDependentAccessRules[319] [320],<br>(2) **export TSF data according to FPT_ITE.2[321] the none[322] [323] [324] to none[325] [326],**<br>(3) **export[327] the following TSF data**<br>**a. Password,**<br>**b. Multi-Reference password,**<br>**c. PUC,**<br>**d. Private keys,**<br>**e. Session keys,**<br>**f. Symmetric authentication keys,**<br>**g. Private authentication keys,**<br>**h. no further TSF data[328],**<br>**and the following user data**<br>**a. Private keys of the user,**<br>**b. Symmetric keys of the user,**<br>**c. no further user data[329] [330]**<br>**to nobody[331].** |

[318] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[319] [assignment: *list of security attributes of subjects*]
[320] [assignment: *the authorised identified roles*]
[321] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[322] [assignment: *list of all TOE specific security attributes not described in COS specification [21]*]
[323] [assignment: *list of TSF data*]
[324] [assignment: *other operations*]
[325] [assignment: *list of security attributes of subjects*]
[326] [assignment: *the authorised identified roles*]
[327] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[328] [assignment: *list of types of TSF data*]
[329] [assignment: *list of types of user data*]
[330] [assignment: *list of TSF data*]
[331] [assignment: *the authorised identified roles*]

### 6.1.7 Cryptographic Functions

The TOE provides cryptographic services based on elliptic curve cryptography (ECC) using the following curves referred 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 [39],

(2) length 384

(a) brainpoolP384r1 defined in RFC5639 [41],

(b) ansix9p384r1 defined in ANSI X.9.62 [39],

(3) length 512 bit

(a) brainpoolP512r1 defined in RFC5639 [41].

The Authentication Protocols produce agreed parameters to generate the message authentication key and – if secure messaging with encryption is required - the encryption key for secure messaging. Key agreement for rsaSessionkey4SM uses RSA only with 2048 bit modulus length.

The COS specification [21] requires to implement random number generation (RNG) for

- the command GET CHALLENGE,
- the authentication protocols as required by FIA_UAU.4,
- the key agreement for secure messaging,
- the key generation (static and ephemeral keys) within the TOE,
- the command GET RANDOM

according to TR-03116-1 [19] section 3.8 and 3.9.

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

| | |
|---|---|
| **FCS_RNG.1** | Random number generation |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FCS_RNG.1.1 | The TSF shall provide a hybrid physical[332] [333] random number generator **of RNG class PTG.3[334] ([5], [6])** that implements:<br>(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.<br>(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.<br>(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.<br>(PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.<br>(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.<br>(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.[335]. |
| FCS_RNG.1.2 | The TSF shall provide random numbers that meet<br>(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.<br>(PTG.3.8) The internal random numbers shall use PTRNG of class PTG.2 as random source for the post-processing.[336] [337]. |

Application note 36: This SFR requires the TOE to generate random numbers used for key generation (static and ephemeral keys) within the TOE according to TR-03116-1 [19] section 3.9, requiring RNG classes identified in the selection in element FCS_RNG.1.1 and recommending RNG of class PTG.3 **(PTG.3 chosen)**. Furthermore, this SFR addresses the random number generation for the command GET CHALLENGE and for use within the framework of authentication protocols and key agreement for secure messaging. For the command GET RANDOM a separate specific SFR is set up, please refer to the following SFR FCS_RNG.1/GR.

The selection in the element FCS_RNG.1.1 includes RNG of classes DRG.3 and DRG.4 **(n/a, PTG.3 chosen)**. Note that the RNG of class DRG.4 are hybrid deterministic and of class PTG.3 are hybrid physical (which are addressed in BSI-CC-PP-0084-2014 [11], but not in BSI-CC-PP-0035-2007 [46]). The quality metric assigned in element FCS_RNG.1.2 shall be chosen to resist attacks with high attack potential **(metric chosen accordingly)**.

The TOE shall meet the requirement "Random number generation – Get random command (FCS_RNG.1/GR)" as specified below.

[332] [selection: *deterministic, hybrid deterministic, physical, hybrid physical*]
[333] [selection: *physical, non-physical true, deterministic, hy*brid]
[334] [selection: *DRG.3, DRG.4, PTG.2, PTG.3*]
[335] [assignment: *list of security capabilities of the selected RNG class*]
[336] [assignment: *a defined quality metric of the selected RNG class*]
[337] [assignment: *a defined quality metric*]

| | |
|---|---|
| **FCS_RNG.1/GR** | Random number generation – Get random command |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FCS_RNG.1.1/GR | The TSF shall provide a **hybrid** physical[338] random number generator of **RNG class PTG.3[339] ([6]) for GET RANDOM** that implements:<br>(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.<br>(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.<br>(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.<br>(PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.<br>(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.<br>(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.[340]. |
| FCS_RNG.1.2/GR | The TSF shall provide random ~~numbers~~ numbers[341] that meet<br>(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.<br>(PTG.3.8) The internal random numbers shall use PTRNG of class PTG.2 as random source for the post-processing.[342]. |

*Application note 37*: This SFR addresses the generation of random numbers for external entities by using the command GET RANDOM. If the TOE provides random numbers by means of the command GET RANDOM that will be used for key generation of external devices as the connector (i.e. usage as gSMC-K) or the eHealth Card Terminals (i.e. usage as gSMC-KT) or that will be used to seed another deterministic RNG of the

external device the TOE shall implement RNG of class PTG.2 or PTG.3 for such purpose. Please note that this SFR exceeds the requirements concerning the RNG class in [21] section 14.9.5 (refer to (N099.356)b).

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

| | |
|---|---|
| **FCS_COP.1/SHA** | Cryptographic operation – SH |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/SHA | The TSF shall perform hashing[343] in accordance with a specified cryptographic algorithm<br>(1) SHA-1,<br>(2) SHA-256,<br>(3) SHA-384,<br>(4) SHA-512[344]<br>and cryptographic key sizes none[345] that meet the following: TR-03116-1 [19], FIPS 180-4 [37][346]. |

[338] [selection: *physical, non-physical true, deterministic, hybrid*]
[339] [selection: *PTG.2, PTG.3*]
[340] [assignment: *list of security capabilities of the selected RNG class*]
[341] [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*]
[342] [assignment: *a defined quality metric of the selected RNG class*]
[343] [assignment: *list of cryptographic operations*]
[344] [assignment: *cryptographic algorithm*]
[345] [assignment: *cryptographic key sizes*]
[346] [assignment: *list of standards*]

The TOE shall meet the requirement "Cryptographic operation – COS for AES (FCS_COP.1/COS.AES)" as specified below.

| | |
|---|---|
| **FCS_COP.1/ COS.AES** | Cryptographic operation – COS for AES |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/ COS.AES | The TSF shall perform<br>(1) encryption and decryption with card internal key for command MUTUAL AUTHENTICATE[347],<br>(2) decryption with card internal key for command GENERAL AUTHENTICATE,<br>(3) encryption and decryption for secure messaging[348]<br>in accordance with a specified cryptographic algorithm AES in CBC mode[349] and cryptographic key sizes 128 bit, 192 bit, 256 bit[350] that meet the following: TR-03116-1 [19], COS specification [21], FIPS 197 [33][351]. |

The TOE shall meet the requirement "Cryptographic key generation – COS for SM keys (FCS_CKM.1/AES.SM)" as specified below.

[347] For the OS PrePersonaliser a card specific OS PrePersonaliser Authentication Key with cryptographic key size 256 bit has been derived using an IDEMIA proprietary Key Derivation mechanism

[348] [assignment: *list of cryptographic operations*]

[349] [assignment: *cryptographic algorithm*]

[350] [assignment: *cryptographic key sizes*]

[351] [assignment: *list of standards*]

| | |
|---|---|
| **FCS_CKM.1/ AES.SM** | Cryptographic key generation – COS for SM keys |
| Hierarchical to: | No other components. |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.1.1/ AES.SM | The TSF shall generate session cryptographic keys in accordance with a specified cryptographic key generation algorithm Key Derivation for AES as specified in sec. 4.3.3.2 in [17][352] and specified cryptographic key sizes 128 bit, 192 bit and 256 bit[353] that meet the following: TR-03111 [17], COS specification [21], FIPS 197 [33][354]. |

*Application note 38*: The Key Generation FCS_CKM.1/AES.SM is done during MUTUAL AUTHENTICATE and GENERAL AUTHENTICATE with establishment of secure messaging (with Package Crypto Box also for trusted channel during commands EXTERNAL AUTHENTICATE and INTERNAL AUTHENTICATE).

[352] [assignment: *cryptographic key generation algor*ithm]
[353] [assignment: *cryptographic key sizes*]
[354] [assignment: *list of standards*]

The TOE shall meet the requirement "Cryptographic operation – COS for CMAC (FCS_COP.1/COS.CMAC)" as specified below.

| | |
|---|---|
| **FCS_COP.1/ COS.CMAC** | Cryptographic operation – COS for CMAC |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/ COS.CMAC | The TSF shall perform<br>(1) computation and verification of cryptographic checksum for command MUTUAL AUTHENTICATE,<br>(2) verification of cryptographic checksum for command GENERAL AUTHENTICATE,<br>(3) computation and verification of cryptographic checksum for secure messaging[355]<br>in accordance with a specified cryptographic algorithm AES CMAC[356] and cryptographic key sizes 128 bit, 192 bit and 256 bit[357] that meet the following: TR-03116-1 [19], COS specification [21], FIPS 197 [33], NIST SP 800-38B [36][358]. |

[355] [assignment: *list of cryptographic operations*]
[356] [assignment: *cryptographic algorithm*]
[357] [assignment: *cryptographic key sizes*]
[358] [assignment: *list of standards*]

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

| | |
|---|---|
| **FCS_CKM.1/ELC** | Cryptographic key generation – ECC key generation |
| Hierarchical to: | No other components. |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution, or<br>FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.1.1/ELC | The TSF shall generate cryptographic **ELC** keys in accordance with a specified cryptographic key generation algorithm ECC Key Generation[359] with COS standard curves[360] and specified cryptographic key sizes 256 bit, 384 bit and 512 bit[361] that meet the following: ANSI X9.62 [39], chapter A4.3, ISO/IEC 14888-3 [200], chapter 6.4.2, IEEE 1363 [201], chapter A.16.9, TR-03111 [17], chapter 4.1.3, COS specification [21][362]. |

*Application note 39:* The COS specification [21] requires the TOE to support elliptic curves listed in COS specification [21], section 6.5 (refered as COS standard curves in this PP) and to implement the command GENERATE ASYMMETRIC KEY PAIR for the generation of ELC key pairs. 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 author shall perform the missing operation in the element FCS_CKM.1/ELC according to the implemented key generation algorithm.

[359] [assignment: *cryptographic key generation algorithm*]
[360] [assignment: *cryptographic key generation algor*ithm]
[361] [assignment: *cryptographic key sizes*]
[362] [assignment: *list of standards*], refinement to "TR-03111 [17], COS specification [21]" which is the given assignment in the Protection Profile [BSI_PP_EHC_G2]

The TOE shall meet the requirement "Cryptographic operation – RSA signature-creation (FCS_COP.1/COS.RSA.S)" as specified below.

| | |
|---|---|
| **FCS_COP.1/COS.RSA.S** | Cryptographic operation – RSA signature-creation |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/ COS.RSA.S | The TSF shall perform digital signature generation for commands<br>(1) PSO COMPUTE DIGITAL SIGNATURE,<br>(2) INTERNAL AUTHENTICATE[363]<br>in accordance with a specified cryptographic algorithm<br>(1) RSASSA-PSS-SIGN with SHA-256,<br>(2) RSA SSA PKCS1-V1_5,<br>(3) RSA ISO9796-2 DS2 with SHA-256 (for PSO COMPUTE DIGITAL SIGNATURE only)[364],<br>and cryptographic key sizes 2048 bit and 3072 bit modulus length[365] that meet the following: TR-03116-1 [19], COS specification [21], [31], [34][366]. |

[363] [assignment: *list of cryptographic operations*]
[364] [assignment: *cryptographic algorithm*]
[365] [assignment: *cryptographic key sizes*]
[366] [assignment: *list of standards*]

The TOE shall meet the requirement "Cryptographic operation – ECDSA signature verification (FCS_COP.1/COS.ECDSA.V)" as specified below.

| | |
|---|---|
| **FCS_COP.1/COS.ECDSA.V** | Cryptographic operation – ECDSA signature verification |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/ COS.ECDSA.V | The TSF shall perform digital signature verification for commands<br>(1) PSO VERIFY CERTIFICATE,<br>(2) PSO VERIFY DIGITAL SIGNATURE,<br>(3) EXTERNAL AUTHENTICATE,<br>(4) **LOAD APPLICATION**[367]<br>in accordance with a specified cryptographic algorithm ECDSA with COS standard curves using<br>(1) SHA-256,<br>(2) SHA-384,<br>(3) SHA-512[368]<br>and cryptographic key sizes 256 bits, 384 bits, 512 bits[369] that meet the following: TR-03111 [17], TR-03116-1 [19], COS specification [21], [39][370]. |

*Application note 40*: The command PSO VERIFY CERTIFICATE may store the imported public keys for 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.

[367] [assignment: *list of cryptographic operations*]
[368] [assignment: *cryptographic algorithm*]
[369] [assignment: *cryptographic key sizes*]
[370] [assignment: *list of standards*]

The TOE shall meet the requirement "Cryptographic operation – ECDSA signature-creation (FCS_COP.1/COS.ECDSA.S)" as specified below.

| | |
|---|---|
| **FCS_COP.1/COS.ECDSA.S** | Cryptographic operation – ECDSA signature-creation |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/ COS.ECDSA.S | The TSF shall perform digital signature generation for the commands<br>(1) PSO COMPUTE DIGITAL SIGNATURE,<br>(2) INTERNAL AUTHENTICATE[371]<br>in accordance with a specified cryptographic algorithm ECDSA with COS standard curves using<br>(1) SHA-256,<br>(2) SHA-384,<br>(3) SHA-512[372]<br>and cryptographic key sizes 256 bits, 384 bits, 512 bits[373] that meet the following: TR-03111 [17], TR-03116-1 [19], COS specification [21], [39][374]. |

*Application note 41*: 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),

[371] [assignment: *list of cryptographic operations*]
[372] [assignment: *cryptographic algorithm*]
[373] [assignment: *cryptographic key sizes*]
[374] [assignment: *list of standards*]

  - 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 following signing algorithm
  - RSA ISO9796-2 DS2 with SHA-256 (see FCS_COP.1/COS.RSA.S)

The TOE shall meet the requirement "Cryptographic operation – RSA encryption and decryption (FCS_COP.1/COS.RSA)" as specified below.

| | |
|---|---|
| **FCS_COP.1/COS.RSA** | Cryptographic operation – RSA encryption and decryption |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/ COS.RSA | The TSF shall perform<br>(1) encryption with passed key for command PSO ENCIPHER,<br>(2) decryption with stored key for command PSO DECIPHER,<br>(3) decryption and encryption for command PSO TRANSCIPHER using RSA (transcipher of data using RSA keys),<br>(4) decryption for command PSO TRANSCIPHER using RSA (transcipher of data from RSA to ELC),<br>(5) encryption for command PSO TRANSCIPHER using ELC (transcipher of data from ELC to RSA)[375]<br>in accordance with a specified cryptographic algorithm<br>(1) for encryption: RSA-OAEP-Encrypt ([34] section 7.1.1),<br>(2) for decryption: RSA-OAEP-Decrypt ([34] section 7.1.2) [376]<br>and cryptographic key sizes 2048 bit and 3072 bit modulus length for RSA private key operation, 2048 bit modulus length for RSA public key operation, and 256 bit, 384 bit and 512 bit for the COS standard curves[377] that meet the following: TR-03116-1 [19], COS specification [21], [34][378]. |

The TOE shall meet the requirement "Cryptographic operation – ECC encryption and decryption (FCS_COP.1/COS.ELC)" as specified below.

[375] [assignment: *list of cryptographic operations*]
[376] [assignment: *cryptographic algorithm*]

| | |
|---|---|
| **FCS_COP.1/COS.ELC** | Cryptographic operation – ECC encryption and decryption |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/ COS.ELC | The TSF shall perform<br>(1) encryption with passed key for command PSO ENCIPHER,<br>(2) decryption with stored key for command PSO DECIPHER,<br>(3) decryption and encryption for command PSO TRANSCIPHER using ELC (transcipher of data using ELC keys),<br>(4) decryption for command PSO TRANSCIPHER using ELC (transcipher of data from ELC to RSA),<br>(5) encryption for command PSO TRANSCIPHER using ELC (transcipher of data from RSA to ELC)[379]<br>in accordance with a specified cryptographic algorithm<br>(1) for encryption ELC encryption,<br>(2) for decryption ELC decryption[380]<br>and cryptographic key sizes 2048 bit and 3072 bit modulus length for RSA private key operation, 2048 bit modulus length for RSA public key operation, and 256 bits, 384 bits, 512 bits for ELC keys with COS standard curves[381] that meet the following: TR-03111 [17], TR-03116-1 [19], and COS specification [21][382]. |

[377] [assignment: *cryptographic key sizes*]
[378] [assignment: *list of standards*]
[379] [assignment: *list of cryptographic operations*]
[380] [assignment: *cryptographic algorithm*]
[381] [assignment: *cryptographic key sizes*]
[382] [assignment: *list of standards*]

*Application note 42*: 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 author is asked to add a SFR FCS_COP.1/CB_HASH specifying the supported hash algorithms. **(n/a: command not supported)**

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

| | |
|---|---|
| **FCS_CKM.4** | Cryptographic key destruction |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] |
| FCS_CKM.4.1 | The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method erasure of the key[383] that meets the following: physical erasure of the key[384]. |

*Application note 43*: 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 author.

[383] [assignment: *cryptographic key destruction method*]
[384] [assignment: *list of standards*]

### 6.1.8 Protection of communication

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

| | |
|---|---|
| **FTP_ITC.1/TC** | Inter-TSF trusted channel |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| 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 | The TSF shall permit another trusted IT product[385] to initiate communication via the trusted channel. |
| FTP_ITC.1.3/TC | The TSF shall initiate communication via the trusted channel for none[386]. |

*Application note 44*: The TOE responds only to commands establishing secure messaging channels.

## 6.2 Security Assurance Requirements for the TOE

This Security Target developed based upon the Protection Profile BSI-CC-PP-0082-V4 [BSI_PP_EHC_G2] will be evaluated according to

Security Target evaluation (Class ASE)

Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation

Assurance Level 4 (EAL4)

[385] [selection: *the TSF, another trusted IT product*]
[386] [assignment: *list of functions for which a trusted channel is r*equired]

and augmented by taking the following components:

ALC_DVS.2 (Development security)

ATE_DPT.2 (Test depth)

AVA_VAN.5 (Advanced methodical vulnerability analysis).

The Security Assurance Requirements are:

| | | |
|---|---|---|
| **Class ADV: Development** | | |
| | Architectural design | (ADV_ARC.1) |
| | Functional specification | (ADV_FSP.4) |
| | Implementation representation | (ADV_IMP.1) |
| | TOE design | (ADV_TDS.3) |
| **Class AGD: Guidance documents** | | |
| | Operational user guidance | (AGD_OPE.1) |
| | Preparative user guidance | (AGD_PRE.1) |
| **Class ALC: Life-cycle support** | | |
| | CM capabilities | (ALC_CMC.4) |
| | CM scope | (ALC_CMS.4) |
| | Delivery | (ALC_DEL.1) |
| | Development security | (ALC_DVS.2) |
| | Life-cycle definition | (ALC_LCD.1) |
| | Tools and techniques | (ALC_TAT.1) |
| **Class ASE: Security Target evaluation** | | |
| | Conformance claims | (ASE_CCL.1) |
| | Extended components definition | (ASE_ECD.1) |
| | ST introduction | (ASE_INT.1) |
| | Security objectives | (ASE_OBJ.2) |
| | Derived security requirements | (ASE_REQ.2) |

| | | |
|---|---|---|
| | Security problem definition | (ASE_SPD.1) |
| | TOE summary specification | (ASE_TSS.1) |
| **Class ATE: Tests** | | |
| | Coverage | (ATE_COV.2) |
| | Depth | (ATE_DPT.2) |
| | Functional tests | (ATE_FUN.1) |
| | Independent testing | (ATE_IND.2) |
| **Class AVA: Vulnerability assessment** | | |
| | Vulnerability analysis | (AVA_VAN.5) |

**Table 26: TOE Security Assurance Requirements**

### 6.2.1 Refinements of the TOE Security Assurance Requirements

In BSI-CC-PP-0084-2014 [11] specific refinements of the TOE Security Assurance Requirements are set up. As the present Security Target takes over the refinements for the SFRs listed in section 6.1.3 "Security Functional Requirements for the TOE taken over from the IC Platform Security Target" (see Table 25), the SAR refinements from BSI-CC-PP-0084-2014 [11] are applied to these refined SFRs. The SAR refinements and the section where these refinements in BSI-CC-PP-0084-2014 [11] are specified are listed in Table 27.

For all other SFRs the TOE Security Assurance Requirements from Common Criteria Part 3 [3] iare used. The TOE Security Assurance Requirements as defined in BSI-CC-PP-0084-2014 [11] (see Table 27) are used for *all* SFRs in the present Security Target.

| Refinements regarding | Reference to [11] |
|---|---|
| Delivery procedure (ALC_DEL) | Section 6.2.1.1 "Refinements regarding Delivery procedure (ALC_DEL)" |
| Development Security (ALC_DVS) | Section 6.2.1.2 "Refinements regarding Development Security (ALC_DVS)" |
| CM scope (ALC_CMS) | Section 6.2.1.3 "Refinements regarding CM scope (ALC_CMS)" |

| | |
|---|---|
| CM capabilities (ALC_CMC) | Section 6.2.1.4 "Refinements regarding CM capabilities (ALC_CMC)" |
| Security Architecture (ADV_ARC) | Section 6.2.1.5 "Refinements regarding Security Architecture (ADV_ARC)" |
| Functional Specification (ADV_FSP) | Section 6.2.1.6 "Refinements regarding Functional Specification (ADV_FSP)" |
| Implementation Representation (ADV_IMP) | Section 6.2.1.7 "Refinements regarding Implementation Representation (ADV_IMP)" |
| Test Coverage (ATE_COV) | Section 6.2.1.8" Refinements regarding Test Coverage (ATE_COV)" |
| User Guidance (AGD_OPE) | Section 6.2.1.9 "Refinements regarding User Guidance (AGD_OPE)" |
| Preparative User Guidance (AGD_PRE) | Section 6.2.1.10 "Refinements regarding Preparative User Guidance (AGD_PRE)" |
| Refinement regarding Vulnerability Analysis (AVA_VAN) | Section 6.2.1.11 "Refinement regarding Vulnerability Analysis (AVA_VAN)" |

**Table 27: Refined TOE Security Assurance Requirements**

The following sections define further specific refinements and application notes to the chosen SARs that have to be applied for the TOE and its evaluation. These refinements and application notes are taken over from the Protection Profile BSI-CC-PP-0082-V4 [BSI_PP_EHC_G2].

### 6.2.2 Refinements to ADV_ARC.1 Security architecture description

The ADV_ARC.1 Security architecture description requires as developer action

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

and the related content and presentation element

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

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.

**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.**

### 6.2.3 Refinements to ADV_FSP.4 Complete functional specification

The following content and presentation element of ADV_FSP.4 Complete functional specification is refined as follows:

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.**

*Application note 45:* 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], section 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.

### 6.2.4 Refinement to ADV_IMP.1

The following content and presentation element of ADV_IMP.1 Implementation representation of the TSF is refined as follows:

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

*Application note 46:* The refinement extends the TSF implementation representation to the TOE implementation representation, i.e. the complete executable code implemented on the Security IC Platform including all IC Embedded Software, especially the Card Operating System (COS) and related configuration data.

### 6.2.5 Refinements to AGD_OPE.1 Operational user guidance

The following content and presentation element of AGD_OPE.1 Operational user guidance is refined as follows:

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.**

*Application note 47*: The wrapper will be used to interact with the smart card for the 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 the 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.

### 6.2.6 Refinements to ATE_FUN.1 Functional tests

The following content and presentation element of ATE_FUN.1 Functional tests is refined as follows:

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 use cases applicable for the TOE and the intended application eHC [22], eHPC [23], SMC-B [24], gSMC-K [25] or gSMC-KT [26].**

*Application note 48*: 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.

### 6.2.7 Refinements to ATE_IND.2 Independent testing – sample

The following content and presentation element of ATE_IND.2 Functional tests is refined as follows:

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 use cases applicable for the TOE and the intended application eHC [22], eHPC [23], SMC-B [24], gSMC-K [25] and gSMC-KT [26].**

*Application note 49*: 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.

## 6.3 Security Requirements Rationale

This section comprises three parts:

- the SFR rationale provided by a table and explanatory text showing the coverage of Security Objectives for the TOE by Security Functional Requirements,
- the SFR dependency rationale, and
- the SAR rationale.

### 6.3.1 Security Functional Requirements Rationale

Section 7.4.1 in the IC Platform Security Target [ST_IC] gives an overview, how the Security Functional Requirements that are taken over in the present ST collaborate to meet the respective Security Objectives. Please refer for the further details to the related justification provided in [ST_IC].

For the TOE's IC part, the following table provides an overview for Security Functional Requirements coverage also giving an evidence for *sufficiency* and *necessity* of the SFRs chosen.

| | O.Identification | O.Leak-Inherent | O.Phys-Probing | O.Malfunction | O.Phys-Manipulation | O.Leak-Forced | O.Abuse-Func | O.RND | O.Authentication | O.Mem-Access | O.AES | O.Add-Functions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FCS_CKM.1/RSA-0_SICP | | | | | | | | | | | | x |

| | O.Identification | O.Leak-Inherent | O.Phys-Probing | O.Malfunction | O.Phys-Manipulation | O.Leak-Forced | O.Abuse-Func | O.RND | O.Authentication | O.Mem-Access | O.AES | O.Add-Functions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FCS_CKM.1/EC-0_SICP | | | | | | | | | | | | x |
| FCS_CKM.4/AES-SCL-1_SICP | | | | | | | | | | | x | |
| FCS_COP.1/AES-SCL-1_SICP | | | | | | | | | | | x | |
| FCS_COP.1/RSA-0_SICP | | | | | | | | | | | | x |
| FCS_COP.1/ECDSA-0_SICP | | | | | | | | | | | | x |
| FCS_COP.1/ECDH-0_SICP | | | | | | | | | | | | x |
| FAU_SAS.1/SICP | x | | | | | | | | | | | |
| FCS_RNG.1/HPRG_SICP | | | | | | | | x | | | | |
| FDP_ACC.1/SICP | | | | | | | | | | x | | |
| FDP_ACF.1/SICP | | | | | | | | | | x | | |
| FDP_IFC.1/SICP | | x | | | | x | x | x | | | | |
| FDP_ITT.1/SICP | | x | | | | x | x | x | | | | |
| FDP_SDC.1/SICP | | | x | | | | | | | | | |
| FDP_SDI.2/SICP | | | | | x | | | | | | | |
| FIA_API.1/SICP | | | | | | | | | x | | | |
| FMT_LIM.1/SICP | | | | | | | x | | | | | |
| FMT_LIM.2/SICP | | | | | | | x | | | | | |
| FMT_MSA.1/SICP | | | | | | | | | | x | | |
| FMT_MSA.3/SICP | | | | | | | | | | x | | |
| FMT_SMF.1/SICP | | | | | | | | | | x | | |
| FPT_FLS.1/SICP | | | | x | | x | x | x | | | | |
| FPT_ITT.1/SICP | | x | | | | x | x | x | | | | |
| FPT_PHP.3/SICP | | | x | | x | x | x | x | | | | |

| | O.Identification | O.Leak-Inherent | O.Phys-Probing | O.Malfunction | O.Phys-Manipulation | O.Leak-Forced | O.Abuse-Func | O.RND | O.Authentication | O.Mem-Access | O.AES | O.Add-Functions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FPT_TST.2/SICP | | | | | x | | | | | | | |
| FRU_FLT.2/SICP | | | | x | | x | x | x | | | | |

**Table 28: Coverage of Security Objectives for the TOE's IC part by SFRs**

As stated in section 2.4, this ST claims conformance to BSI-CC-PP-0084-2014 [11]. The Security Objectives and SFRs as mentioned in Table 28 are defined and handled in the IC Platform Security Target [ST_IC] which claims conformance to [11]. In particular, the rationale for these items and their correlation is given in [ST_IC] and [11] and not repeated here.

In the following, the further Security Objectives for the TOE and SFRs are considered.

| | O.Integrity | O.Confidentiality | O.Resp-COS | O.TSFDataExport | O.Authentication | O.AccessControl | O.KeyManagement | O.Crypto | O.SecureMessaging |
|---|---|---|---|---|---|---|---|---|---|
| FDP_RIP.1 | | x | | | | | | | |
| FDP_SDI.2 | x | | | | | | | | |
| FPT_FLS.1 | x | x | | | | | | | |
| FPT_EMS.1 | | x | | | | | | | |
| FPT_TDC.1 | | | | x | | | | | |
| FPT_ITE.1 | | | | x | | | | | |
| FPT_ITE.2 | | | | x | | | | | |
| FPT_TST.1 | x | x | x | | | | | | |

| | O.Integrity | O.Confidentiality | O.Resp-COS | O.TSFDataExport | O.Authentication | O.AccessControl | O.KeyManagement | O.Crypto | O.SecureMessaging |
|---|---|---|---|---|---|---|---|---|---|
| FIA_SOS.1 | | | | | x | | | | |
| FIA_AFL.1/PIN | | | | | x | | | | |
| FIA_AFL.1/PUC | | | | | x | | | | |
| FIA_ATD.1 | | | | | x | | | | |
| FIA_UAU.1 | | | | | x | | | | |
| FIA_UAU.4 | | | | | x | | | | |
| FIA_UAU.5 | | | | | x | | | | |
| FIA_UAU.6 | | | | | x | | | | |
| FIA_UID.1 | | | | | x | | | | |
| FIA_API.1 | | | | | x | | | | |
| FMT_SMR.1 | | | | | x | x | | | |
| FIA_USB.1 | | | | | x | x | | | |
| FDP_ACC.1/MF_DF | | | | | | x | | | |
| FDP_ACF.1/MF_DF | | | | | | x | | | |
| FDP_ACC.1/EF | | | | | | x | | | |
| FDP_ACF.1/EF | | | | | | x | | | |
| FDP_ACC.1/TEF | | | | | | x | | | |
| FDP_ACF.1/TEF | | | | | | x | | | |
| FDP_ACC.1/SEF | | | | | | x | | | |
| FDP_ACF.1/SEF | | | | | | x | | | |
| FDP_ACC.1/KEY | | | | | | x | x | | |
| FDP_ACF.1/KEY | | | | | | x | x | | |
| FMT_MSA.3 | | | | | | x | | | |
| FMT_SMF.1 | | | | | | x | | | |
| FMT_MSA.1/Life | | | | | x | x | x | | |
| FMT_MSA.1/SEF | | | | | | x | | | |

| | O.Integrity | O.Confidentiality | O.Resp-COS | O.TSFDataExport | O.Authentication | O.AccessControl | O.KeyManagement | O.Crypto | O.SecureMessaging |
|---|---|---|---|---|---|---|---|---|---|
| FMT_MTD.1/PIN | | | | | x | x | | | |
| FMT_MSA.1/PIN | | | | | x | x | | | |
| FMT_MTD.1/Auth | | | | | x | x | | | |
| FMT_MSA.1/Auth | | | | | x | x | | | |
| FMT_MTD.1/NE | | x | | x | | x | | | |
| FCS_RNG.1 | | | | | | | x | x | |
| FCS_RNG.1/GR | | | | | | | | x | |
| FCS_COP.1/SHA | | | | | | | | x | |
| FCS_COP.1/COS.AES | | | | | | | | x | x |
| FCS_CKM.1/AES.SM | | | | | | | x | x | x |
| FCS_CKM.1/ELC | | | | | | | x | x | |
| FCS_COP.1/COS.CMAC | | | | | | | | x | x |
| FCS_COP.1/COS.RSA.S | | | | | | | | x | |
| FCS_COP.1/COS.ECDSA.S | | | | | | | | x | |
| FCS_COP.1/COS.ECDSA.V | | | | | | | | x | |
| FCS_COP.1/COS.RSA | | | | | | | | x | |
| FCS_COP.1/COS.ELC | | | | | | | | x | |
| FCS_CKM.4 | | | | | | | x | | |
| FTP_ITC.1/TC | | | | | | | | | x |

**Table 29: Mapping between Security Objectives for the TOE and SFRs**

A detailed justification required for *suitability* of the Security Functional Requirements to achieve the Security Objectives is given below.

The Security Objective **O.Integrity** "Integrity of internal data" requires the protection of the integrity of User Data, TSF Data and security services. This Security Objective is addressed by the SFRs FDP_SDI.2, FPT_FLS.1 and FPT_TST.1: FPT_TST.1 requires self

tests to demonstrate the correct operation of the TSF and its protection capabilities. FDP_SDI.2 requires the TSF to monitor User Data stored in containers and to take assigned action when data integrity errors are detected. In case of failures, FPT_FLS.1 requires the preservation of a secure state in order to protect the User Data, TSF Data and security services.

The Security Objective **O.Confidentiality** "Confidentiality of internal data" requires the protection of the confidentiality of sensitive User Data and TSF Data. This Security Objective is addressed by the SFRs FDP_RIP.1, FPT_FLS.1, FPT_EMS.1, FPT_TST.1 and FMT_MTD.1/NE:

FMT_MTD.1/NE restricts the ability to export sensitive TSF Data to dedicated roles, some sensitive User Data like private authentication keys are not allowed to be exported at all. FPT_EMS.1 requires that the TOE does not emit any information of sensitive User Data and TSF Data by emissions and via circuit interfaces. Further, FDP_RIP.1 requires that residual information regarding sensitive data in previously used resources will not be available after its usage. FPT_TST.1 requires self tests to demonstrate the correct operation of the TSF and its confidentiality protection capabilities. In case of failures, FPT_FLS.1 requires the preservation of a secure state in order to protect the User Data, TSF Data and security services.

The Security Objective **O.Resp-COS** "Treatment of User and TSF Data" requires the correct treatment of the User Data and TSF Data as defined by the TSF Data of the object system. This correct treatment is ensured by appropriate self tests of the TSF. FPT_TST.1 requires self tests to demonstrate the correct operation of the TSF and its data treatment.

The Security Objective **O.TSFDataExport** "Support of TSF Data export" requires the correct export of TSF Data of the object system excluding confidential TSF Data. This Security Objective is addressed by the SFRs FPT_TDC.1, FPT_ITE.1, FPT_ITE.2 and FMT_MTD.1/NE: FPT_ITE.2 requires the export of dedicated TSF Data but restricts the kind of TSF Data that can be exported. Hence, confidential data shall not be exported. Also, the TSF is required to be able to export the fingerprint of TOE implementation by the SFR FPT_ITE.1. For Card Verifiable Certificates (CVC), the SFR FPT_TDC.1 requires the consistent interpretation when shared between the TSF and another trusted IT product. FMT_MTD.1/NE restricts the ability to export sensitive TSF Data.

The Security Objective **O.Authentication** "Authentication of external entities" requires the support of authentication of human users and external devices as well as the ability of the TSF to authenticate itself. This Security Objective is addressed by the following SFRs:

- FIA_SOS.1 requires that the TSF enforces the length of the secret of the password objects.

- FIA_AFL.1/PIN requires that the TSF detects repeated unsuccessful authentication attempts and blocks the password authentication when the number of unsuccessful authentication attempts reaches a defined number.
- FIA_AFL.1/PUC requires that the TSF detects repeated unsuccessful authentication attempts for the password unblocking function and performs appropriate actions when the number of unsuccessful authentication attempts reaches a defined number.
- FIA_ATD.1 requires that the TSF maintains dedicated security attributes belonging to individual users.
- FIA_UAU.1 requires the processing of dedicated actions before a user is authenticated. Any other actions shall require user authentication.
- FIA_UAU.4 requires the prevention of reuse of authentication data.
- FIA_UAU.5 requires the TSF to support user authentication by providing dedicated commands. Multiple authentication mechanisms like password based and key based authentication are required.
- FIA_UAU.6 requires the TSF to support re-authentication of message senders using a secure messaging channel.
- FIA_UID.1 requires the processing of dedicated actions before a user is identified. Any other actions shall require user identification.
- FIA_API.1 requires that the TSF provides dedicated commands to prove the identity of the TSF itself.
- FMT_SMR.1 requires that the TSF maintains roles and associates users with roles.
- FIA_USB.1 requires that the TSF associates dedicated security attributes with subjects acting on behalf of that user. Also, the TSF shall enforce rules governing changes of these security attributes by the implementation of commands that perform these changes.
- FMT_MSA.1/Life requires that the TSF enforces the access control policy to restrict the ability to manage life cycle relevant security attributes like *lifeCycleStatus*. For that purpose the SFR requires management functions to implement these operations.
- FMT_MTD.1/PIN requires that the TSF restricts the ability to change password objects by the implementation of dedicated commands and management functions.
- FMT_MSA.1/PIN requires that the TSF enforces the access control policy to restrict the ability to change, enable and disable and optionally perform further operations of security attributes for password objects. For that purpose the SFR requires management functions to implement these operations.
- FMT_MTD.1/Auth requires that the TSF restricts the ability to import device authentication reference data by the implementation of dedicated commands and management functions.
- FMT_MSA.1/Auth requires that the TSF enforces the access control policy to restrict the ability to read security attributes for the device authentication

reference data. For that purpose the SFR requires management functions to implement this operation.

The Security Objective **O.AccessControl** "Access Control for Objects" requires the enforcement of an access control policy to restricted objects and devices. Further, the management functionality for the access policy is required. This Security Objective is addressed by the following SFRs:

- FMT_SMR.1 requires that the TSF maintains roles and associates users with roles.
- FIA_USB.1 requires that the TSF associates dedicated security attributes with subjects acting on behalf of that user. Also, the TSF shall enforce rules governing changes of these security attributes by the implementation of commands that perform these changes.
- FDP_ACC.1/MF_DF requires that the TSF enforces an access control policy to restrict operations on MF and folder objects as well as applications performed by subjects of the TOE.
- FDP_ACF.1/MF_DF requires that the TSF enforce an access control policy to restrict operations on MF and folder objects as well as applications based on a set of rules defined in the SFR. Also, the TSF is required to deny access to the MF object in case of "Termination state" of the TOE life cycle.
- FDP_ACC.1/EF requires that the TSF enforces an access control policy to restrict operations on EF objects performed by subjects of the TOE.
- FDP_ACF.1/EF requires that the TSF enforce an access control policy to restrict operations on EF objects based on a set of rules defined in the SFR. Also, the TSF is required to deny access to EF objects in case of "Termination state" of the TOE life cycle.
- FDP_ACC.1/TEF requires that the TSF enforces an access control policy to restrict operations on transparent EF objects performed by subjects of the TOE.
- FDP_ACF.1/TEF requires that the TSF enforce an access control policy to restrict operations on transparent EF objects based on a set of rules defined in the SFR. Also, the TSF is required to deny access to transparent EF objects in case of "Termination state" of the TOE life cycle.
- FDP_ACC.1/SEF requires that the TSF enforces an access control policy to restrict operations on structured EF objects performed by subjects of the TOE.
- FDP_ACF.1/SEF requires that the TSF enforce an access control policy to restrict operations on structured EF objects based on a set of rules defined in the SFR. Also, the TSF is required to deny access to structured EF objects in case of "Termination state" of the TOE life cycle.
- FDP_ACC.1/KEY requires that the TSF enforces an access control policy to restrict operations on dedicated key objects performed by subjects of the TOE.
- FDP_ACF.1/KEY requires that the TSF enforce an access control policy to restrict operations on dedicated key objects based on a set of rules defined in the SFR.

Also, the TSF is required to deny access to dedicated key objects in case of "Termination state" of the TOE life cycle.

- FMT_MSA.3 requires that the TSF enforces an access control policy that provides restrictive default values for the used security attributes. Alternative default values for these security attributes shall only be allowed for dedicated authorised roles.
- FMT_SMF.1 requires that the TSF implements dedicated management functions that are given in the SFR.
- FMT_MSA.1/Life requires that the TSF enforces the access control policy to restrict the ability to manage life cycle relevant security attributes like *lifeCycleStatus*. For that purpose the SFR requires management functions to implement these operations.
- FMT_MSA.1/SEF requires that the TSF enforces the access control policy to restrict the ability to manage of security attributes of records. For that purpose the SFR requires management functions to implement these operations.
- FMT_MTD.1/PIN requires that the TSF restricts the ability to change password objects by the implementation of dedicated commands and management functions.
- FMT_MSA.1/PIN requires that the TSF enforces the access control policy to restrict the ability to read, change, enable, disable and optionally perform further operations of security attributes for password objects. For that purpose the SFR requires management functions to implement these operations.
- FMT_MTD.1/Auth requires that the TSF restricts the ability to import device authentication reference data by the implementation of dedicated commands and management functions.
- FMT_MSA.1/Auth requires that the TSF enforces the access control policy to restrict the ability to read security attributes for the device authentication reference data. For that purpose the SFR requires management functions to implement this operation.
- FMT_MTD.1/NE restricts the ability to export sensitive TSF Data to dedicated roles, some sensitive User Data like private authentication keys are not allowed to be exported at all.

The Security Objective **O.KeyManagement** "Generation and import of keys" requires the ability of the TSF to secure generation, import, distribution, access control and destruction of cryptographic keys. Also, the TSF is required to support the import and export of public keys. This Security Objective is addressed by the following SFRs:

- FCS_RNG.1 requires that the TSF provides a random number generator of a specific class used for generation of keys.
- FCS_CKM.1/AES.SM and FCS_CKM.1/ELC require that the TSF generates cryptographic keys with specific key generation algorithms as stated in the SFRs.

The mentioned SFRs are needed to fulfil different requirements of the intended usage of the cryptographic keys.

- FCS_CKM.4 requires that the TSF destroys cryptographic keys in accordance with a given specific key destruction method.
- FDP_ACC.1/KEY and FDP_ACF.1/KEY control access to the key management and the cryptographic operations using keys.
- FMT_MSA.1/Life requires restriction of the management of security attributes of the keys to subjects 209nitializa for specific commands.

The Security Objective **O.Crypto** "Cryptographic functions" requires the ability of the TSF to implement secure cryptographic algorithms. This Security Objective is addressed by the following SFRs:

- FCS_RNG.1 requires that the TSF provides a random number generator of a specific class used for generation of keys.
- FCS_RNG.1/GR requires that the TSF provides a random number generator of a specific class for providing random numbers to the external world for further use.
- FCS_COP.1/SHA requires that the TSF provides different hashing algorithms that are referenced in the SFR.
- FCS_COP.1/COS.AES requires that the TSF provides decryption and encryption using AES with different key sizes.
- FCS_COP.1/COS.CMAC requires that the TSF provides computation and verification of cryptographic checksums using the CMAC algorithm.
- FCS_COP.1/COS.RSA.S requires that the TSF provides the generation of digital signatures based on the RSA algorithm and different modulus lengths.
- FCS_COP.1/COS.ECDSA.S requires that the TSF provides the generation of digital signatures based on the ECDSA and different hash algorithms and different key sizes.
- FCS_COP.1/COS.ECDSA.V requires that the TSF provides the verification of digital signatures based on the ECDSA and different hash algorithms and different key sizes.
- FCS_COP.1/COS.RSA requires that the TSF provides encryption and decryption capabilities based on RSA algorithms with different modulus lengths.
- FCS_COP.1/COS.ELC requires that the TSF provides encryption and decryption capabilities based on ELC algorithms with different key sizes.
- FCS_CKM.1/AES.SM and FCS_CKM.1/ELC require that the TSF generates cryptographic keys with specific key generation algorithms as stated in the SFRs. The mentioned SFRs are needed to fulfil different requirements of the intended usage of the cryptographic keys.

The Security Objective **O.SecureMessaging** "Secure messaging" requires the ability of the TSF to use and enforce the use of a trusted channel to successfully authenticated external entities that ensures the integrity and confidentiality of the transmitted data

between the TSF and the external entity. This Security Objective is addressed by the following SFRs:

- FCS_CKM.1/AES.SM requires that the TSF generates cryptographic keys (AES) of different key sizes with specific key generation algorithms as stated in the SFR.
- FCS_COP.1/COS.AES requires that the TSF provides decryption and encryption using AES with different key sizes. One use case of that required functionality is secure messaging.
- FCS_COP.1/COS.CMAC requires that the TSF provides computation and verification of cryptographic checksums using the AES-based CMAC algorithm with different key sizes. One use case of that required functionality is secure messaging.
- FTP_ITC.1/TC requires that the TSF provides a communication channel between itself and another trusted IT product. The channel provides assured identification of its end points and protection of the channel data against modification and disclosure.

### 6.3.2 Rationale for SFR Dependencies

Table 18 in the IC Platform Security Target [ST_IC] lists the Security Functional Requirements defined in [ST_IC], their dependencies and whether they are satisfied by other security requirements defined in that Protection Profile. Please refer for the further details to the related justification provided in [ST_IC].

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

The dependency analysis has directly been made within the description of each SFR in section 6.1 above. All dependencies being expected by CC Part 2 and by extended components definition in section 5 are either fulfilled or their non-fulfilment is justified.

The following table lists the required dependencies of the SFRs of this ST and gives the concrete SFRs from this document which fulfil the required dependencies.

| SFR | dependent | fulfilled by |
|---|---|---|
| FDP_RIP.1 | No dependencies. | n. a. |
| FDP_SDI.2 | No dependencies. | n. a. |

| SFR | dependent | fulfilled by |
|---|---|---|
| FPT_FLS.1 | No dependencies. | n. a. |
| FPT_EMS.1 | No dependencies. | n. a. |
| FPT_TDC.1 | No dependencies. | n. a. |
| FPT_ITE.1 | No dependencies. | n. a. |
| FPT_ITE.2 | No dependencies. | n. a. |
| FPT_TST.1 | No dependencies. | n. a. |
| FIA_SOS.1 | No dependencies. | n. a. |
| FIA_AFL.1/PIN | FIA_UAU.1 Timing of authentication | FIA_UAU.1 |
| FIA_AFL.1/PUC | FIA_UAU.1 Timing of authentication | FIA_UAU.1 |
| FIA_ATD.1 | No dependencies. | n. a. |
| FIA_UAU.1 | FIA_UID.1 Timing of identification | FIA_UID.1 |
| FIA_UAU.4 | No dependencies. | n. a. |
| FIA_UAU.5 | No dependencies. | n. a. |
| FIA_UAU.6 | No dependencies. | n. a. |
| FIA_UID.1 | No dependencies. | n. a. |
| FIA_API.1 | No dependencies. | n. a. |
| FMT_SMR.1 | FIA_UID.1 Timing of identification | FIA_UID.1 |
| FIA_USB.1 | FIA_ATD.1 User attribute definition | FIA_ATD.1 |
| FDP_ACC.1/MF_DF | FDP_ACF.1 Security attribute based access control | FDP_ACF.1/MF_DF |
| FDP_ACF.1/MF_DF | FDP_ACC.1 Subset access control,<br>FMT_MSA.3 Static attribute initialisation | FDP_ACC.1/MF_DF,<br>FMT_MSA.3 |

| SFR | dependent | fulfilled by |
|---|---|---|
| FDP_ACC.1/EF | FDP_ACF.1 Security attribute based access control | FDP_ACF.1/EF |
| FDP_ACF.1/EF | FDP_ACC.1 Subset access control,<br>FMT_MSA.3 Static attribute initialisation | FDP_ACC.1/EF,<br>FMT_MSA.3 |
| FDP_ACC.1/TEF | FDP_ACF.1 Security attribute based access control | FDP_ACF.1/TEF |
| FDP_ACF.1/TEF | FDP_ACC.1 Subset access control,<br>FMT_MSA.3 Static attribute initialisation | FDP_ACC.1/TEF,<br>FMT_MSA.3 |
| FDP_ACC.1/SEF | FDP_ACF.1 Security attribute based access control | FDP_ACF.1/SEF |
| FDP_ACF.1/SEF | FDP_ACC.1 Subset access control,<br>FMT_MSA.3 Static attribute initialisation | FDP_ACC.1/SEF,<br>FMT_MSA.3 |
| FDP_ACC.1/KEY | FDP_ACF.1 Security attribute based access control | FDP_ACF.1/KEY |
| FDP_ACF.1/KEY | FDP_ACC.1 Subset access control,<br>FMT_MSA.3 Static attribute initialisation | FDP_ACC.1/KEY,<br>FMT_MSA.3 |
| FMT_MSA.3 | FMT_MSA.1 Management of security attributes,<br>FMT_SMR.1 Security roles | FMT_MSA.1/Life,<br>FMT_MSA.1/SEF,<br>FMT_MSA.1/PIN,<br>FMT_MSA.1/Auth,<br>FMT_SMR.1 |
| FMT_SMF.1 | No dependencies. | n. a. |
| FMT_MSA.1/Life | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control],<br>FMT_SMR.1 Security roles, | FDP_ACC.1/MF_DF,<br>FDP_ACC.1/EF,<br>FDP_ACC.1/TEF,<br>FDP_ACC.1/SEF,<br>FDP_ACC.1/KEY, |

| SFR | dependent | fulfilled by |
|---|---|---|
| | FMT_SMF.1 Specification of Management Functions | FMT_SMR.1, FMT_SMF.1 |
| FMT_MSA.1/SEF | [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions | FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY, FMT_SMR.1, FMT_SMF.1 |
| FMT_MTD.1/PIN | FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions | FMT_SMR.1, FMT_SMF.1 |
| FMT_MSA.1/PIN | [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions | FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY, FMT_SMR.1, FMT_SMF.1 |
| FMT_MTD.1/Auth | FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions | FMT_SMR.1, FMT_SMF.1 |
| FMT_MSA.1/Auth | [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions | FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY, FMT_SMR.1, FMT_SMF.1 |
| FMT_MTD.1/NE | FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions | FMT_SMR.1, FMT_SMF.1 |
| FCS_RNG.1 | No dependencies. | n. a. |
| FCS_RNG.1/GR | No dependencies. | n. a. |
| FCS_COP.1/SHA | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic | The dependent SFRs are not applicable here because FCS_COP.1/SHA does not use any keys. |

| SFR | dependent | fulfilled by |
|---|---|---|
| | key generation],<br>FCS_CKM.4 Cryptographic key destruction | |
| FCS_COP.1/COS.AES | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | FCS_CKM.1/AES.SM,<br>FCS_CKM.4 |
| FCS_CKM.1/AES.SM | [FCS_CKM.2 Cryptographic key distribution, or<br>FCS_COP.1 Cryptographic operation],<br>FCS_CKM.4 Cryptographic key destruction | FCS_COP.1/COS.AES,<br>FCS_CKM.4 |
| FCS_CKM.1/ELC | [FCS_CKM.2 Cryptographic key distribution, or<br>FCS_COP.1 Cryptographic operation],<br>FCS_CKM.4 Cryptographic key destruction | FCS_COP.1/COS.ELC,<br>FCS_COP.1/COS.ECDSA.S,<br>FCS_CKM.4 |
| FCS_COP.1/COS.CMAC | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | FCS_CKM.1/AES.SM,<br>FCS_CKM.4 |
| FCS_COP.1/COS.RSA.S | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | *FCS_CKM.1/RSA* in the case that the TOE provides RSA key generation functionality, i.e. Package RSA Key Generation is applied. ~~Otherwise, dependency on FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1 is not applicable as neither key~~ |

| SFR | dependent | fulfilled by |
|---|---|---|
| | | ~~import nor key generation by the TOE for RSA key pairs / private keys are relevant for the operational phase.~~[387]<br>FCS_CKM.4 |
| FCS_COP.1/COS.ECDSA.S | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | FCS_CKM.1/ELC,<br>FCS_CKM.4 |
| FCS_COP.1/COS.ECDSA.V | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | FMT_MTD.1/Auth requires import keys of type TSF Data used by FCS_COP.1/COS.ECDSA.V (instead of import of User Data addressed in FDP_ITC.1 and FDP_ITC.2). Furthermore, FCS_CKM.1 is not applicable for the same reason.<br>FCS_CKM.4 |
| FCS_COP.1/COS.RSA | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation], | *FCS_CKM.1/RSA* in the case that the TOE provides RSA key generation functionality, i.e. Package RSA Key Generation is applied. ~~Otherwise, dependency on FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1 is not~~ |

[387] Package RSA Key Generation **is** applied

| SFR | dependent | fulfilled by |
|---|---|---|
| | FCS_CKM.4 Cryptographic key destruction | ~~applicable as neither key import nor key generation by the TOE for RSA key pairs / private keys are relevant for the operational phase.~~[388]<br>FCS_CKM.4 |
| FCS_COP.1/COS.ELC | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | FCS_CKM.1/ELC,<br>FCS_CKM.4 |
| FCS_CKM.4 | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation] | FCS_CKM.1/AES.SM,<br>*FCS_CKM.1/RSA* in the case that the TOE provides RSA key generation functionality, i.e. Package RSA Key Generation is applied,[389]<br>FCS_CKM.1/ELC |
| FTP_ITC.1/TC | No dependencies. | n. a. |

**Table 30: Dependencies of the SFRs**

### 6.3.3 Security Assurance Requirements Rationale

The present Assurance Package was chosen based on the pre-defined Assurance Package EAL4. This Package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which,

[388] Package RSA Key Generation **is** applied
[389] Package RSA Key Generation **is** applied

though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. 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.

Please refer as well to BSI-CC-PP-0084-2014 [11], section 6.3.3 "Rationale for the Assurance Requirements" 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 smart card 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-CC-PP-0084-2014 [11] would have been sufficient to fulfil the conformance, but this would contradict the intention of BSI-CC-PP-0084-2014. Therefore the augmentation with ATE_DPT.2 is required for the complete Security Target.

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 Security Assurance Requirements being part of EAL4 fulfils all dependencies a priori.

The augmentation of EAL4 chosen comprises the following assurance components:

- ATE_DPT.2,
- ALC_DVS.2, and
- AVA_VAN.5.

For these additional assurance components, all dependencies are met or exceeded in the EAL4 Assurance Package:

| Component | Dependencies required by CC Part 3 | Dependency fulfilled by |
|---|---|---|
| TOE Security Assurance Requirements (only additional to EAL4) | | |
| ALC_DVS.2 | no dependencies | - |
| ATE_DPT.2 | ADV_ARC.1 | ADV_ARC.1 |
| | ADV_TDS.3 | ADV_TDS.3 |
| | ATE_FUN.1 | ATE_FUN.1 |
| AVA_VAN.5 | ADV_ARC.1 | ADV_ARC.1 |
| | ADV_FSP.4 | ADV_FSP.4 |
| | ADV_TDS.3 | ADV_TDS.3 |
| | ADV_IMP.1 | ADV_IMP.1 |
| | AGD_OPE.1 | AGD_OPE.1 |
| | AGD_PRE.1 | AGD_PRE.1 |
| | ATE_DPT.1 | ATE_DPT.2 |

**Table 31: SAR Dependencies**

# 7 Package Contactless

The COS supports additional functionality for contactless communication of the Proximity Integrated Circuit Chip (PICC) using the chip part of the PACE protocol according to [21]. This section defines the Package Contactless as used by the ST author.

## 7.1 TOE Overview for Package Contactless

This Package describes additional TSF used for contactless communication as PICC with a terminal. The COS has to detect by itself if the underlying chip uses a contactless interface and has to use interface dependent access rules in that case.

## 7.2 Security Problem Definition for Package Contactless

### 7.2.1 Assets and External Entities

**Assets**

The assets do not differ from the assets defined in section 3.1.

**Security Attributes of Users and Subjects**

The PACE protocol provides mutual authentication between a smart card running the Proximity Integrated Circuit Chip (PICC) role and a terminal running the Proximity Coupling Devices (PCD) role of the protocol as described in [16] Part 2. The TOE supporting the Package Contactless implements the PICC role of the PACE protocol. When the TOE is running the PICC role of the PACE protocol the subject gains security attributes used by the access control and bound to the use of the established secure messaging channel after successful authentication.

The support of contactless communication introduces additional security attributes of users and subjects bound to external entities.

| User type | Definition |
|---|---|
| Device with contactless communication | An external device communicating with the TOE through the contactless interface. The subject bind to this device has the security attribute "kontaktlos" (contactless communication). |
| Device authenticated using PACE protocol in PCD role | An external device communicating with the TOE through the contactless interface and successfully authenticated by the PACE protocol in PCD role. |

**Table 32: User type for Package Contactless**

### 7.2.2 Threats

There are no additional Threats for the Package Contactless beyond the Threats already defined in section 3.2.

### 7.2.3 Organisational Security Policies

There are no additional Organisational Security Policies for the Package Contactless beyond the Organisational Security Policies already defined in section 3.3.

### 7.2.4 Assumptions

There are no additional Assumptions for the Package Contactless beyond the Assumptions already defined in section 3.4.

## 7.3 Security Objectives for Package Contactless

The Security Objectives for the TOE (section 4.1) and the Security Objectives for the Operational Environment (section 4.2) are supplemented for the Package Contactless. Therefore the Security Objective Rationale (section 4.3) is supplemented as well.

The TOE shall fulfil the Security Objective "Protection of contactless communication with PACE/PICC (O.PACE_CHIP)" as specified below.

| | |
|---|---|
| **O.PACE_Chip** | **Protection of contactless communication with PACE/PICC**<br>The TOE supports the chip part of the PACE protocol in order to protect the confidentiality and the integrity of data communicated through the contactless interface of the TOE. |

The operational environment of the TOE shall fulfil the Security Objective "PACE support by contactless terminal (OE.PACE_Terminal)" as specified below.

| | |
|---|---|
| **OE.PACE_Terminal** | **PACE support by contactless terminal**<br>The external device communicating through a contactless interface with the TOE using PACE shall support the terminal part of the PACE protocol. |

The Security Objectives O.PACE_CHIP and OE.PACE_Terminal mitigate the Threat T.Intercept if contactless communication between the TOE and the terminal is used and the operational environment is not able to protect the communication by other means.

## 7.4 Security Requirements for Package Contactless

In addition to the authentication reference data of the devices listed in Table 20 the following table defines for the TOE with Package Contactless the authentication reference data of the user in PCD role and the authentication verification data used by the TSF itself (cf. FIA_API.1) in PICC role.

| User type / Subject type | Authentication data and security attributes | Operations |
|---|---|---|
| Device as PCD | **Symmetric Card Connection Object** (SCCO)<br>Authentication reference data<br>SCCO stored in the TOE and corresponding to the CAN, MAC session key SK4SM<br>Security attributes<br>*keyIdentifier* of the SCCO in the *globalSecurityList* if SCCO was in the MF or in *dfSpecificSecurityList* if the SCCO was in the respective folder<br>SK4SM referenced in *macKey* and *SSCmac* | GENERAL AUTHENTICATE with (CLA,INS,P1,P2)=('x0','86','00','00') is used by the TOE running the PACE protocol role as PICC to authenticate the external device running the PACE protocol role as PCD. |
| TOE as PICC | SK4SM referenced in *macKey* and *SSCmac* | SK4SM is used to generate MAC for command responses. |

**Table 33: Authentication data of the COS for Package Contactless**

In addition to the Security Functional Requirements for the TOE defined in section 6.1 the TOE shall meet the following SFRs.

The security functionality for access control in case of contactless communication is covered already by the SFRs FDP_ACF.1/MF_DF, FDP_ACF.1/EF, FDP_ACF.1/TEF, FDP_ACF.1/SEF and FDP_ACF.1/KEY because the TSF shall implement the relevant security attributes described in Table 32 even if the Package Contactless is not included.

The TOE shall meet the requirement "Random number generation – RNG for PACE (FCS_RNG.1/PACE)" as specified below.

| | |
|---|---|
| **FCS_RNG.1/ PACE** | Random number generation – RNG for PACE |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FCS_RNG.1.1/ PACE | The TSF shall provide a hybrid physical[390] [391] random number generator **of RNG class PTG.3[392] ([5], [6]) for PACE protocol** that implements:<br>(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.<br>(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.<br>(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.<br>(PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.<br>(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.<br>(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.[393]. |
| FCS_RNG.1.2/ PACE | The TSF provide random ~~numbers~~ numbers[394] that meet<br>(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.<br>(PTG.3.8) The internal random numbers shall use PTRNG of class PTG.2 as random source for the post-processing.[395]. |

The TOE shall meet the requirement "Cryptographic operation – PACE secure messaging encryption (FCS_COP.1/PACE.PICC.ENC)" as specified below.

| | |
|---|---|
| **FCS_COP.1/ PACE.PICC.ENC** | Cryptographic operation – PACE secure messaging encryption |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/ PACE.PICC.ENC | The TSF shall perform decryption and encryption for secure messaging[396] in accordance with a specified cryptographic algorithm AES in CBC mode[397] and cryptographic key sizes 128 bit, 192 bit, 256 bit[398] [399] that meet the following: TR-03110 [16], COS specification [21][400]. |

*Application note 50*: This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH.PACE.PICC.

[390] [selection: ~~*physical, non-physical true, deterministic,*~~ *hybrid deterministic, hybrid physical*]
[391] [selection: *physical, non-physical true, deterministic, hybrid*]
[392] [selection: *DRG.4, PTG.3*]
[393] [assignment: *list of security capabilities of the selected RNG class*]
[394] [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*]
[395] [assignment: *defined quality metric of the selected RNG class*]
[396] [assignment: *list of cryptographic operations*]
[397] [assignment: *cryptographic algorithm*]
[398] [selection: *128 bit, 192 bit, 256 bit*]
[399] [assignment: *cryptographic key sizes*]
[400] [assignment: *list of standards*]

The TOE shall meet the requirement "Cryptographic operation – PACE secure messaging MAC (FCS_COP.1/PACE.PICC.MAC)" as specified below.

| | |
|---|---|
| **FCS_COP.1/ PACE.PICC.MAC** | Cryptographic operation – PACE secure messaging MAC |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/ PACE.PICC.MAC | The TSF shall perform MAC calculation for secure messaging[401] in accordance with a specified cryptographic algorithm CMAC[402] and cryptographic key sizes 128 bit, 192 bit, 256 bit[403] [404] that meet the following: TR-03110 [16], COS specification [21][405]. |

*Application note 51*: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH.PACE.PICC.

[401] [assignment: *list of cryptographic operations*]
[402] [assignment: *cryptographic algorithm*]
[403] [selection: *128 bit, 192 bit, 256 bit*]
[404] [assignment: *cryptographic key sizes*]
[405] [assignment: *list of standards*]

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

| | |
|---|---|
| **FCS_CKM.1/ DH.PACE.PICC** | Cryptographic key generation – DH by PACE |
| Hierarchical to: | No other components. |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution, or<br>FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.1.1/ DH.PACE.PICC | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [17] using the protocol id-PACE-ECDH-GM-AES-CBC-CMAC-128 with brainpoolP256r1, id-PACE-ECDH-GM-AES-CBC-CMAC-192 with brainpoolP384r1, id-PACE-ECDH-GM-AES-CBC-CMAC-256 with brainpoolP512r1[406] [407] and specified cryptographic key sizes 256 bit, 384 bit, 512 bit[408] [409] that meet the following: TR-03110 [16], TR-03111 [17][410]. |

*Application note 52*: The TOE exchanges a shared secret with the external entity during the PACE protocol, see [16]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [33]) or on the ECDH compliant to TR-03111 [17] (i.e. the elliptic curve cryptographic algorithm ECKA). The shared secret is used for deriving the AES session keys for message encryption and message authentication according to [16] for the TSF as required by FCS_COP.1/PACE.PICC.ENC and FCS_COP.1/PACE.PICC.MAC. FCS_CKM.1/DH.PACE.PICC implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to TR-03110 [16].

[406] [selection: *Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [17] using the protocol [selection: id-PACE-ECDH-GM-AES-CBC-CMAC-128 with brainpoolP256r1, id-PACE-ECDH-GM-AES-CBC-CMAC-192 with brainpoolP384r1, id-PACE-ECDH-GM-AES-CBC-CMAC-256 with brainpoolP512r1]*]

[407] [assignment: *cryptographic key generation algorithm*]

[408] [selection: *256 bit, 384 bit, 512 bit*]

[409] [assignment: *cryptographic key sizes*]

[410] [assignment: *list of standards*]

The TOE shall meet the requirement "Cryptographic key destruction – PACE (FCS_CKM.4/PACE.PICC)" as specified below.

| | |
|---|---|
| **FCS_CKM.4/ PACE.PICC** | Cryptographic key destruction – PACE |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] |
| FCS_CKM.4.1/ PACE.PICC | The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method erasure of the key[411] that meets the following: physical erasure of the key[412]. |

*Application note 53*: The TOE shall destroy the encryption session keys and the message authentication keys for PACE protocol after reset or termination of the secure messaging (or trusted channel) session 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.

[411] [assignment: *cryptographic key destruction method*]
[412] [assignment: *list of standards*]

The TOE shall meet the requirement "Timing of identification – PACE (FIA_UID.1/PACE)" as specified below.

| | |
|---|---|
| **FIA_UID.1/ PACE** | Timing of identification – PACE |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UAU.1 Timing of authentication |
| FIA_UID.1.1/ PACE | The TSF shall allow<br>(1) reading the ATS,<br>(2) to establish a communication channel,<br>(3) MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, SELECT, READ BINARY (EF.CardAccess), GENERAL AUTHENTICATE<br>(4) commands with access control rule ALWAYS for the current life cycle status and depending on the interface[413].<br>on behalf of the user to be performed before the user is identified. |
| FIA_UID.1.2/ PACE | The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. |

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

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

| | |
|---|---|
| **FIA_UAU.1/ PACE** | Timing of authentication – PACE |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UID.1 Timing of identification |
| FIA_UAU.1.1/ PACE | The TSF shall allow<br>(1) reading the ATS,<br>(2) to establish a communication channel,<br>(3) actions allowed according to FIA_UID.1/PACE and FIA_UAU.1,<br>(4) none[414].<br>on behalf of the user to be performed before the user is authenticated. |
| FIA_UAU.1.2/ PACE | The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. |

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

| | |
|---|---|
| **FIA_UAU.4/ PACE.PICC** | Single-use authentication mechanisms – PACE/PICC |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_UAU.4.1/ PACE.PICC | The TSF shall prevent reuse of verification authentication data related to<br>(1) PACE Protocol in PCD role according to TR-03116-1 [19], COS specification [21][415]. |

[414] [assignment: *list of TSF-mediated actions*]
[415] [assignment: *identified authentication mechanism(s)*]

The TOE shall meet the requirement "Multiple authentication mechanisms – PACE/PICC (FIA_UAU.5/PACE.PICC)" as specified below.

| | |
|---|---|
| **FIA_UAU.5/ PACE.PICC** | Multiple authentication mechanisms – PACE/PICC |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_UAU.5.1/ PACE.PICC | The TSF shall provide<br>(1) PACE protocol in PICC role according to [16] and [20] using command GENERAL AUTHENTICATE,<br>(2) secure messaging in MAC-ENC mode using PACE session keys according to [20], section 13, and [16], Part 3, in PICC role[416]<br>to support user authentication. |
| FIA_UAU.5.2/ PACE.PICC | The TSF shall authenticate any user's claimed identity according to the PACE protocol as PICC is used for authentication of the device using the PACE protocol in PCD role and secure messaging in MAC-ENC mode using PACE session keys is used to authenticate its commands[417]. |

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

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

The TOE shall meet the requirement "Re-authenticating – PACE/PICC (FIA_UAU.6/PACE.PICC)" as specified below.

| | |
|---|---|
| **FIA_UAU.6/ PACE.PICC** | Re-authenticating – PACE/PICC |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_UAU.6.1/ PACE.PICC | The TSF shall re-authenticate the user under the conditions after successful run of the PACE protocol as PICC each command received by the TOE shall be verified as being sent by the authenticated PCD[418]. |

*Application note 54*: The TOE running the PACE protocol as PICC specified in [26] checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE.PICC.ENC and FCS_COP.1/PACE.PICC.MAC for further details) and sends all responses secure messaging after successful PACE authentication. The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal (see FIA_UAU.5/PACE.PICC).

The TOE shall meet the requirement "User-subject binding – PACE/PICC (FIA_USB.1/PACE.PICC)" as specified below.

[418] [assignment: *list of conditions under which re-authentication is required*]

| | |
|---|---|
| **FIA_USB.1/ PACE.PICC** | User-subject binding – PACE/PICC |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_ATD.1 User attribute definition |
| FIA_USB.1.1/ PACE.PICC | The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: The authentication state for the device using PACE protocol in PCD role with<br>(1) *keyIdentifier* of the used SCCO in the *globalSecurityList* if SCCO was in MF or in *dfSpecificSecurityList* if the SCCO was in the *respective folder,*<br>(2) *SK4SM referenced* in *macKey* and *SSCmac*[419]. |
| FIA_USB.1.2/ PACE.PICC | The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: see FIA_USB.1[420]. |
| FIA_USB.1.3/ PACE.PICC | The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:<br>(1) The authentication state for the device after successful authentication using PACE protocol in PCD role is set to "authenticated" and<br>a. *keyIdentifier* of the used SCCO in the *globalSecurityList* if SCCO was in MF or in *dfSpecificSecurityList* if the SCCO was in the respective DF,<br>b. the authentication reference data SK4SM is stored in *macKey* and *SSCmac*.<br>(2) If an authentication attempt using PACE protocol in PCD role failed<br>a. Executing GENERAL AUTHENTICATE for PACE Version 2 [16],<br>b. receiving commands failing the MAC verification or encryption defined for secure messaging, |

[419] [assignment: *list of user security attributes*]
[420] [assignment: *rules for the initial association of attributes*]

c. receiving messages violation MAC verification or encryption defined for trusted channel established with PACE,

the authentication state for the specific context of SCCO has to be set to "not authenticated" (i.e. the element in *globalSecurityList* respective in the *dfSpecificSecurityList* and the SK4SM are deleted)[421].

The TOE shall meet the requirement "Subset residual information protection – PACE/PICC (FDP_RIP.1/PACE.PICC)" as specified below.

| | |
|---|---|
| **FDP_RIP.1/ PACE.PICC** | Subset residual information protection – PACE/PICC |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FDP_RIP.1.1/ PACE.PICC | The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[422] the following objects:<br>(1) session keys (immediately after closing related communication session),<br>(2) any ephemeral secret having been generated during DH key exchange,<br>(3) PACE state machine, Nonce[423] [424]. |

[421] [assignment: *rules for the changing of attributes*]
[422] [selection: *allocation of the resource to, deallocation of the resource from*]
[423] [assignment: *list of additional objects*]
[424] [assignment: *list of objects*]

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

| | |
|---|---|
| **FDP_UCT.1/ PACE** | Basic data exchange confidentiality – PACE |
| Hierarchical to: | No other components. |
| Dependencies: | [FTP_ITC.1 Inter-TSF trusted channel, or<br>FTP_TRP.1 Trusted path]<br>[FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control] |
| FDP_UCT.1.1/ PACE | 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[425] to transmit and receive[426] user data in a manner protected from 234nitializati disclosure. |

[425] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[426] [selection: *transmit, receive*]

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

| | |
|---|---|
| **FDP_UIT.1/ PACE** | Data exchange integrity – PACE |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>[FTP_ITC.1 Inter-TSF trusted channel, or<br>FTP_TRP.1 Trusted path] |
| FDP_UIT.1.1/ PACE | 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[427] to transmit and receive[428] user data in a manner protected from modification, deletion, insertion, and replay[429] errors. |
| FDP_UIT.1.2/ PACE | The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, and replay[430] has occurred. |

[427] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[428] [selection: *transmit, receive*]
[429] [selection: *modification, deletion, insertion, replay*]
[430] [selection: *modification, deletion, insertion, replay*]

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

| | |
|---|---|
| **FTP_ITC.1/ PACE.PICC** | Inter-TSF trusted channel – PACE/PICC |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FTP_ITC.1.1/ PACE.PICC | 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/ PACE.PICC | The TSF shall permit another trusted IT product[431] to initiate communication via the trusted channel. |
| FTP_ITC.1.3/ PACE.PICC | The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for data exchange between the TOE and the external user if required by access control rule of the object in the object system[432]. |

*Application note 55*: The trusted IT product is the terminal. In FTP_ITC.1.3/PACE.PICC, the word "initiate" **in [2]** has been changed **by the PP author** to "enforce" because the TOE is a passive device that can not initiate the communication, but can enforce secured communication if required for an object in the object system and shutdown the trusted channel after integrity violation of a received command.

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

The TOE shall meet the requirement "Security roles – PACE/PICC (FMT_SMR.1/PACE.PICC)" as specified below.

| | |
|---|---|
| **FMT_SMR.1/ PACE.PICC** | Security roles – PACE/PICC |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UID.1 Timing of identification |
| FMT_SMR.1.1/ PACE.PICC | The TSF shall maintain the roles<br>(1) the roles defined in FMT_SMR.1,<br>(2) PACE authenticated terminal,<br>(3) none[433] [434]. |
| FMT_SMR.1.2/ PACE.PICC | The TSF shall be able to associate users with roles. |

The TOE shall meet the requirement "Management of TSF data – PACE/PICC (FMT_MTD.1/PACE.PICC)" as specified below.

[433] [assignment: *additional authorised identified roles*]
[434] [assignment: *the authorised identified roles*]

| | |
|---|---|
| **FMT_MTD.1/ PACE.PICC** | Management of TSF data – PACE/PICC |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |
| FMT_MTD.1.1/ PACE.PICC | The TSF shall restrict the ability to read[435] [436] the<br>(1) SCCO used for PACE protocol in PICC role,<br>(2) session keys of secure messaging channel established using PACE protocol in PICC role[437]<br>to none[438]. |

*Application note 56*: The iteration defined an additional rule for managing the SCCO in a special case of the PACE protocol (i.e. the PICC role). The derived session keys SM4SM shall be kept secret.

The TOE shall meet the requirement "Export of TSF data – PACE (FPT_ITE.2/PACE)" as specified below.

[435] [assignment: *other operations*]
[436] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[437] [assignment: *list of TSF data*]
[438] [assignment: *the authorised identified roles*]

| | |
|---|---|
| **FPT_ITE.2/ PACE** | Export of TSF data – PACE |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_ITE.2.1/ PACE | The TOE shall export<br>(1) the public TSF data as defined in FPT_ITE.2.1[439]<br>given the following conditions<br>(1) conditions as defined in FPT_ITE.2.1,<br>(2) no export of the SCCO[440]. |
| FPT_ITE.2.2/ PACE | The TSF shall use Idemia proprietary encoding rules that meet the requirements of the Technical Guideline BSI TR-03143 [20] (so that the exported data can be transformed by the Idemia wrapper implementation into the specified coding format of the Gematik)[441] for the exported data. |

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

| | |
|---|---|
| **FIA_ATD.1/ PACE** | User attribute definition – PACE |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_ATD.1.1/ PACE | The TSF shall maintain the following list of security attributes belonging to individual users:<br>(1) for users defined in FIA_ATD.1,<br>(2) additionally for device: authentication state gained with SCCO[442]. |

[439] [assignment: *list of types of TSF data*]
[440] [assignment: *conditions for export*]
[441] [assignment: *list of encoding rules to be applied by TSF*]
[442] [assignment: *list of security attributes*]

The TOE shall meet the requirement “TOE emanation – PACE/PICC (FPT_EMS.1/PACE.PICC)” as specified below (CC Part 2 extended).

| | |
|---|---|
| **FPT_EMS.1/ PACE.PICC** | TOE emanation – PACE/PICC |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_EMS.1.1/ PACE.PICC | The TOE shall not emit information on IC power consumption, information on command execution time, information on electromagnetic emanations[443] in excess of non-useful information[444] enabling access to<br>(1) Symmetric Card Connection Object (SCCO),<br>(2) PACE session keys,<br>(3) any ephemeral secret having been generated during DH key exchange,<br>(4) any object listed in FPT_EMS.1,<br>(5) no other TSF data[445] [446]<br>and no user data[447]. |
| FPT_EMS.1.2/ PACE.PICC | The TSF shall ensure any users[448] are unable to use the following interface the contactless interface and circuit contacts[449] to gain access to<br>(1) Symmetric Card Connection Object (SCCO),<br>(2) PACE session keys,<br>(3) any ephemeral secret having been generated during DH key exchange,<br>(4) any object listed in FPT_EMS.1,<br>(5) no other TSF data[450] [451]<br>and no user data[452]. |

## 7.5 Security Requirements Rationale for Package Contactless

The following table provides an overview for Security Functional Requirements coverage also giving an evidence for *sufficiency* and *necessity* of the SFRs chosen in the Package Contactless.

[443] [assignment: *types of emissions*]
[444] [assignment: *specified limits*]

| | O.Integrity | O.Confidentiality | O.Resp-COS | O.TSFDataExport | O.Authentication | O.AccessControl | O.KeyManagement | O.Crypto | O.PACE_Chip |
|---|---|---|---|---|---|---|---|---|---|
| FCS_CKM.1/DH.PACE.PICC | | | | | | | | x | x |
| FCS_CKM.4/PACE.PICC | | | | | | | | x | x |
| FCS_COP.1/PACE.PICC.ENC | | | | | | | | x | x |
| FCS_COP.1/PACE.PICC.MAC | | | | | | | | x | x |
| FCS_RNG.1/PACE | | | | | | | x | | x |
| FDP_RIP.1/PACE.PICC | | x | | | | | | | x |
| FDP_UCT.1/PACE | | | | | | | | | x |
| FDP_UIT.1/PACE | | | | | | | | | x |
| FIA_ATD.1/PACE | | | | | x | x | | | x |
| FIA_UAU.1/PACE | | | | | x | x | | | x |
| FIA_UAU.4/PACE.PICC | | | | | x | x | | | x |
| FIA_UAU.5/PACE.PICC | | | | | x | | | | x |
| FIA_UAU.6/PACE.PICC | | | | | x | | | | x |
| FIA_UID.1/PACE | | | | | x | x | | | x |
| FIA_USB.1/PACE.PICC | | | | | x | x | | | x |

445 [assignment: *list of additional types of TSF data*]
446 [assignment: *list of types of TSF data*]
447 [assignment: *list of types of user data*]
448 [assignment*: type of users*]
449 [assignment: *type of connection*]
450 [assignment: *list of additional types of TSF data*]
451 [assignment: *list of types of TSF data*]
452 [assignment: *list of types of user data*]

| | O.Integrity | O.Confidentiality | O.Resp-COS | O.TSFDataExport | O.Authentication | O.AccessControl | O.KeyManagement | O.Crypto | O.PACE_Chip |
|---|---|---|---|---|---|---|---|---|---|
| FMT_MTD.1/PACE.PICC | | x | | | x | | | | x |
| FMT_SMR.1/PACE.PICC | | | | | x | x | | | x |
| FPT_EMS.1/PACE.PICC | | x | | | x | | | | x |
| FPT_ITE.2/PACE | | | | x | | | | | x |
| FTP_ITC.1/PACE.PICC | | | | | x | x | | | x |

**Table 34: Mapping between Security Objectives for the TOE and SFRs for Package Contactless**

Table 34 above should be taken as extension of Table 29 in order to cover the whole set of Security Objectives. Hence, the mappings between Security Objectives and SFRs in the table above are used as *additional* mappings to address the corresponding Security Objectives.

All SFRs of the Package Contactless are implementing security functionality for the Security Objective **O.PACE_Chip**.

The Security Objective **O.Confidentiality** "Confidentiality of internal data" requires the protection of the confidentiality of sensitive User Data and TSF Data. The SFR FDP_RIP.1/PACE.PICC addresses this Security Objective as it requires that residual information regarding sensitive data in previously used resources will not be available after its usage. Further, the SFR FMT_MTD.1/PACE.PICC requires that the TSF denies everyone the read access to dedicated confidential TSF Data as defined in the SFR. The SFR FPT_EMS.1/PACE.PICC protects the confidential authentication data against compromise.

The Security Objective **O.TSFDataExport** "Support of TSF Data export" requires the correct export of TSF Data of the object system excluding confidential TSF Data. The SFR FPT_ITE.2/PACE requires the ability of the TOE to export public TSF Data and defines conditions for exporting these TSF Data.

The Security Objective **O.Authentication** "Authentication of external entities" requires the support of authentication of human users and external devices as well as the ability

of the TSF to authenticate itself. The successful authentication using PACE protocol sets the *keyIdentifier* in the *globalSecurityList* or *dfSpecificSecurityList*. This Security Objective is addressed by the following SFRs:

- FIA_ATD.1/PACE requires that the TSF maintains dedicated security attributes belonging to individual users.
- FIA_USB.1/PACE.PICC requires that the TSF associates the security attribute "authentication state of the PACE terminal" with subjects acting on behalf of that user. Also, the TSF shall enforce rules governing changes of these security attributes by the implementation of commands that perform these changes.
- FIA_UID.1/PACE requires the processing of dedicated actions before a user is identified. Any other actions shall require user identification.
- FIA_UAU.1/PACE requires the processing of dedicated actions before a user is authenticated. Any other actions shall require user authentication.
- FIA_UAU.4/PACE.PICC requires the prevention of reuse of authentication data related to the PACE protocol.
- FIA_UAU.5/PACE.PICC requires the TSF to support the PACE protocol and secure messaging based on PACE session keys. Further, the TSF shall authenticate all users based on the PACE protocol.
- FIA_UAU.6/PACE.PICC requires the TSF to support re-authentication of users under dedicated conditions as given in the SFR.
- FPT_EMS.1/PACE.PICC requires that the TOE does not emit any information of sensitive User Data and TSF Data by emissions and via circuit interfaces.
- FMT_MTD.1/PACE.PICC requires that the TSF prevents SCCO and session keys from reading.
- FTP_ITC.1/PACE.PICC requires that the TSF provides a communication channel between itself and another trusted IT product established by PACE. The channel provides assured identification of its end points and protection of the channel data against modification and disclosure.
- FMT_SMR.1/PACE.PICC requires that the TSF maintains roles including PACE authenticated terminal and associates users with roles.

The Security Objective **O.AccessControl** "Access Control for Objects" requires the enforcement of an access control policy to restricted objects and devices. Further, the management functionality for the access policy is required. The security attribute of the subject *keyIdentifier* in the *globalSecurityList* or *dfSpecificSecurityList* is already described in the access control SFR. This Security Objective is addressed by the following SFRs:

- FIA_UID.1/PACE defines the TSF mediated actions alloed before a user is identified. Any other actions shall require user identification.
- FIA_UAU.1/PACE defines the TSF mediated actions before a user is authenticated. Any other actions shall require user authentication.

- FIA_UAU.4/PACE.PICC requires the prevention of reuse of authentication data related to the PACE protocol.
- FIA_ATD.1/PACE requires that the TSF maintains dedicated security attributes belonging to individual users.
- FIA_USB.1/PACE.PICC requires that the TSF associates the security attribute "authentication state of the PACE terminal" with subjects acting on behalf of that user. Also, the TSF shall enforce rules governing changes of these security attributes by the implementation of commands that perform these changes.
- FMT_SMR.1/PACE requires that the TSF maintains roles and associates users with roles.
- FTP_ITC.1/PACE.PICC requires that the TSF provides a communication channel between itself and another trusted IT product established by PACE. The channel provides assured identification of its end points and protection of the channel data against modification and disclosure.

The Security Objective **O.KeyManagement** "Generation and import of keys" requires the ability of the TSF to secure generation, import, distribution, access control and destruction of cryptographic keys. Also, the TSF is required to support the import and export of public keys. This Security Objective is addressed by the SFR FCS_RNG.1/PACE.PICC that requires that the TSF provides a random number generator of class DRG.4 or PTG.3.

The Security Objective **O.Crypto** "Cryptographic functions" requires the ability of the TSF to implement secure cryptographic algorithms. This Security Objective is addressed by the following SFRs that provide additional cryptographic operations:

- FCS_CKM.1/DH.PACE.PICC requires that the TSF generate cryptographic keys with the Diffie-Hellman-Protocol or ECDH.
- FCS_CKM.4/PACE.PICC requires that the TSF destroys cryptographic keys in accordance with a given specific key destruction method.
- FCS_COP.1/PACE.PICC.ENC requires that the TSF provides decryption and encryption using AES to be used for secure messaging.
- FCS_COP.1/PACE.PICC.MAC requires that the TSF provides computation and verification of cryptographic checksums using the CMAC algorithm to be used for secure messaging.

The Security Objective **O.PACE_Chip** "Protection of contactless communication with PACE/PICC" requires the TOE support of the chip part of the PACE protocol in order to protect the confidentiality and the integrity of data communicated through the contactless interface of the TOE. All SFRs, i.e. FCS_CKM.1/DH.PACE.PICC, FCS_CKM.4/PACE.PICC, FCS_COP.1/PACE.PICC.ENC, FCS_COP.1/PACE.PICC.MAC, FCS_RNG.1/PACE, FDP_RIP.1/PACE.PICC, FDP_UCT.1/PACE, FDP_UIT.1/PACE, FIA_ATD.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE.PICC, FIA_UAU.5/PACE.PICC, FIA_UAU.6/PACE.PICC, FIA_UID.1/PACE, FIA_USB.1/PACE.PICC, FMT_MTD.1/PACE.-

PICC, FMT_SMR.1/PACE.PICC, FPT_EMS.1/PACE.PICC, FPT_ITE.2/PACE, FTP_ITC.1/-PACE.PICC, are defined to implement the Security Objective specific for the Package Contactless.

The following table lists the required dependencies of the SFRs of this PP Package and gives the concrete SFRs from this document which fulfil the required dependencies. Hereby, Table 35 should be taken as extension of Table 30 in order to cover all dependencies.

| SFR | dependent on | fulfilled by |
|---|---|---|
| FCS_CKM.1/ DH.PACE.PICC | [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction | FCS_COP.1/PACE.PICC.ENC, FCS_COP.1/PACE.PICC.MAC, FCS_CKM.4/PACE.PICC |
| FCS_CKM.4/ PACE.PICC | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] | FCS_CKM.1/DH.PACE.PICC |
| FCS_COP.1/ PACE.PICC.ENC | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction | FCS_CKM.1/DH.PACE.PICC, FCS_CKM.4/PACE.PICC |
| FCS_COP.1/ PACE.PICC.MAC | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction | FCS_CKM.1/DH.PACE.PICC, FCS_CKM.4/PACE.PICC |
| FCS_RNG.1/PACE | No dependencies. | n. a. |
| FDP_RIP.1/ PACE.PICC | No dependencies. | n. a. |
| FDP_RIP.1/PACE | No dependencies. | n. a. |
| FDP_UCT.1/PACE | [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access | FTP_ITC.1/PACE, FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, |

| SFR | dependent on | fulfilled by |
|---|---|---|
| | control, or FDP_IFC.1 Subset information flow control] | FDP_ACC.1/SEF, FDP_ACC.1/KEY |
| FDP_UIT.1/PACE | [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] | FTP_ITC.1/PACE, FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY |
| FIA_ATD.1/PACE | No dependencies. | n. a. |
| FIA_UAU.1/PACE | FIA_UID.1 Timing of identification | FIA_UID.1/PACE |
| FIA_UAU.4/ PACE.PICC | No dependencies. | n. a. |
| FIA_UAU.5/ PACE.PICC | No dependencies. | n. a. |
| FIA_UAU.6/ PACE.PICC | No dependencies. | n. a. |
| FIA_UID.1/PACE | FIA_UAU.1 Timing of authentication | FIA_UAU.1/PACE |
| FIA_USB.1/ PACE.PICC | FIA_ATD.1 User attribute definition | FIA_ATD.1/PACE |
| FMT_MTD.1/PACE | FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions | FMT_SMR.1/PACE, FMT_SMF.1 |
| FMT_SMR.1/ PACE.PICC | FIA_UID.1 Timing of identification | FIA_UID.1/PACE |
| FMT_SMR.1/PACE | FIA_UID.1 Timing of identification | FIA_UID.1/PACE |
| FPT_EMS.1/ PACE.PICC | No dependencies. | n. a. |
| FPT_ITE.2/ PACE | No dependencies. | n. a. |
| FTP_ITC.1/ PACE.PICC | No dependencies. | n. a. |
| FTP_ITC.1/PACE | No dependencies. | n. a. |

**Table 35: Dependencies of the SFRs for Package Contactless**

# 8 Package Logical Channel

The COS supports additional functionality for logical channels according to [21]. This section defines the Package Logical Channel as used by the ST author.

## 8.1 TOE Overview for Package Logical Channel

In addition to the TOE definition given in section 1.2.1 “TOE definition and operational usage” the TOE is equipped with additional logic channels. The extension is purely functional.

## 8.2 Security Problem Definition for Package Logical Channel

### 8.2.1 Assets and External Entities

**Assets**

The assets do not differ from the assets defined in section 3.1.

**Subjects and external entities**

There are no additional external entities and subjects for the Package Logical Channel beyond those already defined in section 3.1.

### 8.2.2 Threats

There are no additional Threats for the Package Logical Channel beyond the Threats already defined in section 3.2.

### 8.2.3 Organisational Security Policies

There is a further Organisational Security Policy for the Package Logical Channel additionally to those already defined in section 3.3.

| | |
|---|---|
| **OSP.LogicalChannel** | **Logical channel** |

The TOE supports and the operational environment uses logical channels bound to independent subjects.

*Application note 64:* The COS specification [21] describes the concept of logical channels in section 12.

### 8.2.4 Assumptions

There are no additional Assumptions for the Package Logical Channel beyond the Assumptions already defined in section 3.4.

## 8.3 Security Objectives for Package Logical Channel

The Security Objectives for the TOE (section 4.1) and the Security Objectives for the Operational Environment (section 4.2) are supplemented for the Package Logical Channel. Therefore the Security Objective Rationale (section 4.3) is supplemented as well.

The TOE shall fulfil the Security Objective "Support of more than one logical channel (O.LogicalChannel)" as specified below.

**O.LogicalChannel** **Support of more than one logical channel**

The TOE supports more than one logical channel each bound to an independent subject.

The operational environment of the TOE shall fulfil the Security Objective "Use of logical channels (OE.LogicalChannel)" as specified below.

**OE.LogicalChannel** **Use of logical channels**

The operational environment manages logical channels bound to independent subjects for running independent processes at the same time.

The Security Objectives O.LogicalChannel and OE.LogicalChannel implement the OSP.LogicalChannel.

## 8.4 Security Requirements for Package Logical Channel

In addition to the Security Functional Requirements for the TOE defined in section 6.1 the TOE shall meet the following SFRs.

The TOE shall meet the requirement "User-subject binding – Logical channel (FIA_USB.1/LC)" as specified below.

| | |
|---|---|
| **FIA_USB.1/LC** | User-subject binding – Logical channel |
| Hierarchical to: | No other components. |
| Dependencies: | FIA_ATD.1 User attribute definition |
| FIA_USB.1.1/LC | The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:<br>(1) The authentication state for the context as specified in FIA_USB.1.<br>(2) The authentication state for a context is bound to the logical channel the authentication took place[453]. |
| FIA_USB.1.2/LC | The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:<br>(1) If a new logical channel is opened the authentication state is "not authenticated" for all contexts within that logical channel[454]. |
| FIA_USB.1.3/LC | The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:<br>(1) Every logical channel has its own context. The rules as specified in FIA_USB.1.3 for the context shall be enforced for each logical channel separately.<br>(2) After a logical channel is closed or reset, e.g. by the use of a MANAGE CHANNEL command, the authentication state for all contexts within the closed logical channel must be "not authenticated".<br>(3) The execution of a DELETE command has to be rejected if more than one channel is open.<br>(4) none[455] [456]. |

[453] [assignment: *list of user security attributes*]
[454] [assignment: *rules for the initial association of attributes*]
[455] [assignment: *rules for the changing of attributes*]

The TOE shall meet the requirement "Subset access control – Logical channel (FDP_ACC.1/LC)" as specified below.

| | |
|---|---|
| **FDP_ACC.1/LC** | Subset access control – Logical channel |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACF.1 Security attribute based access control |
| FDP_ACC.1.1/LC | The TSF shall enforce the Logical Channel SFP[457] on<br>(1) the subjects FDP_ACF.1/EF and FDP_ACF.1/ MF_DF,<br>(2) the objects<br>a. logical channel,<br>b. objects as defined in FDP_ACF.1/EF,<br>c. objects as defined in FDP_ACF.1/MF_DF,<br>(3) the operation by command following<br>a. command SELECT,<br>b. command MANAGE CHANNEL to open, reset and close a logical channel[458]. |

The TOE shall meet the requirement "Security attribute based access control – Logical channel (FDP_ACF.1/LC)" as specified below.

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

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

[458] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

| | |
|---|---|
| **FDP_ACF.1/LC** | Security attribute based access control – Logical channel |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACC.1 Subset access control<br>FMT_MSA.3 Static attribute initialisation |
| FDP_ACF.1.1/LC | The TSF shall enforce the Logical Channel SFP[459] to objects based on the following<br>(1) the subjects as defined in FDP_ACF.1/EF and FDP_ACF.1/ MF_DF with security attribute "logical channel",<br>(2) the objects<br>a. logical channel with channel number,<br>b. as defined in FDP_ACF.1/EF and FDP_ACF.1/ MF_DF with security attribute "shareable"[460]. |
| FDP_ACF.1.2/LC | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:<br>(1) The command MANAGE CHANNEL is ALWAYS allowed[461].<br>(2) A subject is allowed to open, reset or close a logical channel with channel number higher than 1 if a logical channel is available and the subject fulfils the access conditions for command MANAGE CHANNEL with the corresponding parameter P1.<br>(3) A subject is allowed to select an object as current object in more than one logical channel if its security attribute "shareable" is set to *TRUE*[462]. |
| FDP_ACF.1.3/LC | The TSF shall explicitly 254nitializ access of subjects to objects based on the following additional rules: none[463]. |
| FDP_ACF.1.4/LC | The TSF shall explicitly deny access of subjects to objects based on the following additional rules:<br>(1) if the security attribute of an object is set to "not shareable" this object is not accessible as current object in more than one logical channel[464]. |

*Application note 65:* The COS specification [21] claims that the security attribute "shareable" is always TRUE.

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

The TOE shall meet the requirement "Static attribute 255nitialization – Logical channel (FMT_MSA.3)" as specified below.

| | |
|---|---|
| **FMT_MSA.3/LC** | Static attribute 255nitialization – Logical channel |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_MSA.1 Management of security attributes<br>FMT_SMR.1 Security roles |
| FMT_MSA.3.1/LC | The TSF shall enforce the Logical Channel SFP[465] to provide restrictive[466] default values for security attributes that are used to enforce the SFP. **After a logical channel is opened the security attributes of the subject associated with this logical channel are set as follows:**<br>(1) ***currentFolder* is root,**<br>(2) ***keyReferenceList, globalSecurityList, globalPasswordList, dfSpecificSecurityList, dfSpecificPasswordList bitSecurityList* are empty,**<br>(3) ***SessionkeyContext.flagSessionEnabled* is set to *noSK*,**<br>(4) ***seIdentifier* is #1,**<br>(5) ***currentFile* is undefined.** |
| FMT_MSA.3.2/LC | The TSF shall allow the subjects allowed to execute the command LOAD APPLICATION[467] to specify alternative initial values to override the default values when an object or information is created. |

[460] [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*]
[461] [selection: *ALWAYS allowed, [assignment: supported access control rules]*]
[462] [assignment*: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[463] [assignment*: rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[464] [assignment*: rules, based on security attributes, that explicitly deny access of subjects to objects*]
[465] [assignment: *access control SFP, information flow control SFP*]
[466] [selection, choose one of*: restrictive, permissive, [assignment: other property]*]
[467] [assignment: *the authorised identified roles*]

## 8.5 Security Requirements Rationale for Package Logical Channel

The following table provides an overview for Security Functional Requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen in the Package Logical Channel.

| | O.Integrity | O.Confidentiality | O.Resp-COS | O.TSFDataExport | O.Authentication | O.AccessControl | O.KeyManagement | O.Crypto | O.SecureMessaging | O.LogicalChannel |
|---|---|---|---|---|---|---|---|---|---|---|
| FCS_RNG.1/GR | | | | | | | | | | x |
| FIA_USB.1/LC | | | | | | x | | | | x |
| FDP_ACC.1/LC | | | | | | x | | | | x |
| FDP_ACF.1/LC | | | | | | x | | | | x |
| FMT_MSA.3/LC | | | | | | x | | | | x |

**Table 36: Mapping between Security Objectives for the TOE and SFRs for Package Logical Channel**

Table 36 above should be taken as extension of Table 29 in order to cover the whole set of Security Objectives. Hence, the mappings between Security Objectives and SFRs in the table above are used as *additional* mappings to address the corresponding Security Objectives. Please note that the SFR FCS_RNG.1/GR is already defined in the PP mandatory part section 6.1.7 and mapped to the TOES's Security Objectives in section 6.3.1, but within this Package Logical Channel an additional mapping to the Package-specific Security Objective O.LogicalChannel is necessary.

The Security Objectives **O.AccessControl** "Access Control for Objects" and **O.LogicalChannel** "Support of more than one logical channel" require the enforcement of an access control policy to restricted objects and devices in more than one logical channel. Further, the management functionality for the access policy is required. These Security Objectives are addressed by the following SFRs:

- FCS_RNG.1/GR provides secure random numbers for external entities, whereby these are the same as for using more than one logical channel.
- FIA_USB.1/LC requires that the TSF associates the user authentication state with subjects acting on behalf of that user. Also, the TSF shall enforce rules governing

changes of these security attributes by the implementation of commands that perform these changes.

- FDP_ACC.1/LC requires that the TSF enforces a logical channel control policy to restrict operations on dedicated EF and DF objects performed by subjects of the TOE.
- FDP_ACF.1/LC requires that the TSF enforce a logical channel control policy to restrict operations on dedicated EF and DF objects based on a set of rules defined in the SFR. Also, the TSF is required to deny access to dedicated EF and DF objects in case that the security attribute of the object is set to "not shareable".
- FMT_MSA.3/LC requires that the TSF assign restrictive security attributes to the subjects of new opened logical channel.

The following table lists the required dependencies of the SFRs of this PP Package and gives the concrete SFRs from this document which fulfil the required dependencies. Hereby, Table 37 should be taken as extension of Table 30 in order to cover all dependencies.

| SFR | dependent on | fulfilled by |
|---|---|---|
| FIA_USB.1/LC | FIA_ATD.1 User attribute definition | FIA_ATD.1 |
| FDP_ACC.1/LC | FDP_ACF.1 Security attribute based access control | FDP_ACF.1/LC |
| FDP_ACF.1/LC | FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation | FDP_ACC.1/LC, FMT_MSA.3 |
| FMT_MSA.3/LC | FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles | FMT_MSA.1/Life, FMT_MSA.1/PIN, FMT_MSA.1/Auth, FMT_SMR.1 |

**Table 37: Dependencies of the SFRs for Package Logical Channel**

# 9 Package RSA Key Generation

The COS supports additional cryptographic functionality related to RSA key generation according to Option_RSA_KeyGeneration in [21]. This section defines the Package RSA Key Generation as used by the ST author.

## 9.1 TOE Overview for Package RSA Key Generation

In addition to the TOE definition given in section 1.2.1 “TOE definition and operational usage” the TOE is equipped with further cryptographic functionality related to RSA key generation by the TOE.

## 9.2 Security Problem Definition for Package RSA Key Generation

### 9.2.1 Assets and External Entities

**Assets**

The assets do not differ from the assets defined in section 3.1.

**Subjects and external entities**

There are no additional external entities and subjects for the Package RSA Key Generation beyond those already defined in section 3.1. However, their scope is widened in view of the RSA key generation functionality according to Option_RSA_KeyGeneration in [21], i.e. the subjects and external entities described in section 3.1 address and cover now as well the RSA key generation functionality.

### 9.2.2 Threats

There are no additional Threats for the Package RSA Key Generation beyond the Threats already defined in section 3.2. However, their scope is widened in view of the RSA key generation functionality according to Option_RSA_KeyGeneration in [21], i.e. the Threats described in section 3.2 address and cover now as well the RSA key generation functionality.

### 9.2.3 Organisational Security Policies

There are no additional Organisational Security Policies for the Package RSA Key Generation beyond the Organisational Security Policies already defined in section 3.3. However, their scope is widened in view of the RSA key generation functionality according to Option_RSA_KeyGeneration in [21], i.e. the Organisational Security Policies described in section 3.3 address and cover now as well the RSA key generation functionality.

### 9.2.4 Assumptions

There are no additional Assumptions for the Package RSA Key Generation beyond the Assumptions already defined in section 3.4. However, their scope is widened in view of the RSA key generation functionality according to Option_RSA_KeyGeneration in [21], i.e. the Assumptions described in section 3.4 address and cover now as well the RSA key generation functionality.

## 9.3 Security Objectives for Package RSA Key Generation

There are no additional Security Objectives for the TOE and no additional Security Objectives for the Operational Environment of the TOE for the Package RSA Key Generation beyond the Security Objectives already defined in sections 4.1 and 4.2. However, their scope is widened in view of the RSA key generation functionality according to Option_RSA_KeyGeneration in [21], i.e. the Security Objectives described in the sections 4.1 and 4.2 address and cover now as well the RSA key generation functionality.

## 9.4 Security Requirements for Package RSA Key Generation

All Security Functional Requirements (SFRs) for the TOE defined in section 6.1 are taken over to the Package RSA Key Generation. However, their scope is widened to the RSA key generation functionality according to Option_RSA_KeyGeneration in [21], i.e. the SFRs set up in the sections 6.1.4, 6.1.5, 6.1.6 and 6.1.7 hold now as well for the RSA keys generated by the TOE.

In addition, the TOE shall meet the following SFR in order to address the additional RSA key generation functionality according to Option_RSA_KeyGeneration in [21].

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

| | |
|---|---|
| **FCS_CKM.1/RSA** | Cryptographic key generation – RSA key generation |
| Hierarchical to: | No other components. |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution, or<br>FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.1.1/RSA | The TSF shall generate cryptographic RSA keys in accordance with a specified cryptographic key generation algorithm RSA Key Generation (with CRT parameters)[468] and specified cryptographic key sizes 2048 bit and 3072 bit modulus length[469] that meet the following: Infineon/Idemia-proprietary algorithm / implementation, whereby the generated keys are in conformance with PKCS#1 [34], chapters 3.1, 3.2 and IEEE 1363 [201], chapter 8.1.3.1, TR-03116-1 [19][470]. |

*Application note 66*: The COS specification [21] specifies the command GENERATE ASYMMETRIC KEY PAIR for the generation of RSA key pairs as an option for the TOE implementation. The TOE ~~may~~ **supports** the generation of asymmetric key pairs for the following operations:

- qualified electronic signatures,
- authentication of external entities,
- document cipher key decipherment.

The ST author shall perform the missing operation in the element FCS_CKM.1/RSA according to the implemented key generation algorithm.

[468] [assignment: *cryptographic key generation algorithm*]

[469] [assignment: *cryptographic key sizes*]

[470] [assignment: *list of standards*], refinement to "TR-03116-1 [19]" which is the given assignment in the Protection Profile [BSI_PP_EHC_G2]

## 9.5 Security Requirements Rationale for Package RSA Key Generation

The following table provides an overview for Security Functional Requirements coverage also giving an evidence for *sufficiency* and *necessity* of the SFRs chosen in the Package RSA Key Generation.

| | O.Integrity | O.Confidentiality | O.Resp-COS | O.TSFDataExport | O.Authentication | O.AccessControl | O.KeyManagement | O.Crypto | O.SecureMessaging |
|---|---|---|---|---|---|---|---|---|---|
| FCS_CKM.1/RSA | | | | | | | x | x | |

**Table 38: Mapping between Security Objectives for the TOE and SFRs for Package RSA Key Generation**

Table 38 above should be taken as extension of Table 29 in order to cover the whole set of Security Objectives. Hence, the mappings between Security Objectives and SFRs in the table above are used as *additional* mappings to address the corresponding Security Objectives.

The Security Objective **O.KeyManagement** "Generation and import of keys" requires the ability of the TSF to secure generation, import, distribution, access control and destruction of cryptographic keys. Also, the TSF is required to support the import and export of public keys. This Security Objective is addressed by the following SFR:

- FCS_CKM.1/RSA requires that the TSF generates cryptographic keys with specific key generation algorithms as stated in the SFR. The mentioned SFR is needed to fulfil different requirements of the intended usage of the cryptographic keys.

The Security Objective **O.Crypto** "Cryptographic functions" requires the ability of the TSF to implement secure cryptographic algorithms. This Security Objective is addressed by the following SFR:

- FCS_CKM.1/RSA requires that the TSF generates cryptographic keys with specific key generation algorithms as stated in the SFR. The mentioned SFR is needed to fulfil different requirements of the intended usage of the cryptographic keys.

The following table lists the required dependencies of the SFR of this PP Package and gives the concrete SFRs from this document which fulfils the required dependencies.

Hereby, Table 39 should be taken as extension of Table 30 in order to cover all dependencies.

| SFR | dependent on | fulfilled by |
|---|---|---|
| FCS_CKM.1/RSA | [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction | FCS_COP.1/COS.RSA.S, FCS_COP.1/COS.RSA, FCS_CKM.4<br>~~*FCS_COP.1/CB.RSA* in the case that the TOE provides crypto box functionality, i.e. Package Crypto Box is applied.~~[471]<br>~~*FCS_COP.1/RSA.CVC.S, FCS_COP.1/RSA.CVC.V* in the case that the TOE provides RSA CVC functionality, i.e. Package RSA CVC is applied.~~[472] |

**Table 39: Dependencies of the SFRs for Package RSA Key Generation**

[471] Package Crypto Box **is not** applied

[472] Package RSA CVC **is not** applied

# 10TOE Summary Specification

## 10.1 Overview

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 AES, RSA, and Elliptic Curve Cryptography.

The product implements PIN-based user authentication and various standardized external and internal device authentication mechanisms based on 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 ALC_DVS.2, ATE_DPT.2 and 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 blocked 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.

### Cryptographic Services

The product implements several cryptographic 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 and verification of digital signatures are additional security services which enable the card holder to effectively sign electronic data and verify such signed 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 264nitializa users which allow for 264nitializ 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 AES symmetric ciphers with up to 256bits as well as additional modes of operation like cipher-block-chaining, or CMAC 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 265nitializa.

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 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 (after Reset or Power On) of the product is secured to ensure that the product properly 265nitializat from a down-state to a secure mode of operation. The domain separation is secured by memory access control based on different privilege levels.

The security features implemented by the product closely collaborate with the protection mechanisms of the underlying security IC.

## 10.2 Coverage of SFRs by TSFs

### 10.2.1 Rationale

**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 265nitialization mechanism allows for the management of user authentication data according to FIA_SOS.1, 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, FIA_UAU.4/PACE.PICC, FIA_UAU.5 and FIA_UAU.5/PACE.PICC 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.

FIA_UAU.6/PACE.PICC refers to the re-authentication mechanism of the PACE protocol.

The internal authentication mechansims implemented by the product target the SFRs FIA_API.1 and FIA_API.1/SICP.

the protection of communication as mandated by FTP_ITC.1/TC is also implementated by the secure channel establishment based on mutual device authentication.

the protection of communication as mandated by FTP_ITC.1/PACE.PICC is implemented by mechanisms of the PACE protocol.

### 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 266nitializat to the implementation of the following SFRs:

the SFR FIA_ATD.1 and FIA_ATD.1/PACE define 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 and FMT_SMR.1/PACE.PICC define the roles for external entities which are maintained by the Security State Model.

the SFR FIA_USB.1, FIA_USB.1/LC and FIA_USB.1/PACE.PICC define the binding of users to subjects in the product which act on behalf of the external user which is also maintained in the Security State Model of the product.

the SFR FMT_MSA.3 and FMT_MSA.3/LC define requirements for the secure initialization of security attributes. As such, it defines the proper initialization of the Security State Model.

the SFR FMT_SMF.1 defines requirements concerning management of security attributes.

### Cryptographic Services

The 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 SFR FDP_UCT.1/PACE and FDP_UIT.1/PACE specify access control when using contactless communication. Additionally the prevention of reading out sensitive PACE protocol data is specified in FMT_MTD.1/PACE.PICC.

**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 and FPT_ITE.2/PACE 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 FIA_UAU.1/PACE and of the identification according to SFR FIA_UID.1 and FIA_UID.1/PACE 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 as well as FDP_ACC.1/LC and FDP_ACF.1/LC specifiy the access rules enforce by the object system before granting access to the MF, DF, EF, TEF, and SEF respectively.

The access control related to the usage of cryptographic keys which are also part of the object system is specified by the SFRs FDP_ACC.1/KEY and FDP_ACF.1/KEY

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 and FCS_CKM.4/PACE.PICC, as well as FCS_CKM.4/AES-SCL-1_SICP by the Security IC.

**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, FCS_RNG.1/GR and FCS_RNG.1/PACE mandate 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/HPRG_SICP.

the SFR FCS_COP.1/SHA requires the implementation of SHA-1, SHA-256, SHA-384 and SHA-512 hash functions.

- the SFR FCS_COP.1/COS.AES defines the elementary AES cipher and decipher operations, together with SFR FCS_COP.1/AES-SCL-1_SICP which specifies AES cipher and decipher operations by the used SCL.
- the SFR FCS_CKM.1/AES.SM specifies the elementary operation for the derivation of AES session keys.
- the SFRs FCS_COP.1/COS.CMAC specifies the CMAC operation, together with SFR FCS_COP.1/AES-SCL-1_SICP which specifies the AES operation by the used SCL, whereby the last block of the AES operation in CBC mode is used as CMAC.
- the SFR FCS_CKM.1/RSA specifies on-card RSA key generation, together with SFR FCS_CKM.1/RSA-0_SICP which specifies RSA key generation by the used ACL v2.09.002.
- the SFR FCS_CKM.1/ELC specifies on-card ELC key generation, together with SFR FCS_CKM.1/EC-0_SICP which specifies ELC key generation by the used ACL v2.09.002
- the SFR FCS_CKM.1/DH.PACE.PICC specifies PACE key generation for the PACE-protocol
- the SFR FCS_COP.1/COS.RSA.S specifies the different RSA signature generation schemes supported by the product, together with SFR FCS_COP.1/RSA-0_SICP which specifies RSA operations by the used ACL v2.09.002.
- 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 verification schemes supported by the product.
- the SFR FCS_COP.1/ECDSA-0_SICP specifies ECDSA signature generation and verification by the used ACL v2.09.002.
- the SFR FCS_COP.1/ECDH-0_SICP specifies ELC Diffie-Hellman key agreement by the used ACL v2.09.002.
- the SFRs FCS_COP.1/COS.RSA and FCS_COP.1/COS_ELC specify the elementary RSA and ELC cipher and decipher mechanisms.
- the SFRs FCS_COP.1/PACE.PICC.ENC and FCS_COP.1/PACE.PICC.MAC specify the cipher and MAC mechanisms for the PACE-protocol.

**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 SFRs FDP_RIP.1 and FDP_RIP.1/PACE.PICC 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 SFRs FPT_EMS.1 and FPT_EMS.1/PACE.PICC 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 SFRs FPT_TST.1 and FPT_TST.2/SICP are directly related to the secure start-up (after Reset or Power On) 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, FDP_SDC.1/SICP, FDP_SDI.2/SICP are enforced by the underlying security IC and contribute to the protection of the product against attacks.

the SFRs FDP_ACC.1/SICP, FDP_ACF.1/SICP, FMT_MSA.1/SICP, FMT_MSA.3/-SICP, FMT_SMF.1/SICP are also enforced by the underlying security IC and contribute the memory access control which is important for the domain separaton.

### 10.2.2 Association Tables

| Security Functional Requirements | TOE Security Functionality |
|---|---|
| FAU_SAS.1/SICP | High Attack Resistance |
| FCS_CKM.1/AES.SM | Elementary Cryptographic Functions |
| FCS_CKM.1/DH.PACE.PICC | Elementary Cryptographic Functions |
| FCS_CKM.1/EC-0_SICP | Elementary Cryptographic Functions |
| FCS_CKM.1/ELC | Elementary Cryptographic Functions |
| FCS_CKM.1/RSA | Elementary Cryptographic Functions |
| FCS_CKM.1/RSA-0_SICP | Elementary Cryptographic Functions |
| FCS_CKM.4 | Secure Access-Controlled Object System |
| FCS_CKM.4/AES-SCL-1_SICP | Secure Access-Controlled Object System |
| FCS_CKM.4/PACE.PICC | Secure Access-Controlled Object System |
| FCS_COP.1/AES-SCL-1_SICP | Elementary Cryptographic Functions |
| FCS_COP.1/COS.AES | Elementary Cryptographic Functions |
| FCS_COP.1/COS.CMAC | Elementary Cryptographic Functions |
| FCS_COP.1/COS.ECDSA.S | Elementary Cryptographic Functions |

| Security Functional Requirements | TOE Security Functionality |
|---|---|
| FCS_COP.1/COS.ECDSA.V | Elementary Cryptographic Functions |
| FCS_COP.1/COS.ELC | Elementary Cryptographic Functions |
| FCS_COP.1/COS.RSA | Elementary Cryptographic Functions |
| FCS_COP.1/COS.RSA.S | Elementary Cryptographic Functions |
| FCS_COP.1/ECDH-0_SICP | Elementary Cryptographic Functions |
| FCS_COP.1/ECDSA-0_SICP | Elementary Cryptographic Functions |
| FCS_COP.1/PACE.PICC.ENC | Elementary Cryptographic Functions |
| FCS_COP.1/PACE.PICC.MAC | Elementary Cryptographic Functions |
| FCS_COP.1/RSA-0_SICP | Elementary Cryptographic Functions |
| FCS_COP.1/SHA | Elementary Cryptographic Functions |
| FCS_RNG.1 | Elementary Cryptographic Functions |
| FCS_RNG.1/GR | Elementary Cryptographic Functions |
| FCS_RNG.1/HPRG_SICP | Elementary Cryptographic Functions |
| FCS_RNG.1/PACE | Elementary Cryptographic Functions |
| FDP_ACC.1/EF | Secure Access-Controlled Object System |
| FDP_ACC.1/KEY | Secure Access-Controlled Object System |
| FDP_ACC.1/LC | Secure Access-Controlled Object System |
| FDP_ACC.1/MF_DF | Secure Access-Controlled Object System |
| FDP_ACC.1/SEF | Secure Access-Controlled Object System |
| FDP_ACC.1/SICP | High Attack Resistance |
| FDP_ACC.1/TEF | Secure Access-Controlled Object System |
| FDP_ACF.1/EF | Secure Access-Controlled Object System |
| FDP_ACF.1/KEY | Secure Access-Controlled Object System |
| FDP_ACF.1/LC | Secure Access-Controlled Object System |

| Security Functional Requirements | TOE Security Functionality |
|---|---|
| FDP_ACF.1/MF_DF | Secure Access-Controlled Object System |
| FDP_ACF.1/SEF | Secure Access-Controlled Object System |
| FDP_ACF.1/SICP | High Attack Resistance |
| FDP_ACF.1/TEF | Secure Access-Controlled Object System |
| FDP_IFC.1/SICP | High Attack Resistance |
| FDP_ITT.1/SICP | High Attack Resistance |
| FDP_RIP.1 | High Attack Resistance |
| FDP_RIP.1/PACE.PICC | High Attack Resistance |
| FDP_SDC.1/SICP | High Attack Resistance |
| FDP_SDI.2 | High Attack Resistance |
| FDP_SDI.2/SICP | High Attack Resistance |
| FDP_UCT.1/PACE | Access-Controlled Cryptographic Services |
| FDP_UIT.1/PACE | Access-Controlled Cryptographic Services |
| FIA_AFL.1/PIN | User Authentication |
| FIA_AFL.1/PUC | User Authentication |
| FIA_API.1 | Internal and External Device Authentication |
| FIA_API.1/SICP | Internal and External Device Authentication |
| FIA_ATD.1 | Security State Model |
| FIA_ATD.1/PACE | Security State Model |
| FIA_SOS.1 | User Authentication |
| FIA_UAU.1 | Secure Access-Controlled Object System |
| FIA_UAU.1/PACE | Secure Access-Controlled Object System |
| FIA_UAU.4 | Internal and External Device Authentication |
| FIA_UAU.4/PACE.PICC | Internal and External Device Authentication |

| Security Functional Requirements | TOE Security Functionality |
|---|---|
| FIA_UAU.5 | Internal and External Device Authentication |
| FIA_UAU.5/PACE.PICC | Internal and External Device Authentication |
| FIA_UAU.6 | Internal and External Device Authentication |
| FIA_UAU.6/PACE.PICC | Internal and External Device Authentication |
| FIA_UID.1 | Secure Access-Controlled Object System |
| FIA_UID.1/PACE | Secure Access-Controlled Object System |
| FIA_USB.1 | Security State Model |
| FIA_USB.1/LC | Security State Model |
| FIA_USB.1/PACE.PICC | Security State Model |
| FMT_LIM.1/SICP | High Attack Resistance |
| FMT_LIM.2/SICP | High Attack Resistance |
| FMT_MSA.1/Auth | Access-Controlled Cryptographic Services |
| FMT_MSA.1/Life | Secure Access-Controlled Object System |
| FMT_MSA.1/PIN | User Authentication |
| FMT_MSA.1/SEF | Secure Access-Controlled Object System |
| FMT_MSA.1/SICP | High Attack Resistance |
| FMT_MSA.3 | Security State Model |
| FMT_MSA.3/LC | Security State Model |
| FMT_MSA.3/SICP | High Attack Resistance |
| FMT_MTD.1/Auth | Access-Controlled Cryptographic Services |
| FMT_MTD.1/NE | Secure Access-Controlled Object System |
| FMT_MTD.1/PACE.PICC | Access-Controlled Cryptographic Services |
| FMT_MTD.1/PIN | User Authentication |
| FMT_SMF.1 | Security State Model |

| Security Functional Requirements | TOE Security Functionality |
|---|---|
| FMT_SMF.1/SICP | High Attack Resistance |
| FMT_SMR.1 | Security State Model |
| FMT_SMR.1/PACE.PICC | Security State Model |
| FPT_EMS.1 | High Attack Resistance |
| FPT_EMS.1/PACE.PICC | High Attack Resistance |
| FPT_FLS.1 | High Attack Resistance |
| FPT_FLS.1/SICP | High Attack Resistance |
| FPT_ITE.1 | Access-Controlled Cryptographic Services |
| FPT_ITE.2 | Secure Access-Controlled Object System |
| FPT_ITE.2/PACE | Secure Access-Controlled Object System |
| FPT_ITT.1/SICP | High Attack Resistance |
| FPT_PHP.3/SICP | High Attack Resistance |
| FPT_TDC.1 | Access-Controlled Cryptographic Services |
| FPT_TST.1 | High Attack Resistance |
| FPT_TST.2/SICP | High Attack Resistance |
| FRU_FLT.2/SICP | High Attack Resistance |
| FTP_ITC.1/PACE.PICC | Internal and External Device Authentication |
| FTP_ITC.1/TC | Internal and External Device Authentication |

**Table 40: SFRs and TSF - Coverage**

| TOE Security Functionality | Security Functional Requirements |
|---|---|
| User Authentication | FIA_AFL.1/PIN, FIA_AFL.1/PUC, FIA_SOS.1, FMT_MSA.1/PIN, FMT_MTD.1/PIN |
| Internal and External Device Authentication | FIA_API.1, FIA_API.1/SICP, FIA_UAU.4, FIA_UAU.4/PACE.PICC, FIA_UAU.5, FIA_UAU.5/PACE.PICC, FIA_UAU.6, |

| TOE Security Functionality | Security Functional Requirements |
|---|---|
| | FIA_UAU.6/PACE.PICC, FTP_ITC.1/PACE.PICC, FTP_ITC.1/TC |
| Security State Model | FIA_ATD.1, FIA_ATD.1/PACE, FIA_USB.1, FIA_USB.1/LC, FIA_USB.1/PACE.PICC, FMT_MSA.3, FMT_MSA.3/LC, FMT_SMF.1, FMT_SMR.1, FMT_SMR.1/PACE.PICC |
| Access-Controlled Cryptographic Services | FDP_UCT.1/PACE, FDP_UIT.1/PACE, FMT_MSA.1/Auth, FMT_MTD.1/Auth, FMT_MTD.1/PACE.PICC, FPT_ITE.1, FPT_TDC.1 |
| Secure Access-Controlled Object System | FCS_CKM.4, FCS_CKM.4/AES-SCL-1_SICP, FCS_CKM.4/PACE.PICC, FDP_ACC.1/EF, FDP_ACC.1/LC, FDP_ACC.1/MF_DF, FDP_ACC.1/SEF, FDP_ACC.1/TEF, FDP_ACF.1/EF, FDP_ACF.1/LC, FDP_ACF.1/MF_DF, FDP_ACF.1/SEF, FDP_ACF.1/TEF, FDP_ACC.1/KEY, FDP_ACF.1/KEY, FIA_UAU.1, FIA_UAU.1/PACE, FIA_UID.1, FIA_UID.1/PACE, FMT_MSA.1/Life, FMT_MSA.1/SEF, FMT_MTD.1/NE, FPT_ITE.2, FPT_ITE.2/PACE |
| Elementary Cryptographic Functions | FCS_CKM.1/AES.SM, FCS_CKM.1/DH.PACE.PICC, FCS_CKM.1/EC-0_SICP, FCS_CKM.1/ELC, FCS_CKM.1/RSA, FCS_CKM.1/RSA-0_SICP, FCS_COP.1/AES-SCL-1_SICP, FCS_COP.1/COS.AES, FCS_COP.1/COS.CMAC, FCS_COP.1/COS.ECDSA.S, FCS_COP.1/COS.ECDSA.V, FCS_COP.1/COS.ELC, FCS_COP.1/COS.RSA, FCS_COP.1/COS.RSA.S, FCS_COP.1/ECDH-0_SICP, FCS_COP.1/ECDSA-0_SICP, FCS_COP.1/PACE.PICC.ENC, FCS_COP.1/PACE.PICC.MAC, FCS_COP.1/RSA-0_SICP, FCS_COP.1/SHA, FCS_RNG.1, FCS_RNG.1/GR, FCS_RNG.1/HPRG_SICP, FCS_RNG.1/PACE |
| High Attack Resistance | FAU_SAS.1/SICP, FDP_ACC.1/SICP, FDP_ACF.1/SICP, FDP_IFC.1/SICP, FDP_ITT.1/SICP, FDP_RIP.1, FDP_RIP.1/PACE.PICC, FDP_SDC.1/SICP, FDP_SDI.2, FDP_SDI.2/SICP, FMT_LIM.1/SICP, FMT_LIM.2/SICP, FMT_MSA.1/SICP, FMT_MSA.3/SICP, FMT_SMF.1/SICP, FPT_EMS.1, FPT_EMS.1/PACE.PICC, FPT_FLS.1, FPT_FLS.1/SICP, FPT_ITT.1/SICP, FPT_PHP.3/SICP, FPT_TST.1, FPT_TST.2/SICP, FRU_FLT.2/SICP |

**Table 41: TSF and SFRs - Coverage**

# 11Statement of Compatibility

This is the statement of compatibility between this Composite Security Target and the Security Target of the underlying hardware [ST_IC] according to the specific requirements for composite evaluation as stated in the document "Composite product evaluation for Smartcards and similar devices" [EXS_JIL_COMP].

## 11.1 Statement concerning Platform-TSF

This section describes the separation of relevant security functionality described in the ST of the Infineon Integrated Circuit family H13 being used by this ST. The security functionality provided by the IC platform is summarized in [ST_IC]. The following table lists the security functionality of the platform and the relevance for the composite TOE.

| **Platform-TSF** | | **Relevance for the composite TOE** |
|---|---|---|
| SF_DPM | Device Phase Management | YES |
| SF_PS | Protection against Snooping | YES |
| SF_PMA | Protection against Modification Attacks (including Hardware Support Library HSL)[473] | YES |
| SF_PLA | Protection against Logical Attacks | YES |
| SF_CS<br><br>Cryptographic Support | Implementation of AES and TDES by Symmetric Cryptographic Coprocessor SCP | NO (SCP not used by the composite TOE) |
| | Implementation of TDES, AES and CMAC by Symmetric Crypraphic Library SCL<br>• Triple DES for both versions<br>• AES for both versions[474]<br>• CMAC only for version v02.04.002 | <br><br>NO (TDES not used)<br>YES<br>YES |

[473] Hardware Support Library HSL v03.12.8812 used by the TOE

[474] Symmetric Crypraphic Library SCL v02.04.002 used by the TOE

| Platform-TSF | | Relevance for the composite TOE |
|---|---|---|
| | RSA Cryptographic Library for versions v2.09.002 , v2.08.007, v2.07.003 and v2.06.003[475] | YES |
| | Elliptic Curves Cryptographic Library for versions v2.09.002, v2.08.007, v2.07.003 and v2.06.003[476] | YES |
| | Toolbox Library for versions v2.09.002 , v2.08.007, v2.07.003 and v2.06.003 | NO (Toolbox Library not used) |
| | CIPURSE™ Cryptographic Library for both versions | NO (CIPURSE™not used) |
| | Hybrid PTRNG<br>• True Random Number Generation, meeting AIS31 PTG.2<br>• Hybrid Random Number Generation, meeting AIS31 PTG.3<br>• Deterministic Random Number Generation (DRNG) AIS31 DRG.3<br>• Key Stream Generation (KSG), stream cipher generation AIS31 DRG.2 | NO (TRNG not used)<br>YES<br>NO (DRNG not used)<br>NO (KSG not used) |

**Table 42: Relevance of IC platform security functionality**

All listed TSFs of the IC Platform Security Target [ST_IC] are relevant for the Composite-ST, except for the unused optional features of SF_CS which are not relevant. Thus, the Platform-TSFs are complete and consistent to the Composite-TOE.

## 11.2 Statement concerning Threats, OSPs and Assumptions

The Threats of the IC Platform Security Target [ST_IC], including threats for the relevant optional packages, are taken over into this ST for the present TOE. There is no conflict between Threats of the Composite Security Target and the IC Security Target. All IC platform Threats taken over are relevant.

[475] RSA Cryptographic Library (ACL) v2.09.002 used by the TOE
[476] Elliptic Curves Cryptographic Library (ACL) v2.09.002 used by the TOE

| Platform Threat | Relevance for the composite TOE |
|---|---|
| T.Leak-Inherent | YES |
| T.Phys-Probing | YES |
| T.Malfunction | YES |
| T.Phys-Manipulation | YES |
| T.Leak-Forced | YES |
| T.Abuse-Func | YES |
| T.RND | YES |
| T.Masquerade_TOE | YES |
| T.Mem-Access | YES |
| T.Open_Samples_Diffusion | NO (Secure Loader blocked) |

**Table 43: Relevance of Threats of the IC Platform**

The following table maps the IC platform Threats to Threats of the Composite-ST:

| IC platform / Composite-TOE | T.Leak-Inherent | T.Phys-Probing | T.Malfunction | T.Phys-Manipulation | T.Leak-Forced | T.Abuse-Func | T.RND | T.Masquerade_TOE | T.Mem-Access |
|---|---|---|---|---|---|---|---|---|---|
| T.Leak-Inherent | x | | | | | | | | |
| T.Phys-Probing | | x | | | | | | | |
| T.Malfunction | | | x | | | | | | |
| T.Phys-Manipulation | | | | x | | | | | |
| T.Leak-Forced | | | | | x | | | | |
| T.Abuse-Func | | | | | | x | | | |
| T.RND | | | | | | | x | | |
| T.Masquerade_TOE | | | | | | | | x | |
| T.Mem-Access | | | | | | | | | x |

**Table 44: Mapping of Threats of the IC Platform to Threats of the Composite-TOE**

The OSPs of the IC Platform Security Target [ST_IC], including OSPs for the relevant optional packages, are taken over into this ST for the present TOE. There is no conflict between OSPs of the Composite Security Target and the IC Security Target. All IC platform OSPs taken over are relevant.

| Platform OSP | Relevance for the composite TOE |
|---|---|
| P.Process-TOE | YES |
| P.Lim_Block_Loader | NO (Secure Loader blocked) |
| P.Ctlr_Loader | NO (Secure Loader blocked) |
| P.Crypto-Service | YES |
| P.Add-Functions | YES |

**Table 45: Relevance of OSPs of the IC Platform**

The following table maps the IC platform OSPs to OSPs of the Composite-ST:

| IC platform / Composite-TOE | P.Process-TOE | P.Crypto_Service | P.Add-Functions |
|---|---|---|---|
| P.Process-TOE | x | | |
| P.Crypto_Service | | x | |
| P.Add-Functions | | | x |

**Table 46: Mapping of OSPs of the IC Platform to the Composite-TOE**

The Assumptions of the IC Platform Security Target [ST_IC], including modifications for the relevant optional packages, are redefined or not taken over into this ST for the present TOE. There is no conflict between Assumptions of the Composite Security Target and the IC Security Target.

| Platform Assumption | Redefined Assumption | Remark |
|---|---|---|
| A.Process-Sec-IC | A.Process-Sec-SC | Platform Assumption not relevant; no conflict by redefined Assumption |
| A.Resp-Appl | A.Resp-ObjS | Platform Assumption not relevant; no conflict by redefined Assumption |
| A.Key-Function | not taken over | not relevant, covered by T.Leak-Inherent and T.Leak-Forced instead |

**Table 47: Relevance of Assumptions of the IC Platform**

The following table maps the IC platform Assumptions to Assumptions and Threats of the Composite-ST:

| IC platform / Composite-TOE | A.Process-Sec-IC | A.Resp-Appl | A.Key-Function |
|---|---|---|---|
| A.Process-Sec-SC | x | | |
| A.Resp-ObjS | | x | |
| T.Leak-Inherent | | | X |
| T.Leak-Forced | | | X |

**Table 48: Mapping of Assumptions of the IC Platform to the Composite-TOE**

## 11.3 Statement concerning Security Objectives

The Security Objectives for the TOE of the IC Platform Security Target [ST_IC], including Security Objectives for the TOE for the relevant optional packages, are taken over into this ST for the present TOE. There is no conflict between Security Objectives for the TOE of the Composite Security Target and the IC Security Target. All IC platform Security Objectives for the TOE taken over are relevant.

| Platform Security Objective for the TOE | Relevance for the composite TOE |
|---|---|
| O.Leak-Inherent | YES |
| O.Phys-Probing | YES |
| O.Malfunction | YES |
| O.Phys-Manipulation | YES |
| O.Leak-Forced | YES |
| O.Abuse-Func | YES |
| O.Identification | YES |
| O.RND | YES |
| O.Authentication | YES |
| O.Cap_Avail_Loader | NO (Secure Loader blocked) |
| O.Ctrl_Auth_Loader | NO (Secure Loader blocked) |
| O.AES | YES |
| O.Add-Functions | YES |
| O.Mem-Access | YES |
| O.Prot_TSF_Confidentiality | NO (Secure Loader blocked) |
| O.TDS | NO (TDES cryptography not used) |
| O.Ctrl_Auth_CCL | NO (CIPURSE™ not used) |
| O.Prot_Integrity | NO (CIPURSE™ not used) |
| O.Prot_Confidentiality | NO (CIPURSE™ not used) |

**Table 49: Relevance of Security Objectives for the TOE of the IC Platform**

The following table maps the IC platform Security Objectives for the TOE to Security Objectives of the Composite-ST:

| IC platform / Composite-TOE | O.Leak-Inherent | O.Phys-Probing | O.Malfunction | O.Phys-Manipulation | O.Leak-Forced | O.Abuse-Func | O.Identification | O.RND | O.Authentication | O.AES | O.Add-Functions | O.Mem-Access |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.Leak-Inherent | x | | | | | | | | | | | |
| O.Phys-Probing | | x | | | | | | | | | | |
| O.Malfunction | | | x | | | | | | | | | |
| O.Phys-Manipulation | | | | x | | | | | | | | |
| O.Leak-Forced | | | | | x | | | | | | | |
| O.Abuse-Func | | | | | | x | | | | | | |
| O.Identification | | | | | | | x | | | | | |
| O.RND | | | | | | | | x | | | | |
| O.Authentication | | | | | | | | | x | | | |
| O.AES | | | | | | | | | | x | | |
| O.Add-Functions | | | | | | | | | | | x | |
| O.Mem-Access | | | | | | | | | | | | x |
| O.Crypto | | | | | | | | x | | x | | |
| O.SecureMessaging | | | | | | | | | | x | | |
| O.PACE_Chip | | | | | | | | x | | x | | |

**Table 50: Mapping of Security Objectives for the TOE of the IC Platform to the Composite-TOE**

The Security Objectives for the Operational Environment of the Security IC Platform, including Security Objectives for the Operational Environment for the relevant optional packages, are either split and redefined or taken over unmodified into this ST for the present TOE. Thereby, there is no conflict between Security Objectives for the Operational Environment of the Composite Security Target and Security Objectives for the Operational Environment of the IC Security Target.

| Platform Security Objective for the Operational Environment of the TOE | Redefined Security Objective or taken over | Remark |
|---|---|---|
| OE.Resp-Appl | OE.Resp-ObjS<br>OE.Plat-COS | Platform Security Objective not relevant; no conflict by redefined Security Objectives; additionally covered by O.Resp_COS |
| OE.Process-Sec-IC | OE.Process-Card | Platform Security Objective not relevant; no conflict by redefined Security Objective |
| OE.TOE_AUTH | taken over | no conflict |
| OE.Lim_Block_Loader | not taken over | not relevant (Secure Loader blocked) |
| OE.Loader_Usage | not taken over | not relevant (Secure Loader blocked) |

**Table 51: Relevance of Security Objectives for the Operational Environment of theTOE of the IC Platform**

The following table maps the IC platform Security Objectives for the Operational Environment to Security Objectives of the Composite-ST:

| IC platform / Composite-TOE | OE.Resp-Appl | OE.Process-Sec-IC | OE.TOE_AUTH |
|---|---|---|---|
| OE.Resp-ObjS | x | | |
| OE.Plat-COS | x | | |
| O.Resp_COS | x | | |
| OE.Process-Card | | x | |
| OE.TOE_AUTH | | | x |

**Table 52: Mapping of Security Objectives for the Operational Environment of the IC Platform to the Composite-TOE**

## 11.4 Statement concerning Security Requirements

### 11.4.1 Security Funtional Requirements

All relevant Security Requirements of the IC Platform Security Target [ST_IC], including Security Requirements for the relevant optional packages, are taken over into this ST for the present TOE. There is no conflict between Security Requirements of the Composite Security Target and the IC Security Target.

| SFR name | Taken over as | Remark |
|---|---|---|
| By the ACLs | | |
| FCS_CKM.1/RSA-0 | FCS_CKM.1/RSA-0_SICP | relevant, no conflict |
| FCS_CKM.1/RSA-1 | - | Not relevant |
| FCS_CKM.1/RSA-2 | - | not relevant |
| FCS_CKM.1/RSA-3 | - | not relevant |
| FCS_CKM.1/EC-0 | FCS_CKM.1/EC-0_SICP | relevant, no conflict |
| FCS_CKM.1/EC-1 | - | not relevant |

| SFR name | Taken over as | Remark |
|---|---|---|
| FCS_CKM.1/EC-2 | - | not relevant |
| FCS_CKM.1/EC-3 | - | not relevant |
| FCS_COP.1/RSA-0 | FCS_COP.1/RSA-0_SICP | relevant, no conflict |
| FCS_COP.1/RSA-1 | - | not relevant |
| FCS_COP.1/RSA-2 | - | not relevant |
| FCS_COP.1/RSA-3 | - | not relevant |
| FCS_COP.1/ECDSA-0 | FCS_COP.1/ECDSA-0_SICP | relevant, no conflict |
| FCS_COP.1/ECDSA-1 | - | not relevant |
| FCS_COP.1/ECDSA-2 | - | not relevant |
| FCS_COP.1/ECDSA-3 | - | not relevant |
| FCS_COP.1/ECDH-0 | FCS_COP.1/ECDH-0_SICP | relevant, no conflict |
| FCS_COP.1/ECDH-1 | - | not relevant |
| FCS_COP.1/ECDH-2 | - | not relevant |
| FCS_COP.1/ECDH-3 | - | not relevant |
| By the SCLs | | |
| FCS_COP.1/TDES-SCL-1 | - | not relevant |
| FCS_CKM.4/TDES-SCL-1 | - | not relevant |
| FCS_COP.1/AES-SCL-1 | FCS_COP.1/AES-SCL-1_SICP | relevant, no conflict |
| FCS_CKM.4/AES-SCL-1 | FCS_CKM.4/AES-SCL-1_SICP | relevant, no conflict |
| FCS_COP.1/CMAC-SCL-1 | - | not relevant |
| FCS_CKM.4/CMAC-SCL-1 | - | not relevant |
| FCS_COP.1/TDES-SCL-2 | - | not relevant |
| FCS_CKM.4/TDES-SCL-2 | - | not relevant |

| SFR name | Taken over as | Remark |
|---|---|---|
| FCS_COP.1/AES-SCL-2 | - | not relevant |
| FCS_CKM.4/AES-SCL-2 | - | not relevant |
| By the CIPURSE™ CLs | | |
| FCS_CKM.1/CCL | - | not relevant |
| FCS_CKM.4/CCL | - | not relevant |
| FCS_COP.1/CCL | - | not relevant |
| By Hardware, Firmware and the HSLs | | |
| FCS_CKM.4/AES | - | not relevant |
| FCS_COP.1/AES | - | not relevant |
| FCS_CKM.4/TDES | - | not relevant |
| FCS_COP.1/TDES | - | not relevant |
| FAU_SAS.1 | FAU_SAS.1/SICP | relevant, no conflict |
| FCS_RNG.1/DRNG | - | not relevant |
| FCS_RNG.1/HPRG | FCS_RNG.1/HPRG_SICP | relevant, no conflict |
| FCS_RNG.1/KSG | - | not relevant |
| FCS_RNG.1/TRNG | - | not relevant |
| FDP_ACC.1 | FDP_ACC.1/SICP | relevant, no conflict |
| FDP_ACC.1/Loader | - | not relevant |
| FDP_ACF.1 | FDP_ACF.1/SICP | relevant, no conflict |
| FDP_ACF.1/Loader | - | not relevant |
| FDP_IFC.1 | FDP_IFC.1/SICP | relevant, no conflict |
| FDP_ITT.1 | FDP_ITT.1/SICP | relevant, no conflict |
| FDP_SDC.1 | FDP_SDC.1/SICP | relevant, no conflict |
| FDP_SDI.2 | FDP_SDI.2/SICP | relevant, no conflict |
| FDP_UCT.1 | - | not relevant |
| FDP_UIT.1 | - | not relevant |
| FIA_API.1 | FIA_API.1/SICP | relevant, no conflict |
| FMT_LIM.1 | FMT_LIM.1/SICP | relevant, no conflict |

| SFR name | Taken over as | Remark |
|---|---|---|
| FMT_LIM.1/Loader | - | not relevant |
| FMT_LIM.2 | FMT_LIM.2/SICP | relevant, no conflict |
| FMT_LIM.2/Loader | - | not relevant |
| FMT_MSA.1 | FMT_MSA.1/SICP | relevant, no conflict |
| FMT_MSA.3 | FMT_MSA.3/SICP | relevant, no conflict |
| FMT_SMF.1 | FMT_SMF.1/SICP | relevant, no conflict |
| FPT_FLS.1 | FPT_FLS.1/SICP | relevant, no conflict |
| FTP_ITC.1 | - | not relevant |
| FPT_ITT.1 | FPT_ITT.1/SICP | relevant, no conflict |
| FPT_PHP.3 | FPT_PHP.3/SICP | relevant, no conflict |
| FPT_TST.2 | FPT_TST.2/SICP | relevant, no conflict |
| FRU_FLT.2 | FRU_FLT.2/SICP | relevant, no conflict |

**Table 53: Relevance of Security Requirements of the IC Platform**

The following explanations show in detail that there is no conflict between Security Requirements of the Composite Security Target and the IC Security Target.

**FCS_CKM.1/RSA-0_SICP**

SFR FCS_CKM.1/RSA-0_SICP specifies RSA key generation by the used ACL v2.09.002 . The mechanisms and key sizes listed match the mechanisms and key sizes required by SFR FCS_CKM.1/RSA.

**FCS_CKM.1/EC-0_SICP**

SFR FCS_CKM.1/EC-0_SICP specifies ELC key generation by the used ACL v2.09.002 . The mechanisms and key sizes listed match the mechanisms and key sizes required by SFR FCS_CKM.1/ELC.

**FCS_CKM.4/AES-SCL-1_SICP**

SFR FCS_CKM.4/AES-SCL-1_SICP requires the effective erasure of key material key by overwriting or zeroing. This is consistent with SFRs FCS_CKM.4 and FCS_CKM.4/PACE.PICC mandating physical erasure of the key.

**FCS_COP.1/AES-SCL-1_SICP**

SFR FCS_COP.1/AES-SCL-1_SICP specifies AES cipher and decipher operations by the used SCL. The mechanisms and key sizes listed match the AES mechanisms and key sizes required by SFR FCS_COP.1/COS.AES and COP.1/COS.CMAC as well as FCS_COP.1/PACE.PICC.ENC and FCS_COP.1/PACE.PICC.MAC.

**FCS_COP.1/RSA-0_SICP**

SFR_FCS_COP.1/RSA-0_SICP specifies RSA operations by the used ACL v2.09.002. The algorithm details and key sizes listed match the RSA signature generation schemes specified by SFR FCS_COP.1/COS.RSA.S and FCS_COP.1/COS.RSA.

**FCS_COP.1/ECDSA-0_SICP**

SFR FCS_COP.1/ECDSA-0_SICP specifies ECDSA signature generation and verification by the used ACL v2.09.002. The algorithm details and key sizes listed match the ECDSA signature generation and verification schemes specified by the SFRs FCS_COP.1/COS.ECDSA.S and FCS_COP.1/COS.ECDSA.V.

**FCS_COP.1/ECDH-0_SICP**

SFR FCS_COP.1/ECDH-0_SICP specifies ELC Diffie-Hellman key agreement by the used ACL v2.09.002. The algorithm details and key sizes listed match the ECDH key agreement schemes used in the PACE protocol specified by the SFR FCS_CKM.1/DH.PACE.PICC. The algorithm details and key sizes listed match the ECDH key agreement schemes used in the ELC Cipher specified by the SFR SFR FCS_COP.1/COS.ELC.

**FCS_RNG.1/HPRG_SICP**

SFR FCS_RNG.1/HPRG_SICP specifies the physical random number generation supplied by the security IC. The specified implementation of a high-quality random number generator matches the requirements of random number generation mandated in SFRs FCS_RNG.1, FCS_RNG.1/GR and FCS_RNG.1/PACE.

**FDP_ACC.1/SICP, FDP_ACF.1/SICP, FMT_MSA.1/SICP, FMT_MSA.3/SICP, FMT_SMF.1/SICP**

SFRs FDP_ACC.1/SICP, FDP_ACF.1/SICP, FMT_MSA.1/SICP, FMT_MSA.3/SICP, FMT_SMF.1/SICP contribute the memory access control which is important for the domain separaton. These low level access controls are in line with the higher level access controls mandated by the other iterations of SFR FDP_ACF.1, FDP_ACC.1, FMT_MSA.1 and FMT_MSA.3 in the Composite Security Target and with the SFR FMT_SMF.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_IFC.1/SICP, FDP_ITT.1/SICP, FPT_ITT.1/SICP, FDP_SDC.1/SICP, FDP_SDI.2/SICP**

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, FDP_SDC.1/SICP, FDP_SDI.2/SICP contribute to the protection of the product against attacks and are not interfering with other Security Requirements of the Composite Security Target and provide no potential of conflict. SFR FDP_SDI.2/SICP matches the requirements of the SFR FDP_SDI.2 for data integrity monitoring, as does SFR FPT_FLS.1/SICP with SFR FPT_FLS.1 for the requirements for failure with preservation of secure state.

**FIA_API.1/SICP**

SFR FIA_API.1/SICP defines authentication mechanism requirements that are used in a different production stage and not in conflict with the authentication mechanisms required by FIA_API.1.

**FPT_TST.2/SICP**

The SFRs FPT_TST.1 and FPT_TST.2/SICP are directly related to the secure start-up (after Reset or Power On) enforced by the product and do not state conflicting requirements.

### 11.4.2 Security Assurance Requirements

This statement of compatibility address the requirement specified in [EXS_JIL_COMP] for the security assurance requirements.

The security requirement for the underlying IC family H13 specified in its security target [ST_IC] is EAL6 augmented with the following component: ALC_FLR.1 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.