G+D Mobile Security

Security Target Lite

STARCOS 3.7 COS HBA-SMC

Version 1.0/18.05.2021

Document status:
Public

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstraße 159
81677 Munich
Germany

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstraße 159
81677 Munich
Germany

Table of Contents

List of Tables

1 ST Introduction

1.1 ST reference

1	Title:	Security Target Lite ‘STARCOS 3.7 COS HBA-SMC’
	Origin:	Giesecke+Devrient Mobile Security GmbH
	CC Version:	3.1 (Revision 5)
	Assurance Level:	The assurance level for this Security Target is EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 (refer to section 6.3.3 for more detail)
	General Status:	Final
	Version Number:	Version 1.0/18.05.2021
	PP:	This ST is based on BSI-CC-PP-0082-V4 version 2.1
	TOE:	STARCOS 3.7 COS HBA-SMC
	TOE documentation:	Guidance Documentation STARCOS 3.7 COS HBA-SMC – Main Document Guidance Documentation for the Initialisation Phase STARCOS 3.7 COS HBA-SMC Guidance Documentation for the Personalisation Phase STARCOS 3.7 COS HBA-SMC Guidance Documentation for the Usage Phase STARCOS 3.7 COS HBA-SMC STARCOS 3.7 Functional Specification - Part 1: Interface Specification Guidance Documentation for the Wrapper STARCOS 3.7 COS STARCOS 3.7 Internal Design Specification
	HW-Part of TOE:	IFX_CCI_000005h, evaluated against Common Criteria Version 3.1 [47].

1.2 TOE Overview

2 The aim of this document is to describe the Security Target for STARCOS 3.7 COS HBA-SMC. In the following chapters STARCOS 3.7 COS HBA-SMC stands for the Target of Evaluation (TOE).

3 STARCOS 3.7 COS HBA-SMC is a smart card and is intended to be used as a card operating system platform in accordance with 21, so the TOE provides a platform for applications in combination with the underlying hardware (the TOE evalution is carried out as a ‘Composite Evaluation’). The Security Target “STARCOS 3.7 COS HBA-SMC” is strictly conformant to the Protection Profile BSI-CC-PP-0082-V4.

4 STARCOS 3.7 COS HBA-SMC comprises:

- *the STARCOS 3.7 Health operating system,*
- *the hardware platform IFX_CCI_000005h (certificate BSI-DSZ-CC-1110-V3-2020) with the following configurations:*
  - *Sym.CoPr for DES/AES (SCP): Accessible*
  - *Asym.CoPr for RSA/ECC (Crypto2304T): Accessible*
  - *Interfaces: ISO/IEC 7816*

1.2.1 TOE description

5 The TOE comprises:

- IC embedded software, the card operating system (COS)
- The associated guidance document
- The underlying IC
- The wrapper tool

6 The TOE does not include object systems (i.e. applications eGK, HPC, SMC)

7 The TOE provides the following features:

- ISO 7816 commands and file system
- Secure Messaging
- Cryptographic algorithms and protocols
- Contactbased and contactless communication

8 The TOE implements all COS 21 commands from the mandatory package as well as from the packages “RSA Key Generation”, “Contactless”, “Crypto Box” and “Logical Channel” with the base functionality with the mandatory options, parameters and variants as well as the following optional commands:

- CREATE
- PSO HASH

9 The command CREATE can be used to create a DF or an EF in the object system. The commands CREATE and PSO HASH are part of the TSF. The TOE implements additional commands beyond COS 21 for the TOE’s initialization, personalization and usage phase. The commands are described with options and parameters in the STARCOS 3.7 Functional Specification - Part 1: Interface Specification and in the Guidance Documentations. All commands belong to the TSF.

10 The TOE implements the following crypto algorithms:

- Random generators: DRG.4 (HW random generator for seeding: PTG.2)
- Hash: SHA-1, SHA-224, SHA-384, SHA-256, SHA-512
- AES: 128 bit, 192 bit, 256 bit (with CBC mode)
- CMAC-AES: 128 bit, 192 bit, 256 bit
- RSA: 2048 bit, 3072 bit

- ECDSA-256 with curve brainpoolP256r1
- ECDSA-256 with curve ansix9p256r1
- ECDSA-384 with curve brainpoolP384r1
- ECDSA-384 with curve ansix9p384r1
- ECDSA-512 with curve brainpoolP512r1

11 The TOE implements following protocols:

- 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
- Signature calculation and verification according to RSA, ISO9796-2
- Signature calculation according to RSA, SSA, PKCS1-V1.5
- Signature calculation according to RSA, SSA, PSS
- Signature calculation according to RSA, ISO9796-2, DS2
- Signature calculation and verification according to ECDSA

12 The TOE implements following packages:

- RSA Key Generation
- Contactless
- Crypto Box
- Logical Channel

1.2.2 TOE life cycle

13 The TOE life cycle is part of the product life cycle which goes from product development to its usage by the final user. In detail TOE life cycle consist of development phase, initialisation phase, personalisation phase and usage phase. The development phase and initialisation phase is part of the evaluation. The personalisation phase and usage phase is not part of the evaluation.

Development phase

14 The TOE is developed in this phase.

15 This includes the COS design, implementation, testing and documentation by Giesecke+Devrient Mobile Security GmbH. The development occurs in a controlled environment that avoids disclosure of source code, data and any critical documentation and that guarantees the integrity of these elements. The software development environment is included in the evaluation of the TOE.

Initialisation phase

16 The initialisation phase covers the loading of the TOE's COS implementation and the loading of the object system.

17 The COS is integrated in a flash image which is loaded via the IC's flash loader by Giesecke+Devrient Mobile Security GmbH. Hereby; it is possible to load in addition the object system. In this case the object system is part of the flash image. After flashing the TOE the flash loader is permanently blocked. This is the point when the TOE is delivered either for further initialization or for personalization. The environment for preparing flash images, initialization tables, generating cryptographic keys and conducting the flashing of the TOE is included in the evaluation of the TOE. An object system may also be loaded after flashing the COS by loading an initialisation table which is generated by Giesecke+Devrient Mobile Security GmbH. This can be done if the object system was not loaded during the COS loading or if the object system was deleted after loading. This means, that the object system is not always part of the delivered product. But a delivered product may additionally include the object system beside the TOE. The loading of the object system via intialisation table can be conducted either by Giesecke+Devrient Mobile Security GmbH or a 3rd party initialiser. Giesecke+Devrient Mobile Security GmbH is able to include patches for the COS in the initialization table. Only authentic initialization tables can be loaded on the TOE.

18 The TOE is provided to the personaliser either as completed card or as module. The physical scope of the TOE is only the module. This means that the card body is not in the scope of the TOE even though this component is part of the product if completed cards are delivered. The TOE is already initialized with an object system before providing the product to the personaliser.

Personalisation phase

19 The card is personalised in this phase.

20 A 3rd party personaliser or Giesecke+Devrient Mobile Security GmbH personalize the initialized cards.

21 The product shall be tested again and all critical material including personalization data, test suites and documentation shall be protected from disclosure and modification.

22 The writing of personalization data require a prior authentication with keys dedicated for these operations. These keys are provided by Giesecke+Devrient Mobile Security GmbH. A verification of the COS consistency can be performed by the FINGERPRINT command.

Usage phase

23 The card is used in this phase.

24 Depending on the defined access rules set in the object system that is initially installed and initialised on top of the TOE parts of the object system can also be loaded in this phase by authorized enitities. This can be achieved with the command LOAD APPLICATION which requires an authentication. A verification of the COS consistency after object system loading can be performed by the FINGERPRINT command.

25 The command LOAD APPLICATION is implemented according to the G2 COS-specification in its base variant.

26 By the command LOAD APPLICATION new applications (folders with sub-structures as further folders, data files, key and PIN objects) can be installed. Is it not possible to install key and PIN objects for their own (i.e. without installing a new folder where these new objects are settled).

1.2.3 TOE definition and operational usage

27 The Target of Evaluation (TOE) addressed by the current security target is a smart card platform implementing the Card Operating System (COS) according 21 without any object system. The TOE comprises

i) the Security IC Platform, i.e. the circuitry of the chip incl. the configuration data and initialisation data related to the security functionality of the chip and IC Dedicated Software[1] with the configuration data and initialisation data related to IC Dedicated Software (the integrated circuit, IC),

ii) the IC Embedded Software (operating system)[2], including related configuration data

iii) the wrapper for interpretation of exported TSF Data

iv) the associated guidance documentation.

28 The TOE includes all excutable code running on the Security IC Platform, i.e. IC Dedicated Support Software and the Card Operating System.

29 The TOE does not include the object system, i. e. the application specific structures like the Master File (MF), the Applications, the Application Dedicated Files (ADF), the Dedicated Files (DF[3]), Elementary Files (EF) and internal security objects[4] including TSF Data. The TOE and the application specific object system build an initialized smart card product like an electronic Health Card.

30 The Guidance Documentations describe further developer specific commands and functionality for the TOE's initialisation, personalisation and usage phase implemented in the TOE.

1.2.4 TOE major security features for operational use

31 As a smart card the TOE 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 if implemented.

1.2.5 TOE type

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

---

[1] usually preloaded (and often security certified) by the Chip Manufacturer

[2] usually – together with IC – completely implementing executable functions

[3] The abbreviation DF is commonly used for dedicated files, application and application dedicated files, which are folders with different methods of identification, cf. [21], sec. 8.1.1 and 8.3.1.

[4] containing passwords, private keys etc.

33 The export of non-confidential TSF Data of object systems running on the TOE supports the verification of the correct implementation of the respective object system of the smart card during manufacturing and (conformity) testing. The exported TSF Data include all security attributes of the object system as a whole and of all objects but exclude any confidential authentication data. The wrapper provides communication interfaces between the COS and the verification tool according to the Technical Guideline BSI TR-03143 „eHealth - G2-COS Konsistenz-Prüftool“ [20]. The verification tool sends commands for the COS through the wrapper. The COS exports the TSF Data in a vendor specific format but the wrapper encodes the data into a standardized format for export to the verification tool (cf. [27]). The verification tool compares the response of the smart card with the respective object system definition. The TOE's wrapper is analysed for completeness and correctness in the framework of the TOE's evaluation.

34 The life cycle phases for the TOE are IC and Smartcard Embedded Software Development, Manufacturing[5], Smart Card Product Finishing[6], Smart Card Personalisation and, finally, Smart Card End-Usage as defined in [10]. The TOE will be delivered with completely installed COS and deactivated flash loader.

35 Operational use of the TOE is explicitly in the focus of present ST. Some single properties of the manufacturing and the card issuing life cycle phases being significant for the security of the TOE in its operational phase are also considered by the present ST. The security evaluation / certification of the TOE involved all life cycle phases into consideration to the extent as required by the assurance package chosen here for the TOE (see chap. 2.3 'Package Claim' below).

1.2.6 Non-TOE hardware/software/firmware

36 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].

1.2.7 Options and Packages

37 The specification 21 defines different options which the TOE may implement. The PP BSI-CC-PP-0082-V4 [50] takes account of these options with the following packages:

Option in [21]	Package	Remark
Option_Kryptobox	crypto box	Defines additional cryptographic mechanisms.
Option_kontaktlose_ Schnittstelle	contactless	Defines additional SFR for contactless interfaces of the smart card, i.e. PICC part of PACE.
Option_PACE_PCD	PACE for Proximity Coupling Device	Defines additional SFR for support of contactless interfaces of the terminals, i.e. PCD part of PACE.
Option_logische_Kanäle	logical channel	Defines additional SFR for the support of logical channels.
Option_USB_ Schnittstelle	---	Defines additional communication support on the lower layers. This option does not contain any

[5] IC manufacturing, packaging and testing

[6] including installation of the object system

Option in [21]	Package	Remark
		security related details and is therefore only listed for the sake of completeness.
Option_RSA_CVC	RSA CVC	Defines additional cryptographic SFRs for the support of RSA functionality that is related to CVCs
Option_RSA_KeyGeneration	RSA Key Generation	Defines an additional cryptographic SFR for the support of RSA key generation functionality (see section 12).

Table 1: Mapping between Options and Packages.

38 The Common Criteria for IT Security Evaluation, Version 3.1, Revision 5, defines 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 the PP authors 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.

39 The ST integrates the packages RSA Key Generation, Contactless, Crypto Box and Logical Channel by defining the Security Problem Definition, Security Objectives, Security Requirements and rationals.

40 *Application note 1 (ST writer):* This ST describes in the chapter Conformance Claim, section Package claim which package was chosen and in section Conformance Rationale how these package are integrated in the ST.

2 Conformance Claims

2.1 CC Conformance Claim

41 This security target claims conformance to Common Criteria Version 3.1 Revision 5 part 1 [1], part 2 [2] (extended) and part 3 [3] (conformant).

2.2 PP Claim

42 This ST claims strict conformance to Protection Profile BSI-CC-PP-0082-V4 [50] which claims strict conformance to Protection Profile BSI-CC-PP-0084-2014 [11]. Therefore this ST claims also strict conformance to Protection Profile to BSI-CC-PP-0084-2014 [11].

2.3 Package Claim

43 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]. This ST implements the packages RSA Key Generation, Contactless, Crypto Box and Logical Channel.

2.4 Conformance Claim Rationale

44 All Threats, Assumptions, OSP, security objectives and SFRs from the mandatory part of the PP (covering the G2-COS specification's package with the base functionality) and the optional packages RSA Key Generation, Contactless, Crypto Box and Logical Channel for TOE and OE are directly overtaken from BSI-CC-PP-0082-V4. This ST does not include additional augmentations and refinements.

45 The TOE type is a Card Operating System (COS) according to [21] which is consistent with the TOE type of the claimed PP.

46 From the Security Problem Definition (see section 3: “Security Problem Definition” [50] or [11]) of BSI-CC-PP-0082-V4 and BSI-CC-PP-0084-2014 the threats (see section 3.2 “Threats” [50] or [11]) and the Organisational Security Policies (see section 3.3 “Organisational Security Policies” [50] or [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, and T.RND. The OSP P.Process-TOE is also taken over from BSI-CC-PP-0082-V4 and the OSP P.Crypto-Service is taken over from BSI-CC-PP-0084-2014. See section 3.2 and 3.3 for more details.

47 The assumptions A.Process-Sec-IC and A.Resp-Appl defined in the 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 composite evaluation approach [8]. Therefore these Assumptions are now refined in order to address the Assumptions about the operational environment of the present TOE (cf. chapter 3.4 for details).

48 The Security Objectives for the Security IC Platform as defined in the 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. See paragraph 80 for more details.

49 All Security Functional Requirements with existing refinements are taken over from BSI-CC-PP-0084-2014 into the BSI-CC-PP-0082-V4 and this ST by iterations indicated by "/SICP". Namely these are the following 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, FDP_IFC.1/SICP, FPT_ITT.1/SICP, FDP_SDC.1/SICP, FDP_SDI.2/SICP, FCS_RNG.1/SICP. See section 6.1 for more details.

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

51 The refinements of the Security Assurance Requirements made in BSI-CC-PP-0082-V4 and BSI-CC-PP-0084-2014 are taken over in this Security Target and are applied to the IC Embedded Software (operating system) resp. Security IC platform.

52 As all important parts of the BSI-CC-PP-0082-V4 and BSI-CC-PP-0084-2014 are referred in a way that these are part of this Security Target the rationales still hold. Please refer to sections 4.3 and 6.3 for further details.

53 This ST integrates the package RSA Key Generation from BSI-CC-PP-0082-V4. Therefore the corresponding Security Problem Definition, Security Objectives, Security Functional Requirements defined in BSI-CC-PP-0082-V4 in chapter 12 RSA Key Generation are taken over in this Security Target. Furthermore the cryptographic service package "AES" from BSI-CC-PP-0084-2014 is integrated in the present ST. Therefore the corresponding Security Objective and the Security Functional Requirements defined in BSI-CC-PP-0084-2014 in chapter 7.4.2 Package "AES" are taken over in this Security Target, namely: O.AES, FCS_COP.1/AES.SICP, FCS_CKM.4/AES.SICP.

54 The package Contactless is integrated for contactless communication as PICC. The TOE implements the chip part of the PACE protocol with the corresponding key generation algorithm ECDH. The TSF implements a hyprid deterministic random number generator RNG class DRG.4 for the PACE protocol which generates octets of bits.

55 The package Crypto Box is integrated. Therefore the Security Problem Definition, Security Objectives, Security Functional Requirements defined in BSI-CC-PP-0082-V4 in chapter 7 Package Crypto Box are taken over in this Security Target.

56 The package Logical Channel is integrated. Therefore the Security Problem Definition, Security Objectives, Security Functional Requirements defined in BSI-CC-PP-0082-V4 in chapter 10 Package Logical Channel are taken over in this Security Target.

57 Therefore the strict conformance with BSI-CC-PP-0082-V4 [50] and BSI-CC-PP-0084-2014 [11] is fulfilled by this Security Target.

2.5 Conformance statement

58 This ST claims conformance to PP BSI-CC-PP-0082-V4 and BSI-CC-PP-0084-2014 [11].

3 Security Problem Definition

3.1 Assets and External Entities

59 As defined in section 1.2.3 the TOE is a smart card platform implementing the Card Operating System (COS) according 21 without any object system. In sense of BSI-CC-PP-0084-2007 [11] the COS is User Data and Security IC Embedded Software.

60 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.

61 In section 3.1 “Assets and External Entities” in the BSI-CC-PP-0082-V4 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 BSI-CC-PP-0082-V4,
- 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.

62 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 2: Data objects to be protected by the TOE as primary assets

63 Note: Elementary files (EF) may be stored in the MF, any Dedicated File (DF), or Application and 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 does 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).

64 This ST considers the following external entities:

External entity	Definition
World	Any user independent on identification or successful authentication[7].
Human User	A person authenticated by password or PUC.
Device	An external device authenticated by cryptographic operation

Table 3: External entities[8]

3.2 Threats

65 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.

66 The following Threats are defined in BSI-CC-PP-0084-2014 [11] and referenced in BSI-CC-PP-0082-V4 [50]: T.Leak-Inherent, T.Phys-Probing, T.Malfunction, T.Phys-Manipulation, T.Leak-Forced, T.Abuse-Func, T.RND. All Threats are part of this Security Target and taken over into this ST. Please refer BSI-CC-PP-0084-2014 for further descriptions and details. Table 4 lists all Threats taken over with the corresponding reference to [11].

Threat name	Reference to paragraph in [11]	Short description
T.Leak-Inherent	82	Inherent Information Leakage
T.Phys-Probing	83	Physical Probing
T.Malfunction	84	Malfunction due to Environmental Stress
T.Phys-Manipulation	85	Physical Manipulation
T.Leak-Forced	86	Forced Information Leakage
T.Abuse-Func	87	Abuse of Functionality
T.RND	88	Deficiency of Random Numbers

Table 4: Overview of threats defined in BSI-CC-PP-0084-2014 [11] and taken over into this ST

67 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**

An attacker with high attack potential tries to forge internal User Data or TSF Data.

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

[7] 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.

[8] 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.

TSF management function to change the user authentication data to a known value.

68 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**
	An attacker with high attack potential tries to compromise confidential User Data or TSF Data through the communication interface of the TOE. 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.

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

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

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

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

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

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

72 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.

73 The TOE shall avert the Threat "Wrong Access Rights for User Data or TSF Data (T.Wrong)" 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

74 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.

75 The following OSP is originally defined in BSI-CC-PP-0084-2014 [11] and referenced in BSI-CC-PP-0082-V4 [50]. That OSP is 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 OSP is extended on content level in comparision to BSI-CC-PP-0084-2014. Please refer to BSI-CC-PP-0084-2014 for further descriptions and details. Table 5 lists all OSPs taken over with the corresponding reference.

OSP name	Short description	Reference to paragraph in [11]
P.Process-TOE	Identification during TOE Development and Production	90
P.Crypto-Service	Cryptographic services of the TOE	374

Table 5: Overview of OSP defined in BSI-CC-PP-0084-2014 [11] and taken over into this ST.

3.4 Assumptions

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

77 The Assumptions defined in BSI-CC-PP-0084-2014 [11] and referenced in BSI-CC-PP-0082-V4 [50] 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 appropriately re-defined in BSI-CC-PP-0082-V4 [50] in order to address the Assumptions for the operational environment of the TOE in BSI-CC-PP-0082-V4. Table 6 lists and maps these Assumptions for the operational environment with the corresponding reference.

Assumptions defined in [11]	Reference to paragraph in [11]	Re-defined assumptions for the operational environment of the present TOE	Rationale of the changes
A.Process-Sec-IC	95	A.Process-Sec-SC	While the TOE of BSI-CC-PP-0084-2014 is delivered after Phase 3 'IC Manufactioring' 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	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.

Table 6: Overview of Assumptions defined in BSI-CC-PP-0084-2014 [11] and implemented by the TOE

78 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.

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

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

A.Process-Sec-SC	**Protection during Personalisation** It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to 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

81 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

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

83 The following Security Objectives for the TOE are defined in BSI-CC-PP-0084-2014 [11] and referenced in BSI-CC-PP-0082-V4 [50]. The Security Objectives for the TOE are part of BSI-CC-PP-0082-V4 and are taken over into this ST. Please refer to BSI-CC-PP-0084-2014 for further descriptions and details. Table 7 lists all Security Objectives taken over with the corresponding reference.

Security Objectives name	Short description	Reference to paragraph in [11]
O.Leak-Inherent	Protection against Inherent Information Leakage	105
O.Phys-Probing	Protection against Physical Probing	107
O.Malfunction	Protection against Malfunctions	108
O.Phys-Manipulation	Protection against Physical Manipulation	109
O.Leak-Forced	Protection against Forced Information Leakage	111
O.Abuse-Func	Protection against Abuse of Functionality	112
O.Identification	TOE Identification	113
O.RND	Random Numbers	114
O.AES	Cryptographic service AES	385

Table 7: Overview of Security Objectives for the TOE defined in BSI-CC-PP-0084-2014 [11] and taken over into this ST.

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

85 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.

86 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.

87 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.

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

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

89 The TOE shall fulfil the Security Objective "Authentication of external entities (O.Authentication)" as specified below.

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

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

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

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

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

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

O.Crypto	**Cryptographic functions**

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.

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

O.SecureMessaging **Secure messaging**

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 Operational Environment

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

95 The following Security Objectives for the Operational Environment of the Security IC Platform are defined in the 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 in the BSI-CC-PP-0082-V4. 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 BSI-CC-PP-0082-V4 in new Security Objectives for the Operational Environment of the BSI-CC-PP-0082-V4. 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. Table 8 lists and maps these Security Objectives for the Operational Environment with the corresponding reference.

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
OE.Resp-Appl	117	OE.Resp-ObjS 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

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
			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 environment of the Security IC Platform is appropriately re-defined for the present TOE.

Table 8: Overview of Security Objectives for the Operational Environment defined in BSI-CC-PP-0084-2014 [11] and taken over into this ST.

96 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..

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

OE.Resp-ObjS **Treatment of User Data and TSF Data by the Object System**

All User Data and TSF Data of the object system are defined as required by the security needs of the specific application context.

98 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**

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 to maintain confidentiality and integrity of the TOE and to prevent any theft, unauthorised personalisation or unauthorised use.

4.3 Security Objective Rationale

99 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 the additional threats, organisational policies and assumptions defined in the BSI-CC-PP-0082-V3 [50]. 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.

100 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 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	O.Identification	O.Leak-Inherent	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Leak-Forced	O.Abuse-Func	O.RND	O.AES
(A.Process-Sec-IC[9])	(X)	(X)											
A.Process-Sec-SC		X											
(A.Resp-Appl[10])			(X)	(X)									
A.Resp-ObjS				X									
P.Process-TOE					X								
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	
P.Crypto-Service													X

Table 9: Security Objective Rationale related to the IC platform

[9] Re-defined Assumption, see section 3.4

[10] Re-defined Assumption, see section 3.4

101 The Assumption A.Process-Sec-IC assumes and the Security Objetive OE.Process-Sec-IC requires 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 (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) is covered as follows:

- 'IC Development' (Phase 2) and 'IC manufacturing' (Phase3) 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 covered by 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 is addressed by A.Process-Sec-IC and A.Process-Sec-SC and covered by OE.Process-Sec-SC.

102 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 PP and the Assumption that **AResp-ObjS** that assumes all User Data and TSF Data of the TOE are treated in the object system as defiend 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.

103 The **OSP P.Process-TOE** and the Threats **T.Leak-Inherent, T.Phys-Probing, T.Malfunction, T.Phys-Manipulation, T.Leak-Forced, T.Abuse-Func** and **T.RND** are covered by the Security Objectives as described in BSI-CC-PP-0084-2014. As stated in section 2.4, this ST claims conformance to BSI-PP-0084-2014 [11]. The Security Objectives, Assumptions, Organisational Security Policies and Threats as used in Table 9 are defined and handled in [11]. Hence, the rationale for these items and their correlation with Table 9 is given in [11] and not repeated here.

104 The OSP P.Crypto-Service is covered by the Security Objectives as described in the Security Target of the Security IC Platform [47], which claims conformance to BSI-PP-0084-2014 [11]. Hence, the rationale for this item and their correlation with Table 9 is given in [47] and not repeated here.

105 The present ST defines new Threats and Assumptions for the TOE in comparision to the Security IC platform as TOE defined in BSI-PP-0084-2014 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 10: Security Objective Rationale for the COS part of the TOE

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

107 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.

108 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.

109 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.

110 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.

111 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.

112 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.

113 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.

114 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.

115 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.

116 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.

117 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 Components Definition

118 This Security Target uses components defined as extensions to Common Criteria Part 2 [2]. The following extensions are taken from BSI-CC-PP-0082-V4 [50] and BSI-CC-PP-0084-2014 [11] and are part of this security target:

- BSI-CC-PP-0084-2014 [11] section 5 “Extended Components Definition”:
  - Definition of the Family FMT_LIM,
  - Definition of the Family FAU_SAS,
  - Definition of the Family FDP_SDC,
  - Definition of the Family FCS_RNG
- BSI-CC-PP-0082-V4 [50] section 5 “Extended Components Definition”:
  - Definition of the Family FIA_API,
  - Definition of the Family FPT_EMS,
  - Definition of the Family FPT_ITE.

6 Security Requirements

119 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.

120 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.

121 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.

122 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections made by the PP author are denoted as underlined text. Selections made by the ST author are *italicised*.[11]

123 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments made by the ST author are *italicised*. In some cases the assignment made by the PP authors defines a selection which was performed by the ST author. This text is underlined and italicised like *this*.

124 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.

125 Some SFRs (including the potential exiting refinement) were taken over from the BSI-CC-PP-0084-2014. A list of all SFRs taken from BSI-CC-PP-0084-2014 [11] can be found in section 2.4, additionally the SFRs taken over are labelled with a footnote.

6.1 Security Functional Requirements for the TOE

126 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

127 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 PP defined the following security functional groups and allocated the Security Functional Requirements described in the following sections to them:

[11] Note the parameter defined in the COS specification are printed in italic as well but without indication of selection or assignment.

Security Functional Groups	Security Functional Requirements concerned
Protection against Malfunction	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/SICP
Cryptographic Service AES	FCS_COP.1/AES.SICP, FCS_CKM.4/AES.SICP

Table 11: 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_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, FMT_MSA.3, FMT_SMF.1, FMT_MSA.1/Life, FMT_MSA.1/SEF, FMT_MTD.1/PIN, FMT_MSA.1/PIN, FMT_MTD.1/Auth, FMT_MSA.1/Auth, FMT_MTD.1/NE, FDP_ACC.1/SEF, FDP_ACC.1/TEF, ACC.1/KEY, FDP_ACF.1/SEF, FDP_ACF.1/TEF, FDP_ACF.1/KEY
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, FCS_COP.1/CB_HASH
Protection of communication (section 6.1.8)	FTP_ITC.1/TC

Table 12: Security functional groups vs. SFRs

128 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.
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 13: TSF Data defined for the IC part

6.1.2 Users, subjects and objects

129 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 authorization gained by successful authentication is limited to the command RESET RETRY COUNTER for reset of the *retryCounter* and setting a new *secret*.

130 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** Authentication reference data *secret* Security attributes of the user role *pwIdentifier* *transportStatus* *lifeCycleStatus* *flagEnabled* *startSsecList* Security attributes of the secret *interfaceDependentAccessRules* *startRetryCounter* *retryCounter* *minimumLength* *maximumLength*	The following command is used by the TOE to authenticate the human user and to reset the security attribute retryCounter by PIN: VERIFY. 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’), 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’). The following command is used by the TOE to manage the security attribute *retryCounter* of the authentication reference data PIN without authentication of the human user: RESET RETRY COUNTER (P1=’03’). The command GET PIN STATUS is used to query the security attribute

User type	Authentication reference data and security attributes	Comments
		retryCounter of the authentication reference data PIN with password object specific access control rules. 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, DISABLE VERIFICATION REQUIREMENT (P1='00'). 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'). 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. The command DELETE is used to delete the authentication reference data password with password object specific access control rules.
Human user	**Multi-Reference password** Authentication reference data *Secret* is shared with the password identified by *pwReference.* Security attributes of the user role *pwIdentifier* *lifeCycleStatus* *transportStatus* *flagEnabled* *startSsecList* Security attributes of the secret The security attributes *interfaceDependentAccessRules, minimumLength, maximumLength, startRetryCounter* and *retryCounter* are shared with password identified by *pwReference.*	The commands used by the TOE to authenticate the human user and to manage the authentication reference Multi-Reference password data are the same as for password.

User type	Authentication reference data and security attributes	Comments
Human user	**Personal unblock code (PUC)** Authentication reference data *PUK* Security attributes *pwIdentifier* of the password[12] *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'). 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').

Table 14: Authentication reference data of the human user and security attributes

131 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 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 the 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 CHAT which is referenced in the access control rules of the objects. The security attribute *lifeCycleStatus* is defined for persistently stored keys only.

User type	Authentication reference data and security attributes	Comments
Device	**Symmetric authentication key** Authentication reference data *macKey*[13] Security attributes of the Authentication reference data *keyIdentifier* *interfaceDependentAccessRules* *lifeCycleStatus* *algorithmIdentifier* *numberScenario*	The following commands are used by the TOE to authenticate a device EXTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE and GENERAL AUTHENTICATE, The following commands are used by the TOE to manage the authentication reference data ACTIVATE, DEACTIVATE, DELETE and TERMINATE.

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

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

User type	Authentication reference data and security attributes	Comments
Device	**Asymmetric authentication key** Authentication reference data *Root Public Key* *Certificate* containing the *public key* of the device[14] *persistentCache* *applicationPublicKeyList*[15] Security attributes of the user *Certificate Holder Reference* (*CHR*) *lifeCycleStatus* *interfaceDependentAccessRules,* *Certificate Holder Authorisation Template (CHAT)* for ECC keys Security attributes in the *certificate* *Certificate Profile Identifier (CPI)* *Certification Authority Reference (CAR)* *Object Identifier (OID)*	The following command is used by the TOE to authenticate a device EXTERNAL AUTHENTICATE with *algID* equal to *elcRoleCheck* 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** Authentication reference data MAC session key SK4SM Security attributes of SK4SM *flagSessionEnabled* (equal SK4SM) *Kmac* and *SSCmac* *negotiationKeyInformation*	The TOE authenticates the sender of a received command using secure messaging

Table 15: Authentication reference data of the devices and security attributes

132 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	Comments
TSF	**Private authentication key** Authentication verification data *privateKey*	The following commands are used by the TOE to authenticate themselves to an external device: INTERNAL

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

[15] The command PSO VERIFY CERTIFICATEPSO VERIFY CERTIFICATE may store the successful verified public key temporarily in the *volatileCache* or persistently in the *appliationPublicKeyList 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*.

Subject type	Authentication verification data and security attributes	Comments
	Security attributes *keyIdentifier* *setAlgorithmIdentifier* with *algorithmIdentifier* *lifeCycleStatus*	AUTHENTICATE, MUTUAL AUTHENTICATE
TSF	**Secure messaging channel key** Authentication verification data MAC session key SK4SM Security attributes *flagSessionEnabled (equal SK4SM)* *macKey* and *SSCmac* *encKey* and *SSCenc* *flagCmdEnc* and *flagRspEnc*	Responses using secure messaging. The session keys are linked to the folder of the keys used to them.

Table 16: Authentication verification data of the TSF and security attributes

133 The COS specification associates a subject with a *logical channel* and its *channelContext* (cf. [21], section 12). The TOE supports one subject respective 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*) [16].
currentFolder		Identifier of the (unique) current folder
	seIdentifier	Security environment selected by means of the command MANAGE SECURITY ENVIRONMENT[17]. 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

[16] Note the COS specification [21] describes this security attribute in the context of access control rules in section 8.1.4 only.

[17] 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 commands 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	*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.
SessionkeyContext		This list contains security attributes associated with secure messaging and trusted channels.
	flagSessionEnabled	Value *noSK* indicates no session key established. Value *SK4SM* indicates session keys established for receiving commands and sending responses. Value *SK4TC* indicates session keys established for PSO ENCIPHER, PSO DECIPHER and PSO COMPUTE CRYPTOGRAPHIC CHECKSUM, PSO VERIFY CRYPTOGRAPHIC CHECKSUM.
	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

Security attribute	Elements	Comments
		keyIdentifier may reference to the authentication reference data used for PACE[18].
	accessRulesSession-keys	Access control rules associated with trusted channel support.
globalPasswordList	(*pwReference*, *securityStatusEvaluationCounter*)	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*, *securityStatusEvaluationCounter*)	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	*keyIdentifier*	List of 0, 1, 2 or 3 elements containing results of successful device authentication with authentication reference data in MF: *keyIdentifier* as reference to the used symmetric authentication key or *keyIdentifier* generated by successful authentication with PACE protocol.
dfSpecificSecurityList	*keyIdentifier*	List of 0, 1, 2 or 3 elements containing results of successful device authentication with authentication reference data for each DF: *keyIdentifier* as reference to symmetric authentication key or *keyIdentifier* generated by successful authentication with PACE protocol[19].
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.
Current file		Identifier of the (unique) current file from *currentFolder.children*
securityStatusEvaluationCounter	*startSsec*	Must contain all values of *startSsec* and may be *empty*

Table 17: Security attributes of a subject

134 The following table provides an overview of the objects, operations and security attributes defined in the current ST (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.

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

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

Object type	Security attributes	Operations
Object system	*applicationPublicKeyList* *persistentCache* *pointInTime*	PSO VERIFY CERTIFICATE
Folder (8.3.1)	*accessRules:* *lifeCycleStatus* *shareable*[20] *interfaceDependentAccessRules* *children*	SELECT ACTIVATE DEACTIVATE DELETE FINGERPRINT GET RANDOM LOAD APPLICATION TERMINATE DF
Dedicated File (8.3.1.2)	Additionally for Folder: *fileIdentifier*	Identical to Folder
Application (8.3.1.1)	Additionally for Folder: *applicationIdentifier*	Identical to Folder
Application Dedicated File (8.3.1.3)	Additionally for Folder: *fileIdentifier* *applicationIdentifier* *children*	Identical to Folder
Elementary File (8.3.2)	*fileIdentifier* *list of shortFileIdentifierlifeCycleStatus* *shareable*[21] *accessRules:* *interfaceDependentAccessRules* *flagTransactionMode* *flagChecksum*	SELECT ACTIVATE DEACTIVATE DELETE TERMINATE
Transparent EF (8.3.2.1)	Additionally for Elementary File: *numberOfOctet* *positionLogicalEndOfFile* *body*	Additionally for Elementary File: ERASE BINARY READ BINARY UPDATE BINARY WRITE BINARY
Structured EF (8.3.2.2)	Additionally to Elementary File: *recordList* *maximumNumberOfRecords* *maximumRecordLength* *flagRecordLifeCycleStatus*	Additionally to Elementary File: ACTIVATE RECORD APPEND RECORD DELETE RECORD DEACTIVATE RECORD ERASE RECORD READ RECORD SEARCH RECORD SET LOGICAL EOF UPDATE RECORD

[20] Available with Package Logical Channel.

[21] Available with Package Logical Channel.

Object type	Security attributes	Operations
Regular Password (8.4) (PIN)	*lifeCycleStatus* *pwdIdentifier* *accessRules:* *interfaceDependentAccessRules* *secret: PIN* *minimumLength* *maximumLength* *startRetryCounter* *retryCounter* *transportStatus* *flagEnabled* *startSsecList* *PUC* *pukUsage* channel specific: *securityStatusEvaluationCounter*	ACTIVATE DEACTIVATE DELETE TERMINATE CHANGE REFERENCE DATA DISABLE VERIFICATION REQUIREMENT ENABLE VERIFICATION REQUIREMENT GET PIN STATUS RESET RETRY COUNTER VERIFY
Multi-reference Password (8.5) (MR-PIN)	*lifeCycleStatus* *pwdIdentifier* *accessRules:* *interfaceDependentAccessRules* *startSsecList* *flagEnabled* *passwordReference* *Attributed used together with referred password (PIN):* *secret: PIN* *minimumLength* *maximumLength* *startRetryCounter* *retryCounter* *transportStatus* *PUC* *pukUsage* channel specific: *securityStatusEvaluationCounter*	Identical to Regular Password
PUC	*type pin* *pukUsage*	RESET RETRY COUNTER
Symmetric Key (8.6.1)	*lifeCycleStatus* *keyIdentifier* *accessRules:* *interfaceDependentAccessRules* *encKey* *macKey* *numberScenario* *algorithmIdentifier* *accessRulesSessionkeys:* *interfaceDependentAccessRules*	ACTIVATE DEACTIVATE DELETE TERMINATE EXTERNAL AUTHENTICATE GENERAL AUTHENTICATE INTERNAL AUTHENTICATE MUTUAL AUTHENTICATE

Object type	Security attributes	Operations
Private Asymmetric Key (8.6.4)	*lifeCycleStatus* *keyIdentifier* *accessRules:* *interfaceDependentAccessRules* *privateKey* *listAlgorithmIdentifier* *accessRulesSessionkeys:* *interfaceDependentAccessRules* *algorithmIdentifier* *keyAvailable*	ACTIVATE DEACTIVATE DELETE TERMINATE GENERATE ASYMMETRIC KEY PAIR or key import EXTERNAL AUTHENTICATE GENERAL AUTHENTICATE INTERNAL AUTHENTICATE PSO COMPUTE DIGITAL SIGNATURE PSO DECIPHER PSO TRANSCIPHER
Public Asymmetric Key (8.6.4)	*lifeCycleStatus* *keyIdentifier* *oid* *accessRules:* *interfaceDependentAccessRules*	ACTIVATE DEACTIVATE DELETE TERMINATE
Public Asymmetric Key for signature verification (8.6.4.2)	Additionally for Public Asymmetric Key: *publicRsaKey: oid* or *publicElcKey: oid* *CHAT* *expirationDate: date*	Additionally for Public Asymmetric Key: PSO VERIFY CERTIFICATE, PSO VERIFY DIGITAL SIGNATURE
Public Asymmetric Key for Authentication (8.6.4.3)	Additionally for Public Asymmetric Key: *publicElcKey: oid* *CHAT* *expirationDate: date*	Additionally for Public Asymmetric Key: EXTERNAL AUTHENTICATE GENERAL AUTHENTICATE INTERNAL AUTHENTICATE
Public Asymmetric Key for encryption (8.6.4.4)	Additionally for Public Asymmetric Key: *publicElcKey: oid*	Additionally for Public Asymmetric Key: PSO ENCIPHER
Card verifiable certificate (CVC) (7.1, 7.2)	*Certificate Profile Identifier (CPI)* *Certification Authority Reference (CAR)* *Certificate Holder Reference (CHR)* *Certificate Holder Autorisation (CHAT)* *Object Identifier (OID) signature*	

Table 18: Subjects, objects, operations and security attributes (for the references refer to 21).

135 The TOE supports 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,
- *interfaceDependentAccessRules* for contactless communication (cf. chapter Package Contactless).

136 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.

137 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.[22]

138 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*(*CHAT*) and secure messaging conditions (cf. [21], section 10.2 for details).

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.

139 The Boolean element ALWAYS provides the Boolean value TRUE. The Boolean element NEVER providesthe Boolean value FALSE. The other Boolean elements providethe 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.

140 The following table gives an overview of the commands the COS has to implement and the related SFRs. Please note that the commands printed in italic are described in the Packages. Some commands are not implemented by the COS as defined in [21] and thereforefore 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

[22] 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.

Operation	SFR	Section
CHANGE REFERENCE DATA	FIA_UAU.5, FIA_USB.1, FMT_SMF.1, FMT_MTD.1/PIN, FMT_MSA.1/PIN, FIA_AFL.1/PIN	14.6.1
CREATE	FDP_ACC.1/EF, FMT_SMF.1	14.2.2
DEACTIVATE	FMT_SMF.1, FMT_MSA.1/PIN	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, FMT_SMF.1, FMT_MSA.1/Life, FCS_CKM.4, *FIA_USB.1/LC*	14.2.4
DELETE RECORD	FDP_ACC.1/SEF, FDP_ACF.1/SEF, FMT_MSA.1/SEF	14.4.4
DISABLE VERIFICATION REQUIREMENT	FMT_SMF.1, FMT_MSA.1/PIN, FIA_AFL.1/PIN.FIA_USB.1	14.6.2
ENABLE VERIFICATION REQUIREMENT	FMT_SMF.1, FMT_MSA.1/PIN, FIA_AFL.1/PIN, FIA_USB.1	14.6.3
ENVELOPE	This command is not implemented by the TOE and therefore not addressed in the SFRs of this ST.	14.9.1
ERASE BINARY	FDP_ACC.1/TEF, FDP_ACF.1/TEF	14.3.1
ERASE RECORD	FDP_ACC.1/SEF, FDP_ACF.1/SEF, FMT_MSA.1/SEF	14.4.5
EXTERNAL AUTHENTICATE	FIA_UAU.4, FIA_UAU.5, FIA_USB.1, FCS_RNG.1, FCS_CKM.1/ AES.SM, FCS_COP.1/COS.ECDSA.V, FCS_COP.1/RSA.CVC.V[23], *FCS_COP.1/CB.AES, FCS_COP.1/CB.CMAC*	14.7.1
FINGERPRINT	FPT_ITE.1 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, *FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_USB.1/PACE*	14.7.2
GENERATE ASYMMETRIC KEY PAIR	FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3, FMT_SMF.1, FCS_CKM.1/RSA, FCS_CKM.1/ELC	14.9.3
GET CHALLENGE	FCS_RNG.1	14.9.4
GET DATA	This command is not implemented by the TOE and therefore not addressed in the SFRs of this ST.	14.5.1
GET PIN STATUS	FMT_SMF.1, FMT_MSA.1/PIN	14.6.4
GET RANDOM	FCS_RNG.1/GR	14.9.5

[23] Not supported by the TOE.

Operation	SFR	Section
GET RESPONSE	This command is not implemented by the TOE and therefore not addressed in the SFRs of this ST.	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, FCS_COP.1/ COS.RSA.S, FCS_COP.1/ COS.ECDSA.S, *FCS_COP.1/RSA.CVC.S*[24], *FCS_COP.1/CB.AES*, *FCS_COP.1/CB.CMAC*	14.7.4
LOAD APPLICATION	FDP_ACC.1/ MF_DF, FDP_ACF.1/ MF_DF, FMT_SMF.1, FMT_MSA.1/Life	14.2.5
LIST PUBLIC KEY	FPT_ITE.2, FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF	14.9.7
MANAGE CHANNEL	FIA_UID.1, FIA_UAU.1, *FIA_USB.1/LC*, FMT_MSA.3	14.9.8
MANAGE SECURITY ENVIRONMENT	FIA_USB.1, FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3	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	14.7.1
PSO COMPUTE CRYPTOGRAPHIC CHECKSUM	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*	14.8.1
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	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.S	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, *FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_USB.1/PACE*	14.8.3
PSO ENCIPHER	FIA_API.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, FCS_COP.1/CB.RSA, FCS_COP.1/CB_ELC*	14.8.4
PSO HASH, [ISO/IEC 7816–8]	FCS_COP.1/CB_HASH	-
PSO TRANSCIPHER USING RSA	FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3, FCS_COP.1/ COS.RSA, FCS_COP.1/ COS.ELC	14.8.6.1

[24] Not supported by the TOE.

Operation	SFR	Section
PSO TRANSCIPHER USING ELC	FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3, FCS_COP.1/ COS.RSA, FCS_COP.1/ COS.ELC	14.8.6.3
PSO VERIFY CERTIFICATE	FMT_SMF.1, FMT_MTD.1/Auth, FCS_COP.1/COS.ECDSA.V, FDP_ACC.1/KEY, FDP_ACF.1/KEY, *FCS_COP.1/RSA.CVC.V*[25]	14.8.7
PSO VERIFY CRYPTOGRAPHIC CHECKSUM	FDP_ACC.1/KEY, FDP_ACF.1/KEY, *FIA_USB.1/CB, FCS_COP.1/CB.CMAC*	14.8.8
PSO VERIFY DIGITAL SIGNATURE	FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3, FCS_COP.1/COS.ECDSA.V	14.8.9
PUT DATA	This command is not implemented by the TOE and therefore not addressed in the SFRs of this ST.	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
RESET RETRY COUNTER	FIA_AFL.1/PUC, FIA_UAU.5, FMT_SMF.1, FMT_MTD.1/PIN, FMT_MSA.1/PIN	14.6.5
SEARCH BINARY	This command is not implemented by the TOE and therefore not addressed in the SFRs of this ST.	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	14.2.6
SET LOGICAL EOF	FDP_ACC.1/TEF, FDP_ACF.1/TEF, FDP_ACF.1/TEF	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	14.6.6
WRITE BINARY	FDP_ACC.1/TEF, FDP_ACF.1/TEF	14.3.6
WRITE RECORD	This command is not implemented by the TOE and therefore not addressed in the SFRs of this ST.	14.4.9

Table 19: Mapping between commands described in COS specification 21 and the SFRs

6.1.3 Security Functional Requirements for the TOE taken over from BSI-PP-0084-2014

141 All SFRs from section 6.1 ”Security Functional Requirements for the TOE” of BSI-PP-0084-2014 are part of the present ST. On each SFR of BSI-PP-0084-2014 an iteration operation is performed

[25] Not supported by the TOE.

in the present ST. For the iteration operation the suffix "/SICP" (short for: Secure Integrated Chip Platform) is added to the respective SFR name from the Platform-ST [47].

142 The complete list of the SFRs taken over from BSI-PP-0084-2014 by the present ST follows. For further descriptions, details, and interpretations refer to sections 6.1 and 7.4.2 in BSI-PP-0084-2014 [11] and section 7.1 in the Platform-ST [47].

FRU_FLT.2/SICP: Limited fault tolerance.
FPT_FLS.1/SICP: Failure with preservation of secure state.
FMT_LIM.1/SICP: Limited capabilities.
FMT_LIM.2/SICP: Limited availabilities
FAU_SAS.1/SICP: Audit storage
FDP_SDC.1/SICP: Stored data confidentiality
FDP_SDI.2/SICP: Stored data integrity monitoring and action
FPT_PHP.3/SICP: Resistance to physical attack
FDP_ITT.1/SICP: Basic internal transfer protection
FPT_ITT.1/SICP: Basic internal TSF data transfer protection
FDP_IFC.1/SICP: Subset information flow control
FCS_RNG.1/SICP: Random number generation
FCS_COP.1/AES.SICP: Cryptographic operation – AES
FCS_CKM.4/AES.SICP: Cryptographic key destruction

143 Table 20 maps the SFR name in the present ST to the SFR name in the Platform-ST [47]. This approach allows an easy and unambiguous identification which SFR was taken over from the Platform-ST [47] into the present ST.

SFR name	SFR name in [47]	Reference
FRU_FLT.2/SICP	FRU_FLT.2	Paragraph 151 in [11]
FPT_FLS.1/SICP	FPT_FLS.1	Paragraph 152 in [11]
FMT_LIM.1/SICP	FMT_LIM.1	Paragraph 161 in [11]
FMT_LIM.2/SICP	FMT_LIM.2	Paragraph 162 in [11]
FAU_SAS.1/SICP	FAU_SAS.1	Section 7.1.1.2 in [47]
FDP_SDC.1/SICP	FDP_SDC.1	Section 7.1.5 in [47]
FDP_SDI.2/SICP	FDP_SDI.2	Section 7.1.5 in [47]
FPT_PHP.3/SICP	FPT_PHP.3	Paragraph 170 in [11]
FDP_ITT.1/SICP	FDP_ITT.1	Paragraph 173 in [11]
FPT_ITT.1/SICP	FPT_ITT.1	Paragraph 174 in [11]
FDP_IFC.1/SICP	FDP_IFC.1	Paragraph 175 in [11]
FCS_RNG.1/SICP	FCS_RNG.1/TRNG	Section 7.1.1.1.1 in [47]
FCS_COP.1/AES.SICP	FCS_COP.1/AES	Section 7.1.4.2.2 in [47]
FCS_CKM.4/AES.SICP	FCS_CKM.4/AES	Section 7.1.4.2.2 in [47]

Table 20: Mapping between SFR names in this ST and SFR names in the Platform-ST [47]

144 In some cases Security Functional Requirements from BSI-PP-0084-2014 [11] have been refined by the Platform-ST [47], the corresponding references are given in table 20. In view of refinements specified for Security Assurance Requirements refer to section 6.2.

6.1.4 General Protection of User Data and TSF Data

145 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*[26] the following objects: password objects, secret cryptographic keys, private cryptographic keys, session keys, *none*[27] [28].

146 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 *tampering*[29] on all objects, based on the following attributes: (1) key objects, (2) PIN objects, (3) affectedObject.flagTransactionMode=TRUE, (4) *none*[30] [31].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall *prevent the usage of this key or PIN object*[32].

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

[26] [selection: *allocation of the resource to, deallocation of the resource from*]

[27] *[assignment: other data objects]*

[28] [assignment: *list of objects*].

[29] [assignment: *integrity errors*]

[30] [assignment: *other user data attributes*]

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

[32] [assignment: *action to be taken*]

(2) failure detected by TSF according to FPT_TST.1[33].

148 The TOE shall meet the requirement "FPT_EMS.1 (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 about IC power consumption and command execution time*[34] in excess of *non useful information*[35] enabling access to the following TSF data (1) Regular password, (2) Multi-Reference password, (3) PUC, (4) Session keys, (5) Symmetric authentication keys, (6) Private authentication keys, (7) *none*[36] [37] and the following user data (8) Private asymmetric keys, (9) Symmetric keys, (10) *none*[38] [39].
FPT_EMS.1.2	The TSF shall ensure any user[40] are unable to use the following interface circuit interfaces[41] to gain access to the following TSF data (1) Regular password (2) Multi-Reference password (3) PUC (4) Session keys (5) Symmetric authentication keys (6) Private authentication keys

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

[34] [assignment: *types of emissions*]

[35] [assignment: *specified limits*]

[36] [assignment: *list of additional types of TSF data*]

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

[38] *[assignment: list of additional types of user data]*

[39] [assignment: *list of types of user data*]

[40] [assignment*: type of users*]

[41] [assignment: *type of connection*]

(7) *none*[42] [43]

and the following user data

(8) Private asymmetric keys

(9) Symmetric keys

(10) *none*[44] [45]

149 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)[46] 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),~~ 21, section 7.2 "CV-Certificates for ELC-keys"[47] when interpreting the TSF data from another trusted IT product.

150 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][48].
FPT_ITE.1.2	The TSF shall use *SHA-256 based fingerprint of the TOE implementation*[49] for the exported data.

151 *Application note 2*: The command FINGERPRINT calculates a hash value based fingerprint over the complete executable code actually implemented in 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

42 *[assignment: list of additional types of TSF data]*

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

44 *[assignment: list of additional types of user data]*

45 [assignment: *list of types of user data*]

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

47 [assignment: *list of interpretation rules to be applied by the TSF*]

48 [assignment: *conditions for export*]

49 [assignment: *list of generation rules to be applied by TSF*]

other means as well as all TOE implementation related configuration data. The hash function 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.

152 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 (1) all public authentication reference data, (2) all security attributes of the object system and for all objects of the object system for all commands, (3) *none*[50] given the following conditions (1) no export of secret data, (2) no export of private keys, (3) no export of secure messaging keys, (4) no export of passwords and PUC[51].
FPT_ITE.2.2	The TSF shall use *structure and content of CV certificate according to 21 and access condition encoding schemes according to [29]*[52] [53] for the exported data.

153 *Application note 3*: 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. *persitentPublicKeyList* in [21] and [27], *applicationPublicKeyList* and *persistentCache* in [21]). The bullet (2) in the element FPT_ITE.2.1 covers all security attributes of all objects system (cf. [21], (N019.900), [27], objectLocator 'E0') and of all objects of object types listed in Table 18 and all TOE specific security attributes and parameters (except secrets). The COS specification [21] identifies optional functionality of the TOE may support. The ST lists all security attributes and the TSF shall export all security attributes implemented in addition to the Table 18 and due to these options allowed according to the COS specification. 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.

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

---

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

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

[52] [assignment: *list of encoding rules to be applied by TSF*]

[53] [assignment: *list of encoding rules to be applied by TSF*]

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[54] to demonstrate the correct operation of the TSF[55].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[56].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of TSF[57].

6.1.5 Authentication

155 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*[58].

156 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[59] unsuccessful authentication attempts occur related to consecutive failed human user authentication for the PIN via

54 [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]*]

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

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

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

58 [assignment: *a defined quality metric*]

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

	VERIFY , ENABLE VERIFICATION REQUIREMENT, DISABLE VERIFICATION, REQUIREMENT or CHANGE REFERENCE DATA command[60].
FIA_AFL.1.2/PIN	When the defined number of unsuccessful authentication attempts has been met[61], the TSF shall block the password for authentication until successful unblock using command RESET RETRY COUNTER (1) P1='00' or P1='01' with presenting unblocking code PUC of this password object, (2) P1='02' or P1='03' without presenting unblocking code PUC of this password object[62].

157 *Application note 4:* 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.

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

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[63] ~~unsuccessful~~[64] authentication attempts occur related to usage of a password unblocking code using the RESET RETRY COUNTER command[65].

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

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

[62] [assignment: *list of actions*]

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

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

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

FIA_AFL.1.2/PUC	When the defined number of ~~unsuccessful~~[66] authentication attempts has been met[67], the TSF shall *block the password unblocking code*[6869].

159 *Application note 5:* 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.

160 *Application note 6:* 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.

161 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: (1) for Human User: authentication state gained a. with password: *pwIdentifier* in *globalPasswordList* and pwIdentifier in *dfSpecificPasswordList*, b. with Multi-Reference password: *pwIdentifier* in *globalPasswordList* and *pwIdentifier* in *dfSpecificPasswordList*, (2) for Device: authentication state gained ~~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,~~ b. by CVC with CHAT in *bitSecurityList*, c. with symmetric authentication key: *keyIdentity* of the key, d. with secure messaging keys: *keyIdentity* of the key used for establishing the session key[70].

162 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 (1) reading the ATR,

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

67 [selection: *met, surpassed*]

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

69 [assignment: *list of actions*]

70 [assignment: *list of security attributes*]

(2) *GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, SELECT*[71]

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

(4) none[72] [73]

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.

163 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

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

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

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

(4) *none*[74] [75].

164 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

(1) the execution of the VERIFY command,

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

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

(4) the execution of the EXTERNAL AUTHENTICATE command,

(5) the execution of the MUTUAL AUTHENTICATE command,

(6) the execution of the GENERAL AUTHENTICATE command,

---

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

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

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

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

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

(7) a secure messaging channel,

(8) a trusted channel[76]

to support user authentication.

FIA_UAU.5.2 THE TSF shall authenticate any user's claimed identity according to the following rules:

(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,

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

(3) none[77].

165 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**[78] under the conditions (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[79].

166 *Application note 7*: 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 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. 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 receiver (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

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

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

[78] Refinement identifying the concrete user

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

clearSessionKeys(...).” Furthermore item (N031.700) states that the security status of the key that was involved in the negotiation of the session keys MUST be deleted by means of *clearSessionKeys*(...) if the check of the command CMAC (cf. FCS_COP.1/COS.CMAC) 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.

167 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 (1) reading the ATR (2) *GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, SELECT*[80] (3) commands with access control rule ALWAYS for the current life cycle status and depending on the interface, (4) *none* [81] 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.

168 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 (1) INTERNAL AUTHENTICATE, (2) MUTUAL AUTHENTICATE, (3) GENERAL AUTHENTICATE, to prove the identity of the TSF itself[82] to an external entity.

169 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

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

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

[82] [assignment: *authorised user or rule*]

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

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

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

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

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

(6) *Personalisation Agent*,

(7) *Initialisation Agent*[83].

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

170 *Application note 8*: 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 ST defines the role "World" relevant for all parts of the TOE (e.g. physical protection) and roles for COS related SFR.

171 *Application note 9*: 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.

172 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:

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

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

~~(3) for Device the Role authenticated by RSA-based CVC, 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,~~

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

[83] [assignment: *the authorised identified roles*]

(5) for Device the Role authenticated by symmetric key: *keyIdentifier* and Authentication Context[84].

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:

(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).*

(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[85].

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.

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

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

(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).

(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*[86].

173 *Application note 10:* 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

174 *Application note 11:* This section defines SFR for access control on User Data in the object system. The SFR FDP_ACF.1/ MF_DF, FDP_ACF.1/EF, FDP_ACF.1/TEF, FDP_ACF.1/SEF and FDP_ACF.1/KEY describe the security attributes of the subject gaining access to these objects. The COS specification [21] describes the attributes of logical channels (i.e. subjects in CC terminology) which is valid for the core of COS including all Packages. The *globalSecurityList* and *dfSpecificSecurityList* contain all *keyIdentifier* used for successful device authentications, i.e. the list may be empty, may contain a CHA, a key identifier of a symmetric authentication key or CAN (in form of the *keyIdentifier* of the derived key) used with PACE. Because of this common structure there is no need for separate SFR in package Contactless.

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

175 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[87] on (1) the subjects *logical channel* bind to users a. World, b. Human User, c. Device, d. Human User and Device, e. *none*[88], (2) the objects a. all executable code implemented by the TOE, b. MF, c. Application, d. Dedicated File, e. Application Dedicated File, f. persistent stored public keys, g. *none*[89], (3) the operation by the following commands following a. command SELECT, b. create objects with command LOAD APPLICATION with and without command chaining, c. delete objects with command DELETE, d. read fingerprint with command FINGERPRINT, e. command LIST PUBLIC KEY, f. *none*[90].[91]

176 *Application note 12*: 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).

177 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

87 [assignment: *access control SFP*]

88 [assignment: *list of further subjects*]

89 [assignment*: list of further objects*]

90 [assignment*: all other operations applicable to MF and DF*]

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

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ MF_DF	The TSF shall enforce the access control MF_DF SFP[92] to objects based on the following (1) the subjects *logical channel* with security attributes a. *interface*, b. *globalPasswordList*, c. *globalSecurityList*, d. *dfSpecificPasswordList*, e. *dfSpecificSecurityList*, f. *bitSecurityList*, g. *SessionkeyContext*, h. *none*[93] (2) the objects a. all executable code implemented by the TOE, b. MF with security attributes *lifeCycleStatus*, *seIdentifier* and *interfaceDependentAccessRules*, c. DF with security attributes *lifeCycleStatus*, *seIdentifier* and *interfaceDependentAccessRules*, d. Application with security attributes *lifeCycleStatus*, *seIdentifier* and *interfaceDependentAccessRules*, e. Application Dedicated File with security attributes *lifeCycleStatus*, *seIdentifier* and *interfaceDependentAccessRules*, f. persistent stored public keys, g. *none*[94] [95]
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: (1) SELECT is *ALWAYS allowed* [96]. (2) GET CHALLENGE is *ALWAYS allowed*[97]. (3) A subject is allowed to create new objects (user data or TSF data) in the current folder MF if the security attributes *interface*, *globalPasswordList*, *globalSecurityList* and *SessionkeyContext* of the subject meet the access rules for the command LOAD APPLICATION of the MF dependent on *lifeCycleStatus*, *seIdentifier* and *interfaceDependentAccessRules*. (4) A subject is allowed to create new objects (user data or TSF data) in the current folder Application, Dedicated File or Application Dedicated File if the security attributes *interface*,

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

[93] [assignment*: further subjects listed in FDP_ACC.1.1/MF_DF with their security attributes*]

[94] [assignment: *list of further objects listed in FDP_ACC.1.1/MF_DF with their security attributes*]

[95] [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*]

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

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

globalPasswordList, *globalSecurityList*, *dfSpecificPasswordList*, *dfSpecificSecurityList* and *SessionkeyContext* of the subject meet the access rules for the command LOAD APPLICATION of this object dependent on *lifeCycleStatus*, *seIdentifier* and *interfaceDependentAccessRules*.

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

(6) A subject is allowed to DELETE objects in the current Application, Dedicated File or Application Dedicated File if the security attributes *interface*, *globalPasswordList*, *globalSecurityList*, *SpecificPasswordList*, *dfSpecificSecurityList* and *SessionkeyContext* of the subject meet the access rules for the command DELETE of this object dependent on *lifeCycleStatus*, *seIdentifier* and *interfaceDependentAccessRules*.

(7) A subject is allowed to read fingerprint according to FPT_ITE.1 if it is allowed to execute the command FINGERPRINT *in the current folder*[98].

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

(9) *none*[99]

FDP_ACF.1.3/ MF_DF	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[100]
FDP_ACF.1.4/ MF_DF	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[101].

178 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[102] on (1) the subjects *logical channel* bind to users a. World, b. Human User, c. Device, d. Human User and Device,

98 [assignment*: list of security attributes of subjects*]

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

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

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

102 [assignment: *access control SFP*]

e. *none*[103]

(2) the objects
   a. EF
   b. Transparent EF
   c. Structured EF
   d. *none*[104]

(3) the operation by the following commands
   a. SELECT
   b. DELETE of the current file
   c. *CREATE*[105] [106].

179 *Application note 13*: 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 theses commands are described by FMT_MSA.1/Life. The commands CREATE, GET DATA, GET RESPONSE and PUT DATA are optional. If implemented by the TOE these commands shall be added to the corresponding FDP_ACC.1 and FDP_ACF.1 SFR. 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.

180 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 FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/EF	The TSF shall enforce the access control EF SFP[107] to objects based on the following (1) the subjects *logical channel* with security attributes a. *interface*, b. *globalPasswordList*, c. *globalSecurityList*, d. *dfSpecificPasswordList*, e. *dfSpecificSecurityList* f. *bitSecurityList*, g. *SessionkeyContext*, h. *none*[108] (2) the objects a. EF with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules* of the EF, and *none*[109],

103 [assignment: list of further subjects]

104 [assignment*: list of further objects*]

105 [assignment*: further operations*]

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

107 [assignment: *access control SFP*]

108 [assignment*: further subjects listed in FDP_ACC.1.1/EF*]

109 [selection*: transaction protection Mode*, *checksum*]

b. *none*[110] [111]

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:
(1) SELECT is*ALWAYS allowed*.[112]
(2) A subject is allowed to DELETE the current EF if the security attributes *interface, globalPasswordList, globalSecurityList, dfSpecificPasswordList* and *SessionkeyContext* of the subject meet the access rules for the command DELETE of this object dependent on *lifeCycleStatus, interfaceDependentAccessRules* and *seIdentifier* of the current folder.
(3) *none*[113] [114]

FDP_ACF.1.3/EF The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[115].

FDP_ACF.1.4/EF The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[116]

181 *Application note 14*: 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*) is empty because they are optional in the COS specification [21].

182 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[117] on
(1) the subjects *logical channel* bind to users
a. World,
b. Human User
c. Device
d. Human User and Device,
e. *none*[118]
(2) the objects

110 [assignment: *list of further objects listed in FDP_ACC.1.1/EF with their security attributes*]

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

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

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

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

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

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

117 [assignment: *access control SFP*]

118 [assignment: further *subjects*]

a. Transparent EF,
b. *none*[119]

(3) the operation by the following commands
a. ERASE BINARY
b. READ BINARY
c. SET LOGICAL EOF,
d. UPDATE BINARY
e. WRITE BINARY
f. *none*[120] [121].

183 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 FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/TEF	The TSF shall enforce the access rule TEF SFP[122] to objects based on the following (1) the subjects *logical channel* with security attributes a. *interface*, b. *globalPasswordList*, c. *globalSecurityList*, d. *dfSpecificPasswordList*,*dfSpecificSecurityList*, e. *bitSecurityList*, f. *SessionkeyContext*, a. *none*[123] (2) the objects a. with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules* of the current Transparent EF, and *none*[124], b. *none*[125] [126]
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: (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

[119] [assignment*: list of further objects*]

[120] [assignment*: further operation*]

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

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

[123] [assignment*: further subjects listed in FDP_ACC.1.1/TEF*]

[124] [selection*: transaction protection Mode*, *checksum*]

[125] [assignment: *list of further objects listed in FDP_ACC.1.1/TEF*]

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

meet the access rules of this object for this command dependent on *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules* of the current Transparent EF.

(2) *none*[127] [128].

FDP_ACF.1.3/TEF — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[129].

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*[130] [131].

184 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[132] on

(1) the subjects *logical channel* bind to users
   a. World,
   b. Human User
   c. Device
   d. Human User and Device,
   e. *none*[133]

(2) the objects
   a. record in Structured EF
   b. *none*[134]

(3) the operation by the following commands
   a. Append Record
   b. Erase Record
   c. Delete Record
   d. Read Record
   e. Search Record
   f. Update Record
   g. *none*[135] [136].

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

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

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

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

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

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

[133] [assignment: further *subjects*]

[134] [assignment*: list of further objects*]

[135] [assignment*: further operation*]

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

185 *Application note 15*: 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.

186 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 FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/SEF	The TSF shall enforce the access rule SEF SFP[137] to objects based on the following (1) the subjects *logical channel* with security attributes a. *interface*, b. *globalPasswordList*, c. *globalSecurityList*, d. *dfSpecificPasswordList*, e. *dfSpecificSecurityList*, f. *bitSecurityList*, g. *SessionkeyContext*, h. *none*[138] (2) the objects a. with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules* of the current Structured EF, and *lifeCycleStatus* of the record, b. *none*[139] [140]
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: (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. (2) *none*[141].

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

[138] [assignment*: further subjects listed in FDP_ACC.1.1/SEF*]

[139] [assignment: *list of further objects listed in FDP_ACC.1.1/SEF*

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

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

FDP_ACF.1.3/SEF	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[142].
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*[143].

187 *Application note 16*: 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, 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.

188 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 SFP access control key SFP[144] on (1) the subjects *logical channel* bind to users a. World, b. Human User c. Device d. Human User and Device, e. *none*[145] (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*[146] (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 COMPUTE CRYPTOGRAPHIC CHECKSUM,

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*]

144 [assignment: *access control SFP*]

145 [assignment: further *subjects*]

146 [assignment*: list of further objects*]

h. PSO VERIFY CRYPTOGRAPHIC CHECKSUM,
i. PSO ENCIPHER,
j. PSO DECIPHER,
k. PSO TRANSCIPHER,
l. *none*[147] [148].

189 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 FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/KEY	The TSF shall enforce the access control key SFP[149] to objects based on the following (1) the subjects *logical channel* with security attributes a. *interface*, b. *globalPasswordList*, c. *globalSecurityList*, d. *dfSpecificPaswordList*, e. *dfSpecificSecurityList*, f. *bitSecurityList*, g. *SessionkeyContext*, h. *none*[150] (2) the objects a. symmetric key used for user data with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules*, the *key type* (encryption key or mac key), *interfaceDependentAccessRules* for session keys b. private asymmetric key used for user data with security attributes *seIdentifier* of the current folder, *lifeCycleStatus*, *keyAvailable* and *interfaceDependentAccessRules*, c. public asymmetric key for signature verification used for user data with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules*, d. public asymmetric key for encryption used for user data with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules*, e. CVC with security attributes *certificate content* and *signature*, f. ephemeral keys used during Diffie-Hellman key exchange

[147] [assignment*: further operation*]

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

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

[150] [assignment: *further subjects listed in FDP_ACC.1.1/KEY*]

g. *none*[151] [152]

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*[153] 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 *keyAvaliable* 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*, *dfSpecificPassworldList*, *dfSpecificSecurityList*and *SessionkeyContext* of the subject meet the access rules for the command PSO VERIFY CERTIFICATE of the signature public key to be used for verification of the signature of the CVC dependent on *seIdentifier* of the *current folder*, *lifeCycleStatus*, *key type* and *interfaceDependentAccessRules*,

b) the CVC has valid *certificate content* and *signature*, where the *expiration date* is checked against *pointInTime*.

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

---

[151] [assignment: *list of further objects listed in FDP_ACC.1.1/KEY*]

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

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

(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 decrypt and to encrypt user data using the asymmetric key if the security attributes *interface*, *dfSpecificPasswordList*, *globalSecurityList*, 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*, *dfSpecificPasswordList*, *globalPasswordList*, *globalSecurityList*, *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 using 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*, *SpecificPasswordList*, *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*[154].

FDP_ACF.1.3/KEY	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[155].
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*[156][157].

190 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: (1) Initialisation, (2) Personalisation, (3) Life Cycle Management by means of the commands GENERATE ASYMMETRIC KEY PAIR, DELETE, LOAD APPLICATION, TERMINATE, TERMINATE DF, TERMINATE CARD USAGE, *CREATE*[158] (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, (5) Management of password objects attributes by means of the commands CHANGE REFERENCE DATA, RESET RETRY COUNTER, GET PIN STATUS, VERIFY, LOAD APPLICATION (6) Management of device authentication reference data by means of the commands PSO VERIFY CERTIFICATE, GET SECURITY STATUS KEY, LOAD APPLICATION. (7) *none*[159]

191 *Application note 17*: The Protection Profile BSI-CC-PP-0084-2014 [11] describes initialisation and personalisation as management functions. This ST assigns the COS commands dedicated for these management functions.

192 *Application note 18*: 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

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

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

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

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

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

159 [assignment: *list of management functions to be provided by the TSF*]

public keys. CREATE is an optional command which is implemented in the TOE. This ST lists it to the commands for the Life Cycle Management listed in FMT_SMF.1 and FMT_MSA.1/Life.

193 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 FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles 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[160] to restrict the ability to (1) create[161] **all** security attributes of the new object DF, Application, Application Dedicated File, EF, TEF and SEF [162] to subjects allowed to execute the commands ***CREATE and*** LOAD APPLICATION for the MF, DF, Application or Application Dedicated File where the new object is created[163], (2) **change[164] the security attributes of the object MF, DF, Application, Application Dedicated File, EF, TEF and SEF[165] by means of the command LOAD APPLICATION to *none*[166]** (3) **change[167] the security attributes *lifeCycleStatus* to „*Operational state (active)*"[168] to subjects allowed to execute the command ACTIVATE for the selected object[169],** (4) **change[170] the security attributes *lifeCycleStatus* to „*Operational state (deactivated)*"[171] to subjects allowed to**

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

161 [selection: *change_default, query, modify, delete, [assignment: other operations]*]

162 [assignment: *list of security attributes*]

163 [assignment: *the authorised identified roles*]

164 [selection: change_default, query, modify, delete, [assignment: other operations]]

165 [assignment: list of security attributes]

166 [selection: none, subjects allowed execution of command LOAD APPLICATION for theMF, DF, Application, Application dedicated file where the object is updated]

167 [selection: *change_default, query, modify, delete, [assignment: other operations]*]

168 [assignment: *list of security attributes*]

169 [assignment: *the authorised identified roles*]

170 [selection: *change_default, query, modify, delete, [assignment: other operations]*]

171 [assignment: *list of security attributes*]

execute the command DEACTIVATE for the selected object[172],

(5) **change[173] the security attributes *lifeCycleStatus* to „*Termination state*"[174] to subjects allowed to execute the command TERMINATE for the selected EF, the key object or the password object[175],**

(6) **change[176] the security attributes *lifeCycleStatus* to „*Termination state*"[177] to subjects allowed to execute the command TERMINATE DF for the selected DF, Application or Application Dedicated File[178],**

(7) **change[179] the security attributes *lifeCycleStatus* to „*Termination state*"[180] to subjects allowed to execute the command TERMINATE CARD USAGE[181],**

(8) **query the security attributes lifeCycleStatus by means of the command SELECT to *ALWAYS allowed*[182]**

(9) **delete[183] all security attributes of the selected object[184] to subjects allowed to execute the command DELETE for the selected object[185] to *none*[186].**

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.

194 *Application note 19*: The refinements repeat the structure of the element in order to avoid iteration of the same SFR.

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

FMT_MSA.1/SEF Management of security attributes

172 [assignment: *the authorised identified roles*]

173 [selection: *change_default, query, modify, delete, [assignment: other operations]*]

174 [assignment: *list of security attributes*]

175 [assignment: *the authorised identified roles*]

176 [selection: *change_default, query, modify, delete, [assignment: other operations]*]

177 [assignment: *list of security attributes*]

178 [assignment: *the authorised identified roles*]

179 [selection: *change_default, query, modify, delete, [assignment: other operations]*]

180 [assignment: *list of security attributes*]

181 [assignment: *the authorised identified roles*]

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

183 [selection: *change_default, query, modify, delete, [assignment: other operations]*]

184 [assignment: *list of security attributes*]

185 [assignment: *the authorised identified roles*]

186 [assignment: list of further security attributes with the authorised identified roles]

Hierarchical to:	No other components.
Dependencies:	[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
FMT_MSA.1.1/SEF	The TSF shall enforce the access rule SEF SFP[187] to restrict the ability to (1) change[188] the security attributes *lifeCycleStatus* of the selected record to „*Operational state (active)*“[189] to subjects allowed to execute the command ACTIVATE RECORD[190] (2) **change[191] the security attributes *lifeCycleStatus* of the selected record to „Operational state (deactived)“[192] to subjects allowed to execute the command DEACTIVATE RECORD**[193], (3) **delete[194] all security attributes of the selected record**[195] **to subjects allowed to execute the command DELETE RECORD**[196], (4) *none*[197] **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.**

196 *Application note 20*: 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.

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

FMT_MSA.3	Static attribute initialisation
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes

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

188 [selection: change_default, query, modify, delete, [assignment: other operations]]

189 [assignment: list of security attributes]

190 [assignment: the authorised identified roles]

191 [selection: change_default, query, modify, delete, [assignment: other operations]]

192 [assignment: *list of security attributes*]

193 [assignment: the authorised identified roles]

FMT_MSA.3.1	FMT_SMR.1 Security roles The TSF shall enforce the access control MF_DF_SFP, access control EF_SFP, access rule TEF_SFP, access rule SEF_SFP and access control key SFP[198] to provide restrictive[199] default values for security attributes that are used to enforce the SFP. **After reset the security attributes of the subject are set as follows:** **(1) *currentFolder* is *root*,** **(2) *keyReferenceList, globalSecurityList, globalPasswordList, dfSpecificSecurityList, dfSpecificPasswordList bitSecurityList* are empty,** **(3) *SessionkeyContext.flagSessionEnabled is set* to *noSK*,** **(4) *seIdentifier* is #1,** **(5) *currentFile* is undefined.**
FMT_MSA.3.2	The TSF shall allow the subjects allowed to execute the command LOAD APPLICATION[200] to specify alternative initial values to override the default values when an object or information is created.

198 *Application note 21*: The refinements provide rules for setting restrictive security attributes after reset.

199 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 FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/PIN	The TSF shall restrict the ability to (1) set new *secret* of the password objects by means of the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[201] [202] to subjects successfully authenticated with the old *secret* of this password object[203], (2) **set new *secret* and change *transportStatus* to regular Password of the password objects with *transportStatus* equal to Leer-PIN[204] [205] to subject to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01)[206],**

198 [assignment: *access control SFP, information flow control SFP*]

199 [selection, *choose one of: restrictive, permissive, [assignment: other property]*]

200 [assignment: *the authorised identified roles*]

201 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

202 [assignment: other operations]

203 [assignment: *the authorised identified roles*]

204 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

205 [assignment: other operations]

206 [assignment: the authorised identified roles]

(3) **set new *secret* of the password objects by means of the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,00)[207] [208] to subjects successfully authenticated with the PUC of this password object[209]**

(4) **set new *secret* of the password objects by means of the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02)[210] [211] to subject to execute the command RESET RETRY DATA with (CLA,INS,P1)=(00,2C,02)[212].**

200 *Application note 22*: 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 (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.

201 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 FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles 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 control TEF_SFP, access control SEF_SFP and access control key SFP[213] to restrict the ability to (1) reset by means of the command VERIFY[214] [215] the security attribute retry counter of password objects[216] to subjects successfully authenticated with the secret of this password object[217],

[207] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[208] [assignment: other operations]

[209] [assignment: *the authorised identified roles*]

[210] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[211] [assignment: other operations]

[212] [assignment: the authorised identified roles]

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

[214] [assignment: *other operations*]

[215] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

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

[217] [assignment: *the authorised identified roles*]

(2) **reset by means of the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[218] [219] the security attributes retry counter of password objects [220] to subjects successfully authenticated with the old secret of this password object [221],**

(3) **change by means of the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[222] [223] the security attributes *transportStatus* from Transport-PIN to *regularPassword* to subjects allowed to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[224]**

(4) **change by means of the commands CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01)[225] [226]the security attributes *transportStatus* from Leer-PIN to *regularPassword* to subjects allowed to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01)[227],**

(5) **reset by means of the command DISABLE VERIFICATION REQUIREMENT with (CLA,INS,P1)=(00,26,00)[228] [229] the security attributes retry counter of password objects[230] to subjects successful authenticated with the old secret of this password object[231],**

(6) **reset by means of the command ENABLE VERIFICATION REQUIREMENT with (CLA,INS,P1)=(00,28,00)[232] [233] the security attributes retry counter of password objects[234] to subjects successfully authenticated with the old secret of this password object[235],**

---

[218] [assignment: *other operations*]

[219] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

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

[221] [assignment: *the authorised identified roles*]

[222] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

[223] [assignment: other operations]

[224] [assignment: the authorised identified roles]

[225] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

[226] [assignment: other operations]

[227] [assignment: the authorised identified roles]

[228] [assignment: *other operations*]

[229] [selection: change_default, query, modify, delete, [assignment: other operations]]

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

[231] [assignment: the authorised identified roles]

[232] [assignment: *other operations*]

[233] [selection: change_default, query, modify, delete, [assignment: other operations]]

[234] [assignment: list of security attributes]

[235] [assignment: the authorised identified roles]

(7) **reset by means of the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C, 00) or (CLA,INS,P1)=(00,2C,01)[236] [237] the security attributes retry counter of password objects[238] to subjects successfully authenticated with the PUC of this password object[239],**

(8) **reset by means of the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or (CLA,INS,P1)=(00,2C,03)[240] [241] the security attributes retry counter of password objects[242] to *subjects allowed to execute the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or (CLA,INS,P1)=(00,2C,03)*[243],**

(9) **query by means of the command GET PIN STATUS[244] [245] the security attributes *flagEnabled*, *retry counter*, *transportStatus*[246] to World[247].**

(10) **enable[248] the security attributes *flagEnabled* requiring authentication with the selected password[249] to subjects authenticated with password and allowed to execute the command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,28,00)[250],**

(11) **enable[251] the security attributes *flagEnabled* requiring authentication with the selected password[252] to subjects allowed to execute the command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,28,01)**[253].

---

[236] [assignment: *other operations*]

[237] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

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

[239] [assignment: *the authorised identified roles*]

[240] [assignment: *other operations*]

[241] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

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

[243] [assignment: *the authorised identified roles*]

[244] [assignment: *other operations*]

[245] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

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

[247] [assignment: *the authorised identified roles*]

[248] [assignment: list of security attributes]

[249] [assignment: list of security attributes]

[250] [assignment: *the authorised identified roles*]

[251] [selection: change_default, query, modify, delete, [assignment: other operations]]

[252] [assignment: list of security attributes]

[253] [assignment: *the authorised identified roles*]

(12) **disable[254] the security attributes *flagEnabled* requiring authentication with the selected password[255] to subjects authenticated with password and allowed to execute the command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,00)**[256].

(13) **disable[257] the security attributes *flagEnabled* requiring authentication with the selected password[258] to subjects allowed to execute the command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,01)[259]**

202 *Application note 23*: 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 anybody to disable the verification requirement with the PIN. In order to prevent bypass of the human user authentication defined by the PIN 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 command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,28,01) allows anybody to enable the verification requirement with the PIN and therefore the object system shall define access control to this command according to the intended security policy of the application, cf. OE.Resp-ObjS.

203 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 FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/Auth	The TSF shall restrict the ability to (1) import by means of the command LOAD APPLICATION[260] the root public keys to roles authorised to execute this command[261],

254 [selection: change_default, query, modify, delete, [assignment: other operations]]

255 [assignment: list of security attributes]

256 [assignment: the authorised identified roles]

257 [selection: change_default, query, modify, delete, [assignment: other operations]]

258 [assignment: *list of security attributes*]

259 [assignment: the authorised identified roles]

260 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

261 [assignment: *the authorised identified roles*]

(2) import by means of the command PSO VERIFY CERTIFICATE[262] the root public keys to roles authrised to execute this command[263],

(3) import by means of the command PSO VERIFY CERTIFICATE[264] the certificate as device authentication reference data to roles authorised to execute this command[265],

(4) **select by means of the command MANAGE SECURITY ENVIRONMENT[266] the device authentication reference data to *World*[267 268].**

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.

204 *Application note 24*: The TOE provides access control to the commands depending on the object system. The refinements repeat the structure of the element in order to avoid iteration of the same SFR. If root public keys are imported according to clause (2) this public key will be stored in the *persistentPublicKeyList* of the object system.

205 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 FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1/Auth	The TSF shall enforce the access control key SFP[269] to restrict the ability to query[270 271] the security attributes access control rights set for the key[272] to meet the access rules of command GET SECURITY

262 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

263 [assignment: *the authorised identified roles*]

264 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

265 [assignment: *the authorised identified roles*]

266 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

267 [selection: *World, roles autorized to execute this command*]

268 [assignment: *the authorised identified roles*]

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

270 [assignment: other operations]

271 [selection: change_default, query, modify, delete, [assignment: other operations]]

272 [assignment: *list of security attributes*]

STATUS KEY of the object dependent on *lifeCycleStatus*, *seIdentifier* and *interfaceDependentAccessRules*[273].

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

FMT_MTD.1/NE	Management of TSF data – No export
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/NE	The TSF shall restrict the ability to (1) export TSF data according to FTP_ITE.2[274] the (a) public authentication reference data, (b) security attributes for objects of the object system to *none*[275] **(2) export TSF data according to FPT_ITE.2[276] the *none*[277] [278] [279] to *none*[280] [281]** **(3) export[282] the following TSF-data** **a) Password** **b) Multi-Reference password** **c) PUC** **d) Private keys** **e) Session keys** **f) Symmetric authentication keys** **g) Private authentication keys** **h) *none*[283]** **and the following user data** **a) Private keys of the user** **b) Symmetric keys of the user** **c) *none*[284] [285]**

[273] [assignment: *the authorised identified roles*]

[274] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[275] [assignment: list of security attributes of subjects]

[276] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

[277] [assignment: list of all TOE specific security attributes not described in COS specification [21]]

[278] [assignment: *list of TSF data*]

[279] [assignment: other operations]

[280] [assignment: list of security attributes of subjects]

[281] [assignment: *the authorised identified roles*]

[282] [assignment: *list of TSF data*]

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

[284] [assignment: *list of types of user data*]

[285] [assignment: *list of TSF data*]

to nobody[286].

6.1.7 Cryptographic Functions

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

(1) length 256 bit

(a) brainpoolP256r1 defined in RFC5639 [41]

(b) ansix9p256r1 defined in ANSI X.9.62 [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].

208 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.

209 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

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

211 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 deterministic*[287] [288] random number generator of RNG class ***DRG.4***[289] [7] that implements: ***(DRG.4.1) The internal state of the RNG uses a PTRNG of class PTG.2 as a random source.*** ***(DRG.4.2) The RNG provides forward secrecy.***

[286] [assignment: *the authorised identified roles*]

[287] [selection: *deterministic, hybrid deterministic, physical, hybrid physical*]

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

[289] [selection: *DRG.3, DRG.4, PTG.2, PTG.3*]

	(DRG.4.3) The RNG provides backward secrecy, even if the current internal state is known.
	(DRG.4.4) The RNG provides enhanced forward secrecy for every call.
	(DRG.4.5)The internal state of the RNG is seeded by a PTRNG of class PTG.2.[290]
FCS_RNG.1.2	The TSF shall provide random numbers that meet
	(DRG.4.6) The RNG generates output for which two strings of bit length 128 are mutually different with probability 1 - 2^128.
	(DRG.4.7) Statistical test suites cannot practically distinguish the random number from output sequences of an ideal RNG. The random numbers pass test procedure A as defined in AIS20/31.[291]

212 *Application note 25*: This SFR requires the TOE to generate random numbers used for key generation (static and ephemeral keys) whithin 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. 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.

213 The selection in the element FCS_RNG.1.1 includes RNG of classes DRG.3 and DRG.4. 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 is chosen to resist attacks with high attack potential.

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

FCS_RNG.1/GR	Random number generation – Get random command
Hierarchical to:	No other components.
Dependencies:	No dependencies.

[290] [assignment: *list of security capabilities* ***of the selected RNG class***]

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

FCS_RNG.1.1/GR	The TSF shall provide physical[292] random number generator of RNG class **PTG.2**[293] **([6]) for GET RANDOM** that implements *(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.* *(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.* *(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.* *(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.* *(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.*[294]
FCS_RNG.1.2/GR	The TSF shall provide random ~~numbers~~ ***octets of bits***[295] that meet *(1) Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.* *(2) The average Shannon entropy per internal random bit exceeds 0.997.*[296]

215 Application note *26*: 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).

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

FCS_COP.1/SHA	Cryptographic operation SHA
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 Cryptographic key destruction

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

[293] [selection*: **PTG.2, PTG.3***]

[294] [assignment: *list of security capabilities* ***of the selected RNG class***]

[295] [*selection:* ***bits, octets of bits, numbers [assignment: format of the numbers]***]

[296] [assignment: ~~*a*~~ *defined quality metric* ***of the selected RNG class***]

FCS_COP.1.1/SHA	The TSF shall perform hashing[297] in accordance with a specified cryptographic algorithm (1) SHA-1, (2) SHA-384, (3) SHA-256, (4) SHA-512 [298] and cryptographic key sizes none[299] that meet the following TR-03116-1 [19], FIPS 180-4[37][300].

217 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 FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ COS.AES	The TSF shall perform 1. encryption and decryption with card internal key for command MUTUAL AUTHENTICATE, 2. decryption with card internal key for command GENERAL AUTHENTICATE. 3. encryption and decryption for secure messaging[301] in accordance with a specified cryptographic algorithm AES in CBC mode[302] and cryptographic key sizes 128 bit, 192 bit, 256 bit[303] that meet the following: TR-03116-1 [19], COS specification [21], FIPS 197 [33][304].

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

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] 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

297 [assignment: *list of cryptographic operations*]

298 [assignment: *cryptographic algorithm*]

299 [assignment: *cryptographic key sizes*]

300 [assignment: *list of standards*]

301 [assignment: *list of cryptographic operations*]

302 [assignment: *cryptographic algorithm*]

303 [assignment: *cryptographic key sizes*]

304 [assignment: *list of standards*]

	for AES as specified in sec. 4.3.3.2 in [17][305] and specified cryptographic key sizes 128 bit, 192 bit and 256 bit[306] that meet the following: BSI TR-03111 [17], COS specification [21], FIPS 197 [33][307].

219 *Application note 27*: The Key Generation FCS_CKM.1/AES.SM is done during MUTUAL AUTHENTICATE and GENERAL AUTHENTICATE with establishment of secure messaging.

220 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 FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ COS.CMAC	The TSF shall perform (1) computation and verification of cryptographic checksum for command MUTUAL AUTHENTICATE, (2) verification of cryptographic checksum for command GENERAL AUTHENTICATE, (3) computation and verification of cryptographic checksum for secure messaging[308] in accordance with a specified cryptographic algorithm AES CMAC[309] and cryptographic key sizes 128 bit, 192 bit and 256 bit[310] that meet the following TR-03116-1 [19] section 3.2.2, COS specification [21], FIPS 197 [33], NIST SP 800-38B [36][311].

221 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 FCS_COP.1 Cryptographic operation] 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 *ECDH compliant to*

305 [assignment: *cryptographic key generation algorithm*]

306 [assignment: *cryptographic key sizes*]

307 [assignment: *list of standards*]

308 [assignment: *list of cryptographic operations*]

309 [assignment: *cryptographic algorithm*]

310 [assignment: *cryptographic key sizes*]

311 [assignment: *list of standards*]

[17][312] **with COS standard curves[313]** and specified cryptographic key sizes 256 bit, 384 bit and 512 bit[314] that meet the following TR-03111 [17], COS specification [21][315].

222 *Application note 28*: The COS specification 21 requires the TOE to support elliptic curves listed in COS specification [21], section 6.5 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.

223 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 FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1 /COS.RSA.S	The TSF shall perform digital signature generation for commands (1) PSO COMPUTE DIGITAL SIGNATURE, (2) INTERNAL AUTHENTICATE[316] in accordance with a specified cryptographic algorithm (1) RSASSA-PSS-SIGN with SHA-256, (2) RSA SSA PKCS1-V1_5, (3) RSA ISO9796-2 DS2 with SHA-256 (for PSO Compute DIGITAL SIGNATURE only) [317], and cryptographic key sizes 2048 bit and 3072 bit modulus length[318] that meet the following: TR-03116-1 [19], COS specification [21], [31], [34][319].

224 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.

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

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

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

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

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

[317] [assignment: *cryptographic algorithm*]

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

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

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/COS.ECDSA.V	The TSF shall perform digital signature verification for the commands (1) PSO VERIFY CERTIFICATE, (2) PSO VERIFY DIGITAL SIGNATURE, (3) EXTERNAL AUTHENTICATE[320] in accordance with a specified cryptographic algorithm ECDSA with COS standard curves using (4) SHA-256, (5) SHA-384, (6) SHA-512[321] and cryptographic key sizes 256 bits, 384 bits, 512 bits[322] that meet the following TR-03116-1 [19], BSI TR-03111 [17], COS specification [21], [40][323].

225 *Application note 29:* The command PSO VERIFY CERTIFICATE may store the imported public keys for ELC temporarily in the *volatileCache* or permanently in the *persistentCache* or *applicationPublicList*. These keys may be used as authentication reference data for asymmetric key based device authentication (cf. FIA_UAU.5) or user data.

226 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 FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ COS.ECDSA.S	The TSF shall perform digital signature generation for the commands (1) PSO COMPUTE DIGITAL SIGNATURE (2) INTERNAL AUTHENTICATE[324] in accordance with a specified cryptographic algorithm ECDSA with COS standard curves using (1) SHA-256, (2) SHA-384, (3) SHA-512[325]

320 [assignment: *list of cryptographic operations*]

321 [assignment: *cryptographic algorithm*]

322 [assignment: *cryptographic key sizes*]

323 [assignment: *list of standards*]

324 [assignment: *list of cryptographic operations*]

325 [assignment: *cryptographic algorithm*]

and cryptographic key sizes 256 bits, 384 bits, 512 bits[326] that meet the following TR-03116-1 [19], BSI TR-03111 [17], COS specification [21], [40][327].

227 *Application note 30*: The TOE shall support two variants of the PSO COMPUTE DIGITAL SIGNATURE.

- PSO COMPUTE DIGITAL SIGNATURE without Message Recovery shall be used for the signing algorithms
  - RSASSA-PSS-SIGN with SHA-256 (see FCS_COP.1/ COS.RSA.S),
  - RSA SSA PKCS1-V1_5, RSA (see FCS_COP.1/ COS.RSA.S),
  - ECDSA with SHA-256, SHA-384 and SHA-512 (see FCS_COP.1/ COS.ECDSA.S)
- PSO COMPUTE DIGITAL SIGNATURE with Message Recovery shall be used for the following signing algorithm
  1. RSA ISO9796-2 DS2 with SHA-256 (see FCS_COP.1/COS.RSA.S)

228 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 FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ COS.RSA	The TSF shall perform (1) encryption with passed key for command PSO ENCIPHER (2) decryption with stored key for command PSO DECIPHER (3) decryption and encryption for command PSO TRANSCIPHER using RSA (transcipher of data using RSA keys) (4) decryption for command PSO TRANSCIPHER using RSA (transcipher of data from RSA to ELC) (5) encryption for command PSO TRANSCIPHER using ELC (transcipher of data from ELC to RSA) [328] in accordance with a specified cryptographic algorithm (1) for encryption: RSA-OAEP-Encrypt ([34] section 7.1.1) (2) for decryption: RSA-OAEP-Decrypt ([34] section 7.1.2) [329] 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[330] that meet the following TR-03116-1 [19], COS specification [21], [34][331].

326 [assignment: *cryptographic key sizes*]

327 [assignment: *list of standards*]

328 [assignment: *list of cryptographic operations*]

329 [assignment: *cryptographic algorithm*]

330 [assignment: *cryptographic key sizes*]

331 [assignment: *list of standards*]

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

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] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ COS.ELC	The TSF shall perform (1) encryption with passed key for command PSO ENCIPHER (2) decryption with stored key for command PSO DECIPHER (3) decryption and encryption for command PSO TRANSCIPHER using ELC (transcipher of data using ELC keys) (4) decryption for command PSO TRANSCIPHER using ELC (transcipher of data from ELC to RSA) (5) encryption for command PSO TRANSCIPHER using ELC (transcipher of data from RSA to ELC) [332] in accordance with a specified cryptographic algorithm (1) for encryption ELC encryption, (2) for decryption ELC decryption[333] 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[334] that meet the following TR-03111 [17], TR-03116-1 [19], and COS specification [21][335].

230 *Application note 31*: The TOE supports the command PSO HASH (following standard [30]). Therefore this ST adds a SFR FCS_COP.1/CB_HASH specifying the supported hash algorithms. PSO HASH should not be used for processing confidential data.

FCS_COP.1/ CB_HASH	Cryptographic operation – Hash
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, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ CB_HASH	The TSF shall perform *a hash value*[336] in accordance with a specified cryptographic algorithm (1) SHA-1 (2) SHA-224

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

[333] [assignment: *cryptographic algorithm*]

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

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

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

(3) SHA-256
(4) SHA-384
(3) SHA-512 [337]

and cryptographic key sizes *none*[338] that meet the following [17], [19], and [21][339].

231 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 *overwriting the key value with 'FF' values*[340] that meets the following: *none*[341].

232 *Application note 32*: The TOE destroys 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 clears 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 is taken into account by the TOE.

6.1.8 Protection of communication

233 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[342] to initiate communication via the trusted channel.

[337] [assignment: *cryptographic algorithm*]

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

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

[340] [assignment: *cryptographic key destruction method*]

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

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

FTP_ITC.1.3/TC	The TSF shall initiate communication via the trusted channel for none[343].

234 *Application note 33*: The TOE responds only to commands establishing secure messaging channels.

6.2 Security Assurance Requirements for the TOE

235 The Security Target to be developed based upon this Protection Profile will be evaluated according to

Security Target evaluation (Class ASE)

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

Assurance Level 4 (EAL4)

237 and augmented by taking the following components:

ALC_DVS.2 (Development security)

ATE_DPT.2 (Test depth)

AVA_VAN.5 (Advanced methodical vulnerability analysis).

238 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)

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

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 21: TOE Security Assurance Requirements

6.2.1 Refinements of the TOE Security Assurance Requirements

239 In BSI-CC-PP-0084-2014 [11] refinements of the TOE Security Assurance Requirements are setup. As the Security Target takes over the refinements for the SFRs listed in section 6.1.3 “Security Functional Requirements for the TOE taken over from BSI-CC-PP-0084-2014” (see Table 20), the SAR refinements from BSI-CC-PP-0084-2014 [11] must be applied to these refined SFRs. The SAR refinements and the sections where these refinements in BSI-CC-PP-0084-2014 [11] are specified are listed in Table 22.

240 For all other SFRs the TOE Security Assurance Requirements from Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5 [3] should be used. Note that it is possible to use the TOE Security Assurance Requirements as defined in BSI-CC-PP-0084-2014 [11] (see Table 22) for all SFRs in this Security Target. According to Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-05-001, Version 3.1, Revision 5 [1] for that choice a justification of why the preferred option was not chosen is required.

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)”

Refinements regarding	Reference to [11]
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 22: Refined TOE Security Assurance Requirements

241 The following sections define further specific refinements and application notes to the chosen SARs that have be applied for the TOE and its evaluation.

6.2.2 Refinements to ADV_ARC.1 Security architecture description

242 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.

243 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 the features and commands identified as optional in the COS specification are not part of the TSF the security architecture description shall demonstrate that they do not bypass the SFR-enforcing functionality.

6.2.3 Refinements to ADV_FSP.4 Complete functional specification

244 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.

245 *Application note 34:* 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

246 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**.

247 *Application note 35:* 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

248 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.

249 *Application note 36:* 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’s guidance documentation describes 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

250 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 uses cases applicable for the TOE and the intended application eHC, eHPC, gSMC-KT, SMC-B or gSMC-K.

251 *Application note 37*: 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

252 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 uses cases applicable for the TOE and the intended application eHC, eHPC, SMC-B, gSMC-K and gSMC-KT.

253 *Application note 38*: 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 ST and the optional Packages included in this ST.

6.3 Security Requirements Rationale

254 This section comprises three parts:

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

6.3.1 Security Functional Requirements Rationale

255 Table 2 in BSI-CC-PP-0084-2014 [11], section 6.3.1 “Rational for security functional requirements” gives an overview, how the Security Functional Requirements that are taken over in the ST collaborate to meet the respective Security Objectives. Please refer for the further details to the related justification provided in BSI-CC-PP-0084-2014 [11].

256 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.AES
FAU_SAS.1/SICP	X								

	O.Identification	O.Leak-Inherent	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Leak-Forced	O.Abuse-Func	O.RND	O.AES
FCS_RNG.1/SICP								X	
FDP_IFC.1/SICP		X				X	X	X	
FDP_ITT.1/SICP		X				X	X	X	
FMT_LIM.1/SICP							X		
FMT_LIM.2/SICP							X		
FPT_FLS.1/SICP				X		X	X	X	
FPT_ITT.1/SICP		X				X	X	X	
FDP_SDC.1/SICP			X						
FDP_SDI.2/SICP					X				
FPT_PHP.3/SICP			X		X	X	X	X	
FRU_FLT.2/SICP				X		X	X	X	
FCS_COP.1/AES.SICP									X
FCS_CKM.4/AES.SICP									X

Table 23: Coverage of Security Objectives for the TOE's IC part by SFRs

257 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 23 are defined and handled in [11]. In particular, the rationale for these items and their correlation is given in [11] and not repeated here.

258 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						
FIA_AFL.1/PIN					X				

	O.Integrity	O.Confidentiality	O.Resp-COS	O.TSFDataExport	O.Authentication	O.AccessControl	O.KeyManagement	O.Crypto	O.SecureMessaging
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			
FIA_SOS.1					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		
FMT_MSA.1/SEF						X			
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			
FCS_RNG.1							X	X	
FCS_RNG.1/GR								X	
FCS_CKM.1/ AES.SM							X	X	X
FCS_CKM.1/ELC							X	X	
FCS_COP.1/SHA								X	

	O.Integrity	O.Confidentiality	O.Resp-COS	O.TSFDataExport	O.Authentication	O.AccessControl	O.KeyManagement	O.Crypto	O.SecureMessaging
FCS_COP.1/CB_HASH								X	
FCS_COP.1/ COS.AES								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 24: Mapping between Security Objectives for the TOE and SFRs

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

260 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.

261 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.

262 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.

263 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 and FPT_ITE.2: 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 TSF 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.

264 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 read, change 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.

265 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 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 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.

266 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 controls 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 authorised for specific commands.

267 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 profices a random number generator of a specific class for providing random numbers to the external world for future use.
- FCS_COP.1/SHA requires that the TSF provides different hashing algorithms that are referenced in the SFR.
- FCS_COP.1/CB_HASH 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.

268 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

269 Table 3 in BSI-CC-PP-0084-2014 [11], section 6.3.2 "Dependencies of security functional requirements" lists the security functional requirements defined in BSI-CC-PP-0084-2014, 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 BSI-CC-PP-0084-2014 [11].

270 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.

271 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.

272 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 on	fulfilled by
FDP_RIP.1	No dependencies.	n. a.
FDP_SDI.2	No dependencies	n.a.
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, FMT_MSA.3 Static attribute initialisation.	FDP_ACC.1/ MF_DF, FMT_MSA.3
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, FMT_MSA.3 Static attribute initialisation.	FDP_ACC.1/EF, 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, FMT_MSA.3 Static attribute initialisation.	FDP_ACC.1/TEF, FMT_MSA.3

SFR	dependent on	fulfilled by
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, FMT_MSA.3 Static attribute initialisation.	FDP_ACC.1/SEF, 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, FMT_MSA.3 Static attribute initialisation.	FDP_ACC.1/KEY, FMT_MSA.3
FMT_MSA.3	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles.	FMT_MSA.1/Life, FMT_MSA.1/SEF, FMT_MSA.1/PIN, FMT_MSA.1/Auth, FMT_SMR.1
FMT_SMF.1	No dependencies.	n. a.
FMT_MSA.1/Life	[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_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,	FDP_ACC.1/ MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY,

SFR	dependent on	fulfilled by
	FMT_SMF.1 Specification of Management Functions.	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 key generation], FCS_CKM.4 Cryptographic key destruction.	The dependent SFRs are not applicable here because FCS_COP.1/SHA does not use any keys.
FCS_COP.1/ COS.AES	[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/ AES.SM, FCS_CKM.4
FCS_CKM.1/ AES.SM	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction.	FCS_COP.1/ COS.AES, FCS_CKM.4
FCS_CKM.1/ELC	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction.	FCS_COP.1/ COS.ELC, FCS_COP.1/ COS.ECDSA.S, FCS_CKM.4
FCS_COP.1/ CB_HASH	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_COP.1 Cryptographic operation, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	The dependent SFRs are not applicable here because FCS_COP.1/CB_HASH does not use any keys.
FCS_COP.1/ COS.CMAC	[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	FCS_CKM.1/ AES.SM, FCS_CKM.4

SFR	dependent on	fulfilled by
	generation], FCS_CKM.4 Cryptographic key destruction.	
FCS_COP.1/ COS.RSA.S	[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/RSA, FCS_CKM.4
FCS_COP.1/ COS.ECDSA.S	[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/ELC, FCS_CKM.4
FCS_COP.1/COS.ECDSA.V	[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.	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. FCS_CKM.4
FCS_COP.1/ COS.RSA	[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/RSA FCS_CKM.4
FCS_COP.1/ COS.ELC	[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/ELC, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with	FCS_CKM.1/ AES.SM, FCS_CKM.1/RSA, FCS_CKM.1/ELC

SFR	dependent on	fulfilled by
	security attributes, or FCS_CKM.1 Cryptographic key generation].	
FTP_ITC.1/TC	No dependencies.	n. a.

Table 25: Dependencies of the SFR

6.3.3 Security Assurance Requirements Rationale

273 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, 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.

274 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.

275 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 done for the complete Protection Profile.

276 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.

277 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.

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

279 The augmentation of EAL4 chosen comprises the following assurance components:

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

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

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
TOE Security Assurance Requirements (only additional to EAL4)		
ALC_DVS.2	no dependencies	-

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
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 26: SAR Dependencies

7 Package RSA Key Generation

281 The COS supports additional cryptographic functionality related to RSA key generation according to Option_RSA_KeyGeneration in [21]. This section includes the Package RSA KeyGeneration in the present ST.

7.1 TOE Overview for Package RSA Key Generation

282 In addition to the TOE definition given in section 1.2.3 “TOE definition and operational usage” the TOE is equipped with further cryptographic functionality related to RSA key generation by the TOE.

7.2 Security Problem Definition for Package RSA Key Generation

7.2.1 Assets and External Entities

Assets

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

Subjects and external entities

284 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.

7.2.2 Threats

285 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.

7.2.3 Organisational Security Policies

286 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.

7.2.4 Assumptions

287 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.

7.3 Security Objectives for Package RSA Key Generation

288 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.

7.4 Security Requirements for Package RSA Key Generation

289 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.

290 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].

291 The TOE shall meet the requirement "Cryptographic key generation – RSA key generation" 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 FCS_COP.1 Cryptographic operation] 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 *G&D_RSAKeyGen* [344] and specified cryptographic key 2048 bit and 3072 bit modulo length[345] that meet the following TR-03116-1 [19][346].

7.5 Security Requirements Rationale for Package RSA Key Generation

292 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.

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

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

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

	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 27: Mapping between Security Objectives for the TOE and SFRs for Package RSA Key Generation

Table 27 above should be taken as extension of **Table 24** 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.

293 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.

294 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.

295 The following table lists the required dependencies of the SFR of this PP Package and gives the concrete SFRs from this document which fulfil the required dependencies. Hereby, **Table 28** should be taken as extension of **Table 25** 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

Table 28: Dependencies of the SFR for Package RSA Key Generation

8 Package Contactless

296 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 used by the TOE as part of its security functionality.

8.1 TOE overview for Package Contactless

297 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 dependend access rules in that case.

8.2 Security Problem Definition for Package Contactless

8.2.1 Assets and External Entities

Assets

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

Security Attributes of Users and Subjects

299 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.

300 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 29 User type of Package Contactless

8.2.2 Threats

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

8.2.3 Organisational Security Policies

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

8.2.4 Assumptions

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

8.3 Security Objectives for Package Contactless

304 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.

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

306 **O.PACE_Chip Protection of contactless communication with PACE/PICC**
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.

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

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

309 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.

8.4 Security Requirements for Package Contactless

310 In addition to the authentication reference data of the devices listed in **Table 15** 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)** Authentication reference data SCCO stored in the TOE and corresponding to the CAN, MAC session key SK4SM Security attributes *keyIdentifier* of the SCCO in the *globalSecurityList* if SCCO was in the MF or in *dfSpecificSecurityList* if the SCCO was in the respective folder 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.

User type / Subject type	Authentication data and security attributes	Operations
TOE as PICC	SK4SM referenced in macKey and *SSCmac*	SK4SM is used to generate MAC for command responses.

Table 30 Authentication data of the COS for Package Contactless

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

312 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 29** even if the Package Contactless is not included.

313 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 deterministic*[347] random number generator of **RNG class DRG.4[348] ([5], [6]) for PACE protocol** that implements:

(*DRG.4.1) The internal state of the RNG uses a PTRNG of class PTG.2 as a random source.*

(DRG.4.2) The RNG provides forward secrecy.

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

(DRG.4.4) The RNG provides enhanced forward secrecy for every call.

(DRG.4.5) The internal state of the RNG is seeded by a PTRNG of class PTG.2.[349]

FCS_RNG.1.2/PACE The TSF provide random numbers **octets of bits** that meet *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*[350].

314 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
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

347 [selection*: hyprid deterministic, hybrid physical*]

348 **[selection: *DRG.4, PTG.3*]**

349 [assignment: *list of security capabilities* ***of the selected RNG class***]

350 [assignment: *a defined quality metric of the selected RNG class*]

FCS_COP.1.1/PACE.PICC.ENC The TSF shall perform decryption and encryption for secure messaging[351] in accordance with a specified cryptographic algorithm AES in CBC mode[352] and cryptographic key sizes ***128 bit, 192 bit, 256 bit***[353] that meet the following: TR-03110 [16], COS specification [21][354].

315 *Application note 39*: 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.

316 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
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/PACE.PICC.MAC The TSF shall perform MAC calculation for secure messaging in accordance with a specified cryptographic algorithm CMAC and cryptographic key sizes ***128 bit, 192 bit, 256 bit*** that meet the following: TR-03110 [16], COS specification [21].

317 Application note 40: 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.

318 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
FCS_COP.1 Cryptographic operation]
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 ***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*** and specified cryptographic key sizes ***256 bit, 384 bit, 512 bit*** that meet the following: TR-03110 [16], TR-03111 [17].

319 *Application note 41*: The TOE exchanges a shared secret with the external entity during the PACE protocol, see [16]. This protocol is based on the ECDH compliant to TR-03111 [17] (i.e.

---

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

[352] [assignment: *cryptographic algorithm*]

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

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

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 TR03110 [16].

320 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 *overwriting the key value with 'FF' values* that meets the following: *none*.

321 *Application note 42*: The TOE destroys 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 clears 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.

322 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

(1) reading the ATS,

(2) to establish a communication channel,

(3) *to carry out the authentication mechanism*

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.

323 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

(1) reading the ATS,

(2) to establish a communication channel,

(3) actions allowed according to FIA_UID.1/PACE and FIA_UAU.1,

(4) *to carry out the authentication mechanism*

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.

324 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

(1) PACE Protocol in PCD role according to TR-03116-1 [19], COS specification [21].

325 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

(1) PACE protocol in PICC role according to [16] and [21] using command GENERAL AUTHENTICATE,

(2) secure messaging in MAC-ENC mode using PACE session keys according to [21], section 13, and [16], Part 3, in PICC role

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.

326 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.

327 *Application note 43*: 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).

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

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

(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,

(2) *SK4SM* referenced in *macKey* and *SSCmac*.

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.

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:

(1) The authentication state for the device after successful authentication using PACE protocol in PCD role is set to "authenticated" and

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,

b. the authentication reference data SK4SM is stored in macKey and SSCmac.

(2) If an authentication attempt using PACE protocol in PCD role failed

a. Executing GENERAL AUTHENTICATE for PACE Version 2 [16],

b. receiving commands failing the MAC verification or encryption defined for secure messaging,

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).

329 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 [selection: allocation of the resource to, deallocation of the resource from] the following objects:

(1) session keys (immediately after closing related communication session),

(2) any ephemeral secret having been generated during DH key exchange,

(3) *none*.

330 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
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
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 to transmit and receive user data in a manner protected from unauthorised disclosure.

331 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
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
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 to transmit and receive user data in a manner protected from modification, deletion, insertion, and replay errors.

FDP_UIT.1.2/ PACE The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, and replay has occurred.

332 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 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.

333 *Application note 44*: The trusted IT product is the terminal. In FTP_ITC.1.3/PACE.PICC, the word "initiate" is changed 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.

334 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

(1) the roles defined in FMT_SMR.1,

(2) PACE authenticated terminal,

(3) *none*.

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

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

FMT_MTD.1/PACE.PICC Management of TSF data – PACE/PICC

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/PACE.PICC The TSF shall restrict the ability to read the

(1) SCCO used for PACE protocol in PICC role,

(2) session keys of secure messaging channel established using PACE protocol in PICC role

to none.

336 *Application note 45*: 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.

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

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

(1) the public TSF data as defined in FPT_ITE.2.1

given the following conditions

(1) conditions as defined in FPT_ITE.2.1,

(2) no export of the SCCO.

FPT_ITE.2.2/ PACE The TSF shall use *structure and content of CV certificate according to 21 and access condition encoding schemes according to [29]* for the exported data.

338 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:

(1) for users defined in FIA_ATD.1,

(2) additionally for device: authentication state gained with SCCO.

339 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 about IC power consumption, electromagnetic radiation and command execution time* in excess of *non useful information* enabling access to

(1) Symmetric Card Connection Object (SCCO),

(2) PACE session keys,

(3) any ephemeral secret having been generated during DH key exchange,

(4) any object listed in FPT_EMS.1,

(5) none

and *none*.

FPT_EMS.1.2/PACE.PICC The TSF shall ensure any users are unable to use the following interface the contactless interface and circuit contacts to gain access to

(1) Symmetric Card Connection Object (SCCO),

(2) PACE session keys,

(3) any ephemeral secret having been generated during DH key exchange,

(4) any object listed in FPT_EMS.1,

(5) *none*

and *none*.

8.5 Security Requirements Rationale for Package Contactless

340 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.

	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			x
FIA_UAU.6/PACE.PICC					x				x
FIA_UID.1/PACE					x	x			x
FIA_USB.1/PACE.PICC					x	x			x
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 31 Mapping between Security Objectives for the TOE and SFRs for Package Contactless

341 **Table 31** above should be taken as extension of **Table 24** 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.

342 All SFRs of the Package Contactless are implementing security functionality for the Security Objective **O.PACE_Chip**.

343 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.

344 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.

345 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.

346 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.

347 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.2.

348 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.

349 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.

350 The following table lists the required dependencies of the SFRs of this ST Package and gives the concrete SFRs from this document which fulfil the required dependencies. Hereby, **Table 32** should be taken as extension of **Table 25** 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 control, or FDP_IFC.1 Subset information flow control]	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
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,
FDP_UIT.1/PACE	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information	FTP_ITC.1/PACE FDP_ACC.1/MF_DF,

SFR	dependent on	fulfilled by
	flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	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 32 Dependencies of the SFRs for Package Contactless

9 Package Crypto Box

351 The COS support additional cryptographic functionality according to [21]. This section defines the Package Crypto Box to be used by the TOE as part of its security functionality.

9.1 TOE Overview for Package Crypto Box

352 In addition to the TOE definition given in section 1.2.3 “TOE definition and operational usage” the TOE is equipped with further cryptographic functionality.

9.2 Security Problem Definition for Package Crypto Box

9.2.1 Assets and External Entities

Assets

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

Subjects and external entities

354 There are no additional external entities and subjects for the Package Crypto Box beyond those already defined in section 3.1.

9.2.2 Threats

355 There are no additional Threats for the Package Crypto Box beyond the Threats already defined in section 3.2.

9.2.3 Organisational Security Policies

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

9.2.4 Assumptions

357 There are no additional Assumptions for the Package Crypto Box beyond the Assumptions already defined in section 3.4.

9.3 Security Objectives for Package Crypto Box

358 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 Crypto Box. Therefore the Security Objective Rationale (section 4.3) is supplemented as well.

359 The TOE shall fulfil the Security Objective “Trusted channel (O.TrustedChannel)” as specified below.

O.TrustedChannel	**Trusted channel** The TOE supports trusted channel for protection of the confidentiality and the integrity for commands to be sent to

successfully authenticated device and receiving responses from this device on demand of the external application.

360 The operational environment of the TOE shall fulfil the Security Objective “Secure messaging support of external devices (OE.SecureMessaging)” as specified below.

OE.SecureMessaging **Secure messaging support of external devices**
The external device communicating with the TOE through a trusted channel supports device authentication with key derivation, secure messaging for received commands and sending responses.

361 The Security Objectives O.TrustedChannel and OE.SecureMessaging mitigate the Threat T.Intercept if the operational environment is not able to protect the communication by other means.

9.4 Security Requirements for Package Crypto Box

362 In addition to the authentication reference data of the devices and security attributes listed in Table 15 the following table defines for the TOE with Package Crypto Box the authentication reference data of subjects.

User type	Authentication data	Operations
Device	Symmetric authentication key	MUTUAL AUTHENTICATE, EXTERNAL AUTHENTICATE, PSO DECIPHER and PSO VERIFY CRYPTOGRAPHIC CHECKSUM used for trusted channel.

Table 33 Authentication data of the devices and security attributes

363 In addition to the authentication verification data of the devices and security attributes listed in Table 15 the following table defines for the TOE with Package Crypto Box the authentication reference data of subjects and the authentication verification data used by the TSF itself (cf. FIA_API.1).

User type / Subject type	Authentication data and security attributes	Operations
Device	**Trusted channel** Authentication reference data Session key SK4TC Security attributes *SK4TC referenced in keyReferenceList.macCalculation and keyReferenceList.dataEncipher*	The commands PSO VERIFY CRYPTOGRAPHIC CHECKSUM and PSO DECIPHER are used to authenticate the responses received after establishment of session keys SK4TC.
TSF	**Trusted channel** Authentication verification data Session key SK4TC Security attributes *SK4TC reference in keyReferenceList.macCalculation and keyReferenceList.dataEncipher*	The commands PSO COMPUTE CRYPTOGRAPHIC CHECKSUM and PSO ENCIPHER are used to generate the commands received by the authenticated PICC with secure messaging.

Table 34 Authentication data of the COS for Package Crypto Box

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

365 The TOE shall meet the requirement "Re-authenticating – Trusted channel (FIA_UAU.6/CB)" as specified below.

FIA_UAU.6/CB	Re-authenticating – Trusted channel
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1/CB	The TSF shall re-authenticate the ~~user~~ **sender of a message**[355] under the conditions (1) each message received after establishing the trusted channel by successful authentication by execution of a combination of INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE, or MUTUAL AUTHENTICATE or GENERAL AUTHENTICATE commands shall be verified as being sent by the authenticated device using the commands PSO VERIFY CRYPTOGRAPHIC CHECKSUM and PSO DECIPHER[356].

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

FIA_API.1/CB	Authentication Proof of Identity – Trusted channel
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1/CB	The TSF shall provide a (1) PSO ENCIPHER and PSO COMPUTE CRYPTOGRAPHIC CHECKSUM with SK4TC used for trusted channel commands[357] to prove the identity of the TSF itself[358] to an external entity.

367 The TOE shall meet the requirement "User-subject binding – Trusted channel (FIA_USB.1/CB)" as specified below.

FIA_USB.1/CB	User-subject binding – Trusted channel
Hierarchical to:	No other components.

[355] Refinement identifying the concrete user

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

[357] [assignment: *authentication mechanism*]

[358] [assignment: *object, authorised user or rule*]

Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1/CB	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: as defined in FIA_USB.1[359].
FIA_USB.1.2/CB	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: as defined in FIA_USB.1[360].
FIA_USB.1.3/CB	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: (1) If the message received in command PSO VERIFY CRYPTOGRAPHIC CHECKSUM fails the verification or the message received in command PSO DECIPHER fails the padding condition the authentication state of the user bound to the SK4TC is changed to "not authenticated" (i.e. the *keyReferenceList.macCalculation*, *keyReferenceList. dataEncipher* and the SK4TC are deleted). (2) none[361] [362].

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

FCS_COP.1/CB.AES	Cryptographic operation – CB AES
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 Cryptographic key destruction
FCS_COP.1.1/CB.AES	The TSF shall perform (1) encryption with negotiated key for command PSO ENCIPHER, (2) decryption with negotiated key for command PSO DECIPHER, (3) encryption and decryption for trusted channel a. PSO ENCIPHER, b. PSO DECIPHER,

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

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

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

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

(4) decryption with card internal key for command EXTERNAL AUTHENTICATE,

(5) encryption with card internal key for command INTERNAL AUTHENTICATE[363]

in accordance with a specified cryptographic algorithm AES in CBC mode[364] and cryptographic key sizes 128 bit, 192 bit, 256 bit[365] that meet the following: TR-03116-1 [19], COS Specification [21]21, FIPS 197 [33][366].

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

FCS_COP.1/CB.CMAC	Cryptographic operation – CB CMAC
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 Cryptographic key destruction
FCS_COP.1.1/CB.CMAC	The TSF shall perform

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

(2) computation and verification of cryptographic checksum for trusted channel

a. PSO COMPUTE CRYPTOGRAPHIC CHECKSUM,

b. PSO VERIFY CRYPTOGRAPHIC CHECKSUM,

(3) verification of cryptographic checksum for command EXTERNAL AUTHENTICATE[367]

in accordance with a specified cryptographic algorithm CMAC[368] and cryptographic key sizes 128 bit, 192 bit and 256 bit[369] that meet the following: TR-03116-1 [19], COS specification 21, [36][370].

---

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

[364] [assignment: *cryptographic algorithm*]

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

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

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

[368] [assignment: *cryptographic algorithm*]

[369] [assignment: *list of cryptographic key sizes*]

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

370 The TOE shall meet the requirement “Cryptographic operation – CB RSA (FCS_COP.1/CB.RSA)” as specified below.

FCS_COP.1/CB.RSA	Cryptographic operation – CB RSA
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 Cryptographic key destruction
FCS_COP.1.1/CB.RSA	The TSF shall perform encryption with stored key for command PSO ENCIPHER[371] in accordance with a specified cryptographic algorithm (1) for encryption: RSA-OAEP-Encrypt ([34] section 7.1.1), (2) for decryption: RSA-OAEP-Decrypt ([34] section 7.1.2)[372] and cryptographic key sizes 2048 bit and 3072 bit modulus length for RSA private key operation and 2048 bit modulus length for RSA public key operation[373] that meet the following: PKCS #1 [34] [374].

Application Note 2 (*ST writer*): Since FCS_COP.1.1/CB.RSA is related to the encryption operation with the command PSO ENCIPHER, the enumeration number (2) for decryption and cryptographic key sizes 2048 bits and 3072 bits modulus length for RSA private key operation is out of scope for the TOE.

371 The TOE shall meet the requirement “Cryptographic operation – CB ECC (FCS_COP.1/CB.ELC)” as specified below.

FCS_COP.1/CB.ELC	Cryptographic operation – CB ECC
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 Cryptographic key destruction
FCS_COP.1.1/CB.ELC	The TSF shall perform encryption with stored key for command PSO ENCIPHER[375] in accordance with a specified cryptographic algorithm ELC encryption with COS standard curves[376] and

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

[372] [assignment: *cryptographic algorithm*]

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

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

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

[376] [assignment: *cryptographic algorithm*]

cryptographic key sizes 256 bits, 384 bits, 512 bits[377] that meet the following: TR-03111 [17], section 4.3.1, 4.3.3 and 5.3.1.2 [378].

9.5 Security Requirements Rationale for Package Crypto Box

372 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 Crypto Box.

	O.Integrity	O.Confidentiality	O.Resp-COS	O.TSFDataExport	O.Authentication	O.AccessControl	O.KeyManagement	O.Crypto	O.SecureMessaging	O.TrustedChannel
FIA_API.1/CB										x
FIA_UAU.6/CB										x
FIA_USB.1/CB										x
FCS_COP.1/CB.AES								x		x
FCS_COP.1/CB.CMAC								x		x
FCS_COP.1/CB.ELC								x		
FCS_COP.1/CB.RSA								x		

Table 35 Mapping between Security Objectives for the TOE and SFRs for Package Crypto Box

373 **Table 31** above should be taken as extension of **Table 24** 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.

374 The Security Objective **O.TrustedChannel** "Trusted channel" requires cryptographic functionality for trusted channel support as described by the SFRs FIA_API.1/CB, FIA_UAU.6/CB, FIA_USB.1/CB, FCS_COP.1/CB.AES and FCS_COP.1/CB.CMAC:

- FIA_API.1/CB requires that the TSF authenticates themselves to the entity receiving communication through trusted channel.
- FIA_UAU.6/CB requires that the TSF to authenticate the entity sending communication through trusted channel.
- FIA_USB.1/CB requires that the TSF to bind the authentication state to the entity sending communication through trusted channel.
- FCS_COP.1/CB.AES requires that the TSF provides decryption and encryption using AES with different key sizes to be used in dedicated commands.

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

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

- FCS_COP.1/CB.CMAC requires that the TSF provides computation and verification of cryptographic checksums using the CMAC algorithm and different key sizes to be used in dedicated commands.

375 The Security Objective **O.Crypto** "Cryptographic functions" requires the provision of security services by implementation of secure cryptographic algorithms and protocols. The following SFRs provide additional cryptographic services:

- FCS_COP.1/CB.AES requires that the TSF provides decryption and encryption using AES with different key sizes to be used in dedicated commands.
- FCS_COP.1/CB.CMAC requires that the TSF provides computation and verification of cryptographic checksums using the CMAC algorithm and different key sizes to be used in dedicated commands.
- FCS_COP.1/CB.ELC requires that the TSF provides encryption capabilities based on ELC algorithms with different key sizes to be used in dedicated commands.
- FCS_COP.1/CB.RSA requires that the TSF provides encryption capabilities based on RSA algorithms with different modulus lengths to be used in dedicated commands.

376 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 32** should be taken as extension of **Table 25** and **Table 28** in order to cover all dependencies. In particular, **Table 32** provides necessary additional assignments for fulfilment of the dependencies that arise from the additional SFRs that are defined for this Package.

SFR	dependent on	fulfilled by
FIA_API.1/CB	No dependencies.	n.a.
FIA_UAU.6/CB	No dependencies.	n.a.
FIA_USB.1/CB	FIA_ATD.1 User attribute definition	FIA_ATD.1
FCS_COP.1/CB.AES	[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/AES.SM, FCS_CKM.4
FCS_COP.1/CB.CMAC	[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/AES.SM, FCS_CKM.4
FCS_COP.1/CB.ELC	[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/ELC, FCS_CKM.4

SFR	dependent on	fulfilled by
	FCS_CKM.4 Cryptographic key destruction	
FCS_COP.1/CB.RSA	[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/RSA FCS_CKM.4
FCS_CKM.1/RSA The TOE provides RSA key generation functionality, i.e. Package RSA Key Generation is applied.	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	In addition to Table 25 and Table 28: FCS_COP.1/CB.RSA

Table 36 Dependencies of the SFRs for Package Crypto Box

10 Package Logical Channel

377 The COS supports additional functionality for logical channels according to [21]. This section defines the Package Logical Channel to be used by the TOE as part of its security functionality.

10.1 TOE Overview for Package Logical Channel

378 In addition to the TOE definition given in section 1.2.3 “TOE definition and operational usage” the TOE is equipped with additional logical channels. The extension is purely functional.

10.2 Security Problem Definition for Package Logical Channel

10.2.1 Assets and External Entities

Assets

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

Subjects and external entities

380 There are no additional external entities and subjects for the Package Logical Channel beyond those already defined in section 3.1.

10.2.2 Threats

381 There are no additional Threats for the Package Logical Channel beyond the Threats already defined in section 3.2.

10.2.3 Organisational Security Policies

382 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.

383 *Application note 46*: The COS specification [21] describes the concept of logical channels in section 12.

10.2.4 Assumptions

384 There are no additional Assumptions for the Package Logical Channel beyond the Assumptions already defined in section 3.4.

10.3 Security Objectives for Package Logical Channel

385 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.

386 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.

387 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.

388 The Security Objectives O.LogicalChannel and OE.LogicalChannel implement the OSP.LogicalChannel.

10.4 Security Requirements for Package Logical Channel

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

390 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: (1) The authentication state for the context as specified in FIA_USB.1. (2) The authentication state for a context is bound to the logical channel the authentication took place[379].
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:

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

(1) If a new logical channel is opened the authentication state is "not authenticated" for all contexts within that logical channel[380].

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: (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. (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". (3) The execution of a DELETE command has to be rejected if more than one channel is open. (4) *none*[381].

391 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[382] on: (1) the subject FDP_ACF.1/EF and FDP_ACF.1/MF_DF, (2) the objects a. logical channel, b. objects as defined in FDP_ACF.1/EF, c. objects as defined in FDP_ACF.1/MF_DF, (3) the operation by command following a. command SELECT, b. command MANAGE CHANNEL to open, reset and close a logical channel[383].

392 The TOE shall meet the requirement "Security attribute based access control – Logical channel (FDP_ACF.1/LC)" as specified below.

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

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

382 [assignment: *access control SFP*]

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

FIA_ACF.1/LC	Security attribute based access control – Logical channel
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/LC	The TSF shall enforce the Logical Channel SFP[384] to objects based on the following: (1) the subjects as defined in FDP_ACF.1/EF and FDP_ACF.1/MF_DF with security attribute "logical channel", (2) the objects a. logical channel with channel number, b. as defined in FDP_ACF.1/EF and FDP_ACF.1/MF_DF with security attribute "shareable" [385].
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: (1) The command MANAGE CHANNEL is *ALWAYS allowed*[386]. (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. (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*[387].
FDP_ACF.1.3/LC	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[388].
FDP_ACF.1.4/LC	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: (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[389].

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

[385] [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*]

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

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

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

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

393 *Application note 47*: The COS specification [21] claims that the security attribute "shareable" is always TRUE.

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

FMT_MSA.3/LC	Static attribute initialisation – Logical channel
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1/LC	The TSF shall enforce the Logical Channel SFP[390] to provide restrictive[391] 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:** **(1) *currentFolder* is root,** **(2) *keyReferenceList, globalSecurityList, globalPasswordList, dfSpecificSecurityList, dfSpecificPasswordList bitSecurityList* are empty,** **(3) *SessionkeyContext.flagSessionEnabled* is set to *noSK,*** **(4) *seIdentifier* is #1,** **(5) *currentFile* is undefined.**
FMT_MSA.3.2/LC	The TSF shall allow the subjects allowed to execute the command LOAD APPLICATION[392] to specify alternative initial values to override the default values when an object or information is created.

10.5 Security Requirements Rationale for Package Logical Channel

395 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.

390 [assignment: *access control SFP, information flow control SFP*]

391 [selection, choose one of*: restrictive, permissive, [assignment: other property]*]

392 [assignment: *the authorised identified roles*]

	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 37 Mapping between Security Objectives for the TOE and SFRs for Package Logical Channel

396 Table 37 above should be taken as extension of Table 24 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 ST mandatory part section 6.1.7 and mapped to the TOE'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.

397 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.

398 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 38 should be taken as extension of Table 25 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 38 Dependencies of the SFRs for Package Logical Channel

11 Statement of Compatibility

399 This is a statement of compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST) of the Infineon chip platform IFX_CCI_000005h. This statement is compliant to the requirements of [8].

11.1 Classification of the Platform TSFs

400 A classification of TSFs of the Platform-ST has been made. Each TSF has been classified as 'relevant' or 'not relevant' for the Composite-ST.

TOE Security Functionality	Relevant	Not relevant
SF_DPM Device Phase Management	x	
SF_PS Protection against Snooping	x	
SF_PMA Protection against Modification Attacks	x	
SF_PLA Protection against Logical Attacks	x	
SF_CS Cryptographic Support	x	

Table 39 Classification of Platform-TSFs

401 All listed TSFs of the Platform-ST are relevant for the Composite-ST.

11.2 Matching statement

402 The TOE relies on fulfillment of the following implicit assumptions on the IC:

- Certified Infineon microcontroller IFX_CCI_000005h
- True Random Number Generation with PTG.2 classification according to AIS31 [6].
- Cryptographic support based on symmetric key algorithms (AES) with 128, 192, 256 bits (AES) key length.
- Cryptographic support based on asymmetric key algorithms (RSA, ECDSA) with 2048, 3072 bits (RSA modulus) and 256-512 bits (elliptic curve) key length, including key generation.

403 The rationale of the Platform-ST has been used to identify the relevant SFRs, TOE objectives, threats and OSPs. All SFRs, objectives for the TOEs, but also all objectives for the TOE-environment, all threats and OSPs of the Platform-ST have been used for the following analysis.

11.2.1 Security objectives

404 This Composite-ST has security objectives which are related to the Platform-ST. These are:

- O.Phys-Probing
- O.Malfunction
- O.Phys-Manipulation

- O.Abuse-Func
- O.Leak-Forced
- O.Leak-Inherent
- O.Identification
- O.RND
- O.Crypto
- O.AES
- O.SecureMessaging
- O.PACE_Chip
- O.TrustedChannel

405 The following platform objectives could be mapped to composite objectives:

- O.Phys-Probing
- O.Malfunction
- O.Phys-Manipulation
- O.Abuse-Func
- O.Leak-Forced
- O.Leak-Inherent
- O.Identification
- O.RND
- O.AES

406 These Platform-ST objectives can be mapped to the Composite-ST objectives as shown in the following table.

Platform-ST		O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Abuse-Func	O.Leak-Forced	O.Leak-Inherent	O.Identification	O.AES	O.RND
Composite-ST	O.Phys-Probing	x								
	O.Malfunction		x							
	O.Phys-Manipulation			x						
	O.Abuse-Func				x					
	O.Leak-Forced					x				
	O.Leak-Inherent						x			
	O.RND									x
	O.Identification							x		
	O.Crypto								x	x

Platform-ST		O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Abuse-Func	O.Leak-Forced	O.Leak-Inherent	O.Identification	O.AES	O.RND
	O.AES								x	
	O.SecureMessaging								x	
	O.PACE_Chip								x	x
	O.TrustedChannel								x	

Table 40 Mapping of objectives

407 The following Platform-ST objectives are not relevant for or cannot be mapped to the Composite-TOE:

- O.Cap_Avail_Loader is not relevant because the Composite-TOE is delivered only with deactivated Flash Loader.
- O.Authentication is not relevant because the Composite-TOE is delivered only with deactivated Flash Loader.
- O.Ctrl_Auth_Loader is not relevant because the Composite-TOE is delivered only with deactivated Flash Loader.
- O.Prot_TSF_Confidentiality is not relevant because the Composite-TOE is delivered only with deactivated Flash Loader.
- O.Mem Access is not relevant because the Composite-TOE does not use area based memory access control.
- O.Add-Functions is not relevant because the Composite-TOE does not use the cryptographic libraries of the HW-platform.
- None of the Security Objectives for the Environment are linked to the platform and are therefore not applicable to this mapping.

408 There is no conflict between security objectives of this Composite-ST and the Platform-ST [47].

11.2.2 Security requirements

11.2.2.1 Security Functional Requirements

409 This Composite-ST has the following platform-related SFRs:

- FCS_COP.1/COS.AES
- FCS_COP.1/COS.CMAC
- FCS_COP.1/PACE.PICC.ENC
- FCS_COP.1/PACE.PICC.MAC
- FCS_CKM.4/PACE.PICC
- FCS_COP.1/CB.CMAC
- FCS_COP.1/CB.AES

- FCS_CKM.4
- FCS_COP.1/AES.SICP
- FCS_CKM.4/AES.SICP
- FCS_CKM.1/RSA
- FCS_RNG.1
- FCS_RNG.1/GR
- FMT_LIM.1/SICP
- FMT_LIM.2/SICP
- FPT_EMS.1
- FPT_ITT.1/SICP
- FPT_PHP.3/SICP
- FDP_ITT.1/SICP
- FAU_SAS.1/SICP
- FRU_FLT.2/SICP
- FPT_FLS.1/SICP
- FDP_SDC.1/SICP
- FDP_SDI.2/SICP
- FDP_IFC.1/SICP
- FCS_RNG.1/SICP

410 The following Platform-SFRs could be mapped to Composite-SFRs:

- FAU_SAS.1
- FCS_COP.1/AES
- FCS_CKM.4/AES
- FCS_RNG.1/TRNG
- FMT_LIM.1
- FMT_LIM.2
- FDP_ITT.1
- FPT_ITT.1
- FPT_PHP.3
- FPT_FLS.1
- FRU_FLT.2
- FDP_SDC.1
- FDP_SDI.2
- FDP_IFC.1

411 They will be mapped as seen in the following table.

Platform-ST		FAU_SAS.1	FCS_COP.1/AES	FCS_CKM.4/AES	FCS_RNG.1/TRNG	FMT_LIM.1	FMT_LIM.2	FPT_ITT.1	FDP_ITT.1	FPT_PHP.3	FPT_FLS.1	FRU_FLT.2	FDP_SDC.1	FDP_SDI.2	FDP_IFC.1
Composite-ST	FAU_SAS.1/SICP	x													
	FCS_COP.1/COS.AES		x												
	FCS_COP.1/COS.CMAC		x												
	FCS_COP.1/PACE.PICC.ENC		x												
	FCS_COP.1/PACE.PICC.MAC		x												
	FCS_CKM.4/PACE.PICC			x											
	FCS_COP.1/CB.CMAC		x												
	FCS_COP.1/CB.AES		x												
	FCS_CKM.1/RSA				x										
	FCS_CKM.4			x											
	FCS_COP.1/AES.SICP		x												
	FCS_CKM.4/AES.SICP			x											
	FCS_RNG.1				x										
	FCS_RNG.1/GR				x										
	FCS_RNG.1/SICP				x										
	FMT_LIM.1/SICP					x									
	FMT_LIM.2/SICP						x								
	FPT_EMS.1							x	x						x
	FPT_ITT.1/SICP							x							
	FDP_ITT.1/SICP								x						
	FPT_PHP.3/SICP									x					
	FPT_FLS.1/SICP										x				
	FRU_FLT.2/SICP											x			
	FDP_SDC.1/SICP												x		
	FDP_SDI.2/SICP													x	
	FDP_IFC.1/SICP														x

Table 41 Mapping of SFRs

11.2.2.2 Assurance Requirements

412 The Composite-ST requires EAL 4 according to Common Criteria V3.1R5 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

413 The Platform-ST has been certified to EAL 6 according to Common Criteria V3.1 R5 augmented by: ALC_FLR.1.

414 As EAL 6 covers all assurance requirements of EAL 4 and the augmented assurance requiremens of the Composite ST, the Platform-ST cover all assurance requirements of the Composite ST.

11.2.3 Security Objectives for the Environment of the Platform-ST

415 The following table shows the mapping of the Platform-ST Security Objectives for the Operational Environment of the platform-ST to the OE. Of the TOE:

Platform-ST		OE.Resp-Appl	OE.Process-Sec-IC
	O.Resp_COS[393]	x	
	OE.Plat-COS	x	
	OE.Resp-ObjS	x	
	OE.Process-Card		x

Table 42 Mapping of OEs

416 The following Platform-ST Security Objectives for the Operational Environment are not relevant for or cannot be mapped to the Composite-TOE:

417 OE.Lim_Block_Loader Loader is not relevant because the Composite-TOE is delivered only with deactivated Flash Loader.

418 OE.TOE_Auth Loader is not relevant because the Composite-TOE is delivered only with deactivated Flash Loader.

419 OE.Loader_Usage Loader is not relevant because the Composite-TOE is delivered only with deactivated Flash Loader.

11.3 Analysis

420 Overall there is no conflict between security requirements of this Composite-ST and the Platform-ST.

[393] See 2.4 §48 and 4.2 §95

12 TOE summary specification

421 This chapter gives the overview description of the different TOE Security Functions composing the TSF.

12.1 TOE Security Functions

12.1.1 SF_AccessControl

422 The TOE provides access control mechanisms that allow the restriction of access to only specific users (world, human users, device) based on different security attributes.

423 The TOE allows the restriction of access based on following attributes:

Attributes bound to the logical channel:

- Security list (Global and DF, bit)
- Password list (Global and DF).
- Interface: Contact based or contactless.
- Session key context

Attributes bound to an object in the object system (MF, DF, Application, keys):

- Life cycle status.
- SE identifier.
- Interface dependent rule: Contact based or contactless

424 The TOE enforces access control for following operations:

- Commands for using keys (creation and verification of digitial signatures, tranciphering, enciphering, deciphering)
- Commands for using PINs (verification)
- Command for generating keys
- Command for the deletion of key objects
- Command for managing the security environment, PINs
- Commands for creation and deletion of objects
- Command for reading the fingerprint
- Command for reading the public keys
- Commands for reading data from files and writing data to files
- Command for selecting a file
- Commands for reading the security attributes of PIN/key objects
- Commands for reading Key/PIN-based security states that are evaluated by the TOE’s access control system

425 The access control mechanisms ensure that access rules can be defined and applied depending on the life cycle status, security environment and the used interface (i.e. contact based or contactless, where as contactless communication is not supported by the TOE).

426 All security attributes under access control are modified in a secure way so that no unauthorised modifications are possible.

427 The access control mechanism assures that the access to files, applications (MF, DF, EF) and keys is limited to specific roles and the privileged access is granted for specific commands depening on interface, life cycle state, security attributes and context (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, FDP_ACC.1/KEY, FDP_ACF.1/KEY, FDP_ACC.1/LC, FDP_ACF.1/LC).

428 The access control mechanism allows to manage and initalize security attributes and TSF data (PINs, keys) and to query and export certain security attributes in a restrictive way (FMT_SMF.1, FMT_MSA.1/Life, FMT_MSA.1/SEF, FMT_MSA.3, FMT_MTD.1/PIN, FMT_MSA.1/PIN, FMT_MTD.1/Auth, FMT_MSA.1/Auth, FMT_MTD.1/NE, FMT_MTD.1/ PACE.PICC, FMT_MSA.3/LC).

12.1.2 SF_Authentication

429 After activation or reset of the TOE no user is authenticated.

430 TSF-mediated actions on behalf of a user require the user's prior successful identification and authentication. This user authentication typically implies a device authentication where the device proofs its identity by proofing the ownership of a cryptographic key. TSF-mediated actions typically imply also a TOE identification and authentication.

431 The TOE contains a deterministic random number generator DRG.4 according to AIS20 [5] that provides random numbers used in the authentication. The seed for the deterministic random number generator is provided by a true random number generator PTG.2 of the underlying IC.

432 The TOE supports user and device authentication by the following means:

- PIN/PUK based authentication
- PACE Protocol
- Symmetric Authentication Mechanism based on AES
- Asymmetric Authentication Mechanism based on RSA, ECC

433 Proving the identity of the TOE is supported by the following means:

- Symmetric Authentication Mechanism based on AES
- Asymmetric Authentication Mechanism based on RSA, ECC

434 The TOE prevents reuse of authentication data related to:

- Symmetric Authentication Mechanism based on AES
- Asymmetric Authentication Mechanism based on RSA, ECC

435 After completion of the authentication protocol, the commands exchanged between terminal and TOE are transferred via secure messaging using the key previously agreed between the terminal and TOE during the authentication. This assures that after authentication user data in transit is protected from unauthorized disclosure, modification, deletion, insertion and replay attacks.

436 The authentication mechanism assures that the user and the TOE is successfully identified and authenticated before an action is performed which requires a user or TOE identification and

authentication before execution, verifies the secrets and handles authentication faiures. The TOE maintains security attributes for performing the authentication (FIA_ATD.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_API.1, FMT_SMR.1, FIA_USB.1, FIA_SOS.1, FIA_AFL.1/PIN, FIA_AFL.1/PUC, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE.PICC, FIA_UAU.5/PACE.PICC, FIA_UAU.6/PACE.PICC, FIA_USB.1/PACE.PICC, FMT_SMR.1/PACE.PICC, FIA_ATD.1/PACE, FIA_USB.1/LC, FIA_USB.1/CB, FIA_UAU.6/CB, FIA_API.1/CB).

12.1.3 SF_AssetProtection

437 The TOE supports the calculation of block check values for data integrity checking. These block check values are stored with persistently stored assets (user data) of the TOE as well as temporarily stored hash values for data to be signed.

438 The TOE hides information about IC power consumption and command execution time ensuring that no confidential information can be derived from this information. The TOE detects electromagnetic radiation with sensors.

439 The TOE implements asset protection by performing an integrity monitoring of sensitive data (key, PINs) stored in the object system. Moreover it implements protection mechanisms which assures that information about IC power consumption and command execution time are not emitted which may be used to figure out senstive data (keys, PIN/PUC) from the TOE. The TOE allows the export public data and prohibits the export of secrets, private keys, PIN/PUC and passwords. The TOE verifies the consistency of TSF data recieved from another trusted IT product by using CV certificates. The TOE assures that all resources containg senstive information (keys, passwords) which are deallocated are completely deleted. The TOE provides protection by setting a secure state if failures occure (FDP_SDI.2, FPT_ITE.2, FPT_TDC.1, FPT_EMS.1, FDP_RIP.1, FPT_FLS.1, FTP_ITC.1/TC). In a contactless communication user data are only transfered by the TOE to an external entity within a trusted channel isolated from other logical channels using PACE (FPT_ITE.2/PACE, FDP_RIP.1/PACE.PICC, FDP_UIT.1/PACE, FTP_ITC.1/PACE.PICC, FDP_UCT.1/PACE, FPT_EMS.1/PACE.PICC). The Wrapper exports all public keyauthentication reference data and all security attributes of the object system for all objects of the object system and for all commands. However, the TOE assures that secret data, private keys, secure messaging keys, passwords and PUCs cannot be exported (FPT_ITE.2).

12.1.4 SF_TSFProtection

440 The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency and temperature.

441 The TOE is resistant to physical tampering on the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

442 The TOE demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections. In the case of inconsistencies in the calculation of the block check values and fault injections during the operation of the TSF the TOE preserves a secure state.

443 The TOE provides protection by setting a secure state if failures occur. The TOE is able to compute a TOE implementation fingerprint which can be used to check the TOE integrity. It computes self-tests during the start-up and checks the integritity of the TSF data (FPT_TDC.1, FPT_ITE.1, FPT_FLS.1, FPT_TST.1).

12.1.5 SF_KeyManagement

444 The TOE supports onboard generation of cryptographic keys based on ECDH as well as generation of RSA and ECC key pairs. Moreover it supports the generation of session keys in authentication mechanisms (sym./asym. Crypto, PACE) which includes a session key negotiation.

445 The TOE supports overwriting the cryptographic keys with zero values as follows:

- any session keys after detection of an error in a received command by verification of the MAC
- any session keys before starting the communication with the terminal in a new power-on-session.
- any ephemeral secret having been generated during DH key exchange
- any secret cryptographic keys, private cryptographic keys and session keys after upon the deallocation of the key object resource.

446 For the cryptographic services the TOE is able to generate cryptographic keys based on random numbers and performs a destruction once the key is not used any more. (FCS_RNG.1, FCS_CKM.1/AES.SM, FCS_CKM.1/RSA, FCS_CKM.1/ELC, FCS_CKM.4, FCS_RNG.1/PACE, FCS_CKM.1/DH.PACE.PICC, FCS_CKM.4/PACE.PICC).

12.1.6 SF_CryptographicFunctions

447 The TOE supports secure messaging for protection of the confidentiality and the integrity of the commands received from a device and response data returned back to the device. Secure messaging is enforced by the TOE based on access conditions defined for an object of the TOE. The TOE supports asymmetric cryptographic algorithms to perform authentication procedures, signature computation and verifications, data decryption and encryption. The TOE supports also symmetric cryptographic algorithms to perform authentication procedures. The TOE includes hash functions in order to compute a hash value over defined data. The TOE is able to generate random and contains a deterministic random number generator DRG.4 according to AIS20 [5] that provides random numbers used in the authentication. The seed for the deterministic random number generator is provided by a true random number generator PTG.2 of the underlying IC.

448 The TOE provides cryptographic services which allows the enchipherment, decipherment, trancipherment, signature computation/verification based based on ECC and RSA, random number generation based on physical and hybrid deterministic generator PTG.2 and DRG.4, hash computation based on SHA algorithms, secure messaging and trusted channels based on AES, PACE, CMAC as well as computation and verification of cryptographic checksum (FCS_RNG.1, FCS_RNG.1/GR, FCS_COP.1/COS.CMAC, FCS_COP.1/COS.AES, FCS_COP.1/COS.RSA.S, FCS_COP.1/COS.ECDSA.S, FCS_COP.1/COS.ECDSA.V, FCS_COP.1/COS.RSA, FCS_COP.1/COS.ELC, FCS_COP.1/SHA, FTP_ITC.1/TC, FCS_COP.1/PACE.PICC.ENC, FCS_COP.1/PACE.PICC.MAC, FCS_COP.1/CB_HASH, FCS_COP.1/CB.AES, FCS_COP.1/CB.CMAC, FCS_COP.1/CB.ELC, FCS_COP.1/CB.RSA).

12.2 Assurance Measure

449 This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 6.2.

450 The following table lists the Assurance measures and references the corresponding documents describing the measures.

Assurance Measures	Description

AM_ADV	The representing of the TSF is described in the documentation for functional specification, in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation.
AM_AGD	The guidance documentation is described in the operational user guidance documentation and in the documentation for preparative procedures.
AM_ALC	The life-cycle support of the TOE during its development and maintenance is described in the life-cycle documentation including configuration management, delivery procedures, development security as well as development tools.
AM_ASE	This security target document includes the conformance claims, ST introduction, security objectives, security problem definition and TOE summary specification.
AM_ATE	The testing of the TOE is described in the test documentation.
AM_AVA	The vulnerability assessment for the TOE is described in the vulnerability analysis documentation.

Table 43 References of Assurance measures

12.3 Fulfilment of the SFRs

451 The following table shows the mapping of the SFRs to security functions of the TOE.

TOE SFR / Security Function	SF_AccessControl	SF_Authentication	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_CryptographicFunctions
FIA_UAU.4/PACE.PICC		x				
FIA_UAU.5/PACE.PICC		x				
FIA_UAU.6/PACE.PICC		x				
FTP_ITC.1/PACE.PICC			x			
FPT_ITE.2/PACE			x			
FMT_MTD.1/PACE.PICC	x					
FMT_SRM.1/PACE.PICC		x				
FDP_UCT.1/PACE			x			
FDP_UIT.1/PACE			x			
FIA_ATD.1/PACE		x				
FIA_UAU.1/PACE		x				
FIA_UID.1/PACE		x				

TOE SFR / Security Function	SF_AccessControl	SF_Authentication	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_CryptographicFunctions
FIA_USB.1/PACE.PICC		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_USB.1		x				
FIA_API.1		x				
FMT_SMR.1		x				
FDP_ACC.1/EF	x					
FDP_ACC.1/MF_DF	x					
FDP_ACC.1/TEF	x					
FDP_ACC.1/SEF	x					
FDP_ACC.1/KEY	x					
FDP_ACF.1/EF	x					
FDP_ACF.1/MF_DF	x					
FDP_ACF.1/TEF	x					
FDP_ACF.1/SEF	x					
FDP_ACF.1/KEY	x					
FMT_MSA.3	x					
FMT_SMF.1	x					
FMT_MSA.1/Life	x					
FMT_MSA.1/SEF	x					
FMT_MTD.1/PIN	x					
FMT_MSA.1/PIN	x					
FMT_MTD.1/Auth	x					
FMT_MSA.1/Auth	x					
FMT_MTD.1/NE	x					
FCS_RNG.1					x	x

TOE SFR / Security Function	SF_AccessControl	SF_Authentication	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_CryptographicFunctions
FCS_RNG.1/PACE					x	
FCS_RNG.1/GR						x
FCS_CKM.1/DH.PACE.PICC					x	
FCS_CKM.4/PACE.PICC					x	
FCS_COP.1/PACE.PICC.MAC						x
FCS_COP.1/PACE.PICC.ENC						x
FCS_COP.1/COS.CMAC						x
FCS_COP.1/COS.AES						x
FCS_CKM.1/AES.SM					x	
FCS_CKM.1/RSA					x	
FCS_CKM.1/ELC					x	
FCS_COP.1/SHA						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_COP.1.1/CB_HASH						x
FCS_COP.1/CB.AES						x
FCS_COP.1/CB.CMAC						x
FCS_COP.1/CB.ELC						x
FCS_COP.1/CB.RSA						x
FCS_CKM.4					x	
FIA_UID.1		x				
FIA_SOS.1		x				
FTP_ITC.1/TC			x			x
FDP_SDI.2			x			
FDP_RIP.1			x			
FDP_RIP.1/PACE.PICC			x			
FPT_FLS.1			x	x		
FPT_EMS.1			x			

TOE SFR / Security Function	SF_AccessControl	SF_Authentication	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_CryptographicFunctions
FPT_EMS.1/PACE.PICC			x			
FPT_TDC.1			x	x		
FPT_ITE.1				x		
FPT_ITE.2			x			
FPT_TST.1				x		
FIA_API.1/CB		x				
FIA_UAU.6/CB		x				
FIA_USB.1/CB		x				
FIA_USB.1/LC		x				
FIA_ACC.1/LC	x					
FDP_ACF.1/LC	x					
FMT_MSA.3/LC	x					

Table 44 Mapping of SFRs to mechanisms of TOE

12.3.1 Correspondence of SFRs and TOE mechanisms

452 Each TOE security functional requirement is implemented by at least one TOE mechanism. In section 11.1 TOE Security Functions the implementation of the TOE security functional requirements is described in form of the TOE mechanism.

13 Glossary and Acronyms

453 The terminology and abbreviations of Common Criteria version 3.1 [1], [2], [3], Revision 5 and the specification [21] apply.

Abbreviation	Term
ADF	Application Dedicated File
CAP	Composed Assurance Package
CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security
CM	Configuration Management
COS	Card Operating System
CSP-QC	Certification Service Provider for qualified certificates
CVC	Card Verifiable Certificate
EAL	Evaluation Assurance Level
EF	Elementary File
DF	Dedicated File, folder in a more general sense (refer to section 1.2.3)
eHC	electronic Health Care Card (elektronische Gesundheitskarte)
eHCT	electronic Health Card Terminal
eHPC	electronic Health Professional Card (elektronischer Heilberufsausweis)
gSMC-K	gerätespezifische Secure Module Card Type K
gSMC-KT	gerätespezifische Secure Module Card Type KT
IC	Integrated Circuit
MF	Master File
OS	Operating System
OSP	Organisational Security Policy
PC	Personal Computer
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PKI	Public Key Infrastructure
PP	Protection Profile
SAR	Security Assurance Requirement
SCA	Signature Creation Applications
SCD	Signature Creation Data
SEF	Structured Elementary File
SFP	Security Function Policy
SFR	Security Functional Requirement
SICP	Secure Integrated Chip Platform
SMC-B	Secure Modul Card Type B
SPD	Security Problem Definition
SSCD	Secure Signature-Creation Device

Abbreviation	Term
SVD	Signature Verification Data
ST	Security Target
TEF	Transparent Elementary File
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

14 Bibliography

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

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

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

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

[5] AIS20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[6] AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.0, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

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

[8] Joint Interpretation Library - Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018, JIL

[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

Protection Profiles

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

[12] not used

[13] not used

[14] not used

[15] not used

[50] BSI-CC-PP-0082-V4 Common Criteria Protection Profile -- Card Operating System Generation 2 (PP COS G2), Version 2.1, 10.07.2019

Technical Guidelines and Specification

[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] not used

[19] Technische Richtlinie TR-03116-1: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1:Telematikinfrastruktur, Version 3.20 vom 21.09.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[20] Technische Richtlinie BSI TR-03143: eHealth G2-COS Konsistenz-Prüftool, Version 1.1 vom 18.5.2017

[21] Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.13.1, 01.11.2019, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[22] not used

[23] not used

[24] not used

[25] not used

[26] not used

[27] Spezifikation Wrapper, Version 1.8.0, 24.08.2016, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

ISO Standards

[28] ISO/IEC 7816-3: 2006 (3rd edition), Identification cards — Integrated circuit cards —Part 3: Cards with contacts - Electrical interface and transmission protocols

[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

[30b] ISO/IEC 14443-4:2018 (4th edition), Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol

Cryptography

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

[32] (deleted)

[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] not used

[36] Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, May 2005 (includes updates as of 10-06-2016), 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, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology (NIST)

[38] (deleted)

[39] American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 16 November 16, 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 2015 (reaffirmed 10 February 2017), ANSI

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

Other Sources

[42] (shifted to [30b])

[43] not used

[44] not used

[45] not used

[46] not used

[47] Public Security Target BSI-DSZ-CC-1110-V3-2020, “Common Criteria Public Security Target EAL6 augmen ted / EAL6+ 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”, Infineon Technologies AG, Revision 1.8, 2020-04-22.