Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Protection Profile

Card Operating System Generation 2 (PP COS G2)

Common Criteria

BSI-CC-PP-0082-V3

Version 2.0 – 19 June 2018

Approved by the
Federal Office for Information Security

Foreword

This Protection Profile 'Card Operating System Generation 2 (PP COS G2)' is issued by Bundesamt für Sicherheit in der Informationstechnik, Germany.

The document has been prepared as a Protection Profile (PP) following the rules and formats of Common Criteria Version 3.1 Revision 5 [1], [2], [3].

Correspondence and comments to this Protection Profile should be referred to:

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn

Telefon: +49 2 28 99 95 82-0
Telefax: +49 2 28 99 95 82-54 00
E-Mail: bsi@bsi.bund.de

Document history

Version	Date	Changes	Comments
1.0	23 August 2013	Final version for evaluation.	
1.1	4 November 2013	Change of FIA_AFL.1/PIN and FMT_MTD.1/PIN in order to comply with COS specification. GET RANDOM moved to Package Logical Channel. FDP_SDI.2 added.	
1.2	20 November 2013	Package PACE for Proximity Coupling Device added.	
1.3	11 February 2014	Update of the Packages. Commands FINGERPRINT and LIST PUBLIC KEY added. FDP_SDI.2 for objects with transaction protection and access control rule for PSO VERIFY CERTIFICATE added.	
1.4	2 April 2014	Clarification on antenna added. Update of Table 15 and Package Crypto Box for trusted channel. FIA_SOS.1 added. Update of FIA_USB.1. FIA_API.1 adapted for BSI-CC-PP-0084. Access condition for command FINGERPRINT adapted in FDP_ACF.1/MF_DF. Refinement to ATE_FUN.1 and ATE_IND.2 adapted due to optional Packages and applications. Update of modulus length of RSA in FCS_COP.1/COS.RSA.V. Any subject allowed to execute the command PSO COMPUTE DIGITAL SIGNATURE.	
1.5	30 April 2014	Update due to BSI comments.	
1.6	4 June 2014	RSA 3072 public key operation removed due to change of COS specification.	
1.7	25 July 2014	Update of Certification-ID. Update of Table 19.	
1.8	10 October 2014	References updated. References to wrapper specification, BSI-CC-PP-0084 and JIL transition guide added. *dfSecurityList* substituted by *dfSpecificSecurityList*, *dfPasswordList* substituted by *dfSpecificPasswordList*. Security attributes of the object system included in Table 18. Update of FMT_SMF.1 and FMT_MSA.1.1/Life for LOAD APPLICATION.	
1.9	18 November 2014	Corrections due to BSI comments. Final version for evaluation / certification under BSI-CC-PP-0082-V2.	

Version	Date	Changes	Comments
2.0a	24 November 2017	Draft version for review. Update according to new version of the G2 COS specification (G2.1) and BSI TR-03143. Removal of DES-related functionality. Creation of the new Package for RSA-based CVC functionality. Switch from PP-0035 to PP-0084. Update due to eIDAS regulation instead of SigG/SigV. Technical and editorial corrections. Update of Bibliography.	
2.0b 2.0c 2.0d 2.0e 2.0f	9 March 2018 24 May 2018 25 May 2018 28 May 2018 8 June 2018	Draft version for review. Update according to a further new version of the G2 COS specification (G2.1). Creation of the new Package for RSA key generation. Technical and editorial corrections, in particular for consistency reasons. Update of Bibliography.	
2.0	19 June 2018	Final version for evaluation / certification under BSI-CC-PP-0082-V3.	

Contents

1 PP Introduction

1 This section provides document management and overview information required to register the Protection Profile and to enable a potential user of the PP to determine, whether the PP is of interest.

1.1 PP reference

Title:	Protection Profile 'Card Operating System Generation 2 (PP COS G2)'
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Editors:	T-Systems GEI GmbH, Bundesamt für Sicherheit in der Informationstechnik (BSI)
CC Version:	3.1 (Revision 5)
Assurance Level:	Assurance level for this Protection Profile is EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 (refer to section 6.3.3 for more details)
General Status:	final
Version Number:	2.0
Date:	19 June 2018
Registration:	BSI-CC-PP-0082-V3
Keywords:	eHealth, Gesundheitskarte, Card Operating System, Cards of Generation 2

1.2 TOE Overview

1.2.1 TOE definition and operational usage

2 The Target of Evaluation (TOE) addressed by the present Protection Profile is a smart card platform implementing the Card Operating System (COS) according to [21] without any object system. The TOE shall comprise at least

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 - if delivered - 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 (Card Operating System, COS)[2], including related configuration data

iii) the wrapper for interpretation of exported TSF Data,

iv) the associated guidance documentation,

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

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

v) the translation table (if applicable).

3 The TOE includes all executable code (including related configuration data) running on the Security IC Platform, i. e. IC Dedicated Support Software, the Card Operating System, application specific code loaded on the smart card by command LOAD CODE or any other means. The TSF of the TOE defined in an ST claiming conformance to this PP shall comprise all security functionality available after delivery of the TOE including vendor specific commands for initialisation, personalisation and operational usage allowed but not described in the specification of the COS [21]. This Protection Profile is written based on the COS specification [21] but also applicable to a COS meeting an updated version of this specification if this update does not change the security functionality specified in [21]. The wrapper interface is specified in [27]. Please consult the certification body for further information related to the validity of the PP due to updates of the specifications.

4 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 may export the TSF Data in a vendor specific format but the wrapper shall encode 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.

5 Optionally, the TOE developer may provide a so-called translation table for the TOE’s command set in the sense of the Technical Guideline BSI TR-03143 „eHealth - G2-COS Konsistenz-Prüftool“ [20] in order to support verification processes (conformity testing) for card products running on the TOE that are carried out by the verification tool. Such translation table is analysed for correctness in the framework of the TOE’s evaluation and appropriately signed by the evaluation body for integrity and authenticity purpose.

6 Note that, if the TOE supports contactless communication the inlay with antenna may be or may be not part of the TOE covered by the evaluation. The ST author shall provide precise definition of the physical scope of the TOE and the form in which the TOE is delivered to the costumer. The guidance documentation shall describe the security measures provided by the manufacturer and the security measures required for protection of the TOE until reception by the end-user.

7 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 initialised smart card product like an electronic Health Card (eHC [22]), an electronic Health Professional Card (eHPC [23]) or a Secure Module Card Type B (SMC-B [24]), K (gSMC-K [25]) and KT (gSMC-KT [26]).

[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.

1.2.2 TOE major security features for operational use

8 This smart card platform 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.

1.2.3 TOE type

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

10 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 may export the TSF Data in a vendor specific format but the wrapper shall encode 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.

11 Optionally, the TOE developer may provide a so-called translation table for the TOE's command set in the sense of the Technical Guideline BSI TR-03143 „eHealth - G2-COS Konsistenz-Prüftool" [20] in order to support verification processes (conformity testing) for card products running on the TOE that are carried out by the verification tool.

12 The typical life cycle phases for the present TOE type are IC and Smart Card 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 should be delivered with completely installed COS. Any patches of the COS may be delivered to the Smart Card Integrator for completion of the COS installation. Any smart card embedded software loaded after these processes

(i) changes the TOE if is part of the COS, or

(ii) is outside the TOE if is not part of the COS, and evidence shall be provided that this executable code cannot affect the security of the TOE.

13 Operational use of the TOE is explicitly in the focus of present PP. 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 PP. A security evaluation /certification being conform with this PP will have to involve all life cycle phases into consideration to the

[5] IC Manufacturing, Packaging and Testing

[6] including installation of the object system

extent as required by the Assurance Package chosen here for the TOE (see section 2.3 ‘Package Claim’ below).

1.2.4 Non-TOE hardware/software/firmware

14 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 [42].

1.2.5 Options and Packages

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

Option in [21]	**Package**	**Remark**
Option_Kryptobox	Crypto Box	Defines additional cryptographic SFRs (see section 7).
Option_kontaktlose_Schnittstelle	Contactless	Defines additional SFRs for the support of the contactless interface of the smart card, i.e. PICC part of PACE (see section 8).
Option_PACE_PCD	PACE for Proximity Coupling Device	Defines additional SFRs for the support of the contactless interface of the terminal, i.e. PCD part of PACE (see section 9).
Option_logische_Kanäle	Logical Channel	Defines additional SFRs for the support of logical channels (see section 10).
Option_USB_Schnittstelle	---	Defines additional communication support on the lower layers. This option does not contain any security related details and is therefore only listed in this table for the sake of completeness.
Option_RSA_CVC	RSA CVC	Defines additional cryptographic SFRs for the support of RSA functionality that is related to CVCs (see section 11).
Option_DES	---	For this option in [21] no corresponding Package is defined in this PP. This is carried out under consideration that DES based cryptographic functionality will not play a role for eHealth applications in future.
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

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

17 If the TOE implements one of these options the ST author must incorporate the corresponding Package definition with the update of the Security Problem Definition, Security Objectives, and the Security Requirements defined in that Package into the ST. Additionally, all rationales must be taken over into the ST.

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

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

2 Conformance Claims

2.1 CC Conformance Claim

20 This Protection Profile claims conformance to

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

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

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

21 as follows

- Part 2 extended,
- Part 3 conformant.

22 The

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

has to be taken into account.

2.2 PP Claim

23 This PP claims **strict** conformance to Protection Profile BSI-CC-PP-0084-2014 [11].

2.3 Package Claim

24 The present PP is conformant to the following Security Requirements Package: Assurance Package EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 as defined in the CC Part 3 [3].

2.4 Conformance Claim Rationale

25 This PP claims strict conformance to the BSI-CC-PP-0084-2014 [11].

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

27 The Assumptions A.Process-Sec-IC and A.Resp-Appl defined in BSI-CC-PP-0084-2014 [11] address the operational environment of the Security IC Platform, i.e. the COS part of the present

TOE and the operational environment of the present TOE. The aspects of these Assumptions are relevant for the COS part of the present TOE, address the development process of the COS and are evaluated according to the composite evaluation approach [8]. Therefore these Assumptions are now refined in order to address the Assumptions about the operational environment of the present TOE (cf. section 3.4 for details).

28 The Security Objectives for the Security IC Platform as defined in BSI-CC-PP-0084-2014 O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced, O.Abuse-Func, O.Identification, O.RND are included as Security Objectives for the present TOE. The Security Objective for the Operational Environment OE.Resp-Appl defined in BSI-CC-PP-0084-2014 is split into the Security Objective O.Resp-COS for the COS part of the TOE and the Security Objectives OE.Plat-COS and OE.Resp-ObjS for the object system in the operational environment of the TOE. In addition, the aspects relevant for the COS part of the present TOE shall be 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 section 4 for more details.

29 All Security Functional Requirements with existing refinements are taken over from BSI-CC-PP-0084-2014 into this PP 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.

30 If the Security IC Platform makes use of an optional Package in BSI-CC-PP-0084-2014 [11] and if such Package is relevant for the present TOE the ST author shall appropriately incorporate the respective Threats, OSPs, Objectives and SFRs of that Package in the ST and adapt the related rationales accordingly.

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

32 The refinements of the Security Assurance Requirements made in BSI-CC-PP-0084-2014 are taken over in this Protection Profile and must be applied to the Security IC Platform.

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

34 Therefore the strict conformance with BSI-CC-PP-0084-2014 [11] is fulfilled by this Protection Profile.

35 Note: The BSI-CC-PP-0035-2007 [46] was updated and replaced by BSI-CC-PP-0084-2014 [11]. The TOE may include a Security IC Platform certified with conformance to BSI-CC-PP-0035-2007 [46] if the transition guide [45] is taken into account and the ST provides appropriate rationale.

2.5 Conformance statement

36 This PP requires ***strict*** conformance of any ST or PP claiming conformance to this PP.

3 Security Problem Definition

3.1 Assets and External Entities

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

38 In section 3.1 “Description of Assets” in BSI-CC-PP-0084-2014 a high level description (in sense of this PP) 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.

39 In this Protection Profile these assets and the protection requirements of these assets are refined because

- the User Data defined in BSI-CC-PP-0084-2014 are User Data or TSF Data in the context of the present PP,
- 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.

40 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

41 Note: Elementary files (EF) may be stored in the MF, any Dedicated File (DF), Application or Application Dedicated File (ADF). The place of an EF in the file hierarchy defines features of the User Data stored in the EF. User Data do not affect the operation of the TSF (cf. CC Part 1, para

100). Cryptographic keys used by the TSF to verify authentication attempts of external entities (i.e. authentication reference data) including the verification of Card Verifiable Certificates (CVC) or authenticate itself to external entities by generation of authentication verification data in a cryptographic protocol are TSF Data (cf. **Table 13**, **Table 14** and **Table 17**)

42 This Protection Profile 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

43 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.

44 The following Threats are defined in BSI-CC-PP-0084-2014 [11]: T.Leak-Inherent, T.Phys-Probing, T.Malfunction, T.Phys-Manipulation, T.Leak-Forced, T.Abuse-Func, T.RND. All Threats are part of this Protection Profile and taken over into this PP. Please refer to 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

[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.

Threat name	Reference to paragraph in [11]	Short description
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 PP

45 If the Security IC Platform makes use of an optional Package in BSI-CC-PP-0084-2014 [11] and if such Package is relevant for the present TOE the ST author shall appropriately incorporate the respective Threats of that Package in the ST and adapt the related rationale accordingly.

46 Additionally, the following Threats for the TOE are defined:

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

48 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.

49 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.

50 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.

51 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.

52 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.

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

T.WrongRights **Wrong Access Rights for User Data or TSF Data**

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

3.3 Organisational Security Policies

54 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.

55 The following OSP is originally defined in BSI-CC-PP-0084-2014 [11]. The OSP is part of the aforementioned Protection Profile and is taken over into this PP for the present TOE. Note that the present PP 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 comparison 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 to [11].

OSP name	Short description	Reference to paragraph in [11]
P.Process-TOE	Identification during TOE Development and Production	90

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

56 If the Security IC Platform makes use of an optional Package in BSI-CC-PP-0084-2014 [11] and if such Package is relevant for the present TOE the ST author shall appropriately incorporate the respective OSPs of that Package in the ST and adapt the related rationale accordingly.

3.4 Assumptions

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

58 The Assumptions defined in BSI-CC-PP-0084-2014 [11] address the operational environment of the Security IC Platform, i.e. the COS part of the present TOE and the operational environment of the present TOE. The aspects of these Assumptions which are relevant for the COS part of the present TOE address the development process of the present TOE and are evaluated according to the composite evaluation approach [8]. Therefore, these Assumptions are now appropriately re-defined in order to address the Assumptions for the operational environment of the present TOE. **Table 6** lists and maps these Assumptions for the operational environment with the corresponding reference to [11].

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 Manufacturing’ or Phase 4 ‘IC Packaging’ the present TOE is delivered after Phase 5 ‘Composite Product Integration’ / ‘Smart Card Product

Assumptions defined in [11]	Reference to paragraph in [11]	Re-defined Assumptions for the operational environment of the present TOE	Rationale of the changes
			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

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

60 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.

61 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.

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

A.Process-Sec-SC	**Protection during Personalisation** 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

63 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

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

65 The following Security Objectives for the TOE are defined in BSI-CC-PP-0084-2014 [11]. The Security Objectives for the TOE are part of this Protection Profile and are taken over into this PP. 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 to [11].

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

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

66 If the Security IC Platform makes use of an optional Package in BSI-CC-PP-0084-2014 [11] and if such Package is relevant for the present TOE the ST author shall appropriately incorporate the respective Objectives of that Package in the ST and adapt the related rationale accordingly.

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

68 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.

69 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.

70 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.

71 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.

72 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.

73 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.

74 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.

75 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 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.

76 The TOE shall fulfil the Security Objective “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 the Operational Environment of the TOE

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

78 The following Security Objectives for the Operational Environment of the Security IC Platform are defined in BSI-CC-PP-0084-2014 [11]. The operational environment of the Security IC Platform as TOE in BSI-CC-PP-0084-2014 comprises the COS part of the present TOE and the operational environment of the present TOE. Therefore these Security Objectives for the Operational Environment are appropriately split and re-defined. The aspects relevant for the COS part of the present TOE shall be fulfilled in the development process of the COS and evaluated according to the composite evaluation approach [8]. The remaining aspects of the Security Objectives for the Operational Environment defined in BSI-CC-PP-0084-2014 are addressed in new Security Objectives for the Operational Environment of the present PP. 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 to [11].

Security Objectives for the Operational Environment defined in [11]	**Reference to paragraph in [11]**	**Re-defined Security Objectives for the Operational Environment of the present TOE**	**Rationale of the changes**
OE.Resp-Appl	117	OE.Resp-ObjS OE.Plat-COS	OE.Resp-Appl requires the Security IC Embedded Software

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
			to treat the User Data as required by the security needs of the specific application context. This Security Objective shall be ensured by the TOE and the object system.
OE.Process-Sec-IC	118	OE.Process-Card	The Security Objective defined for the environment of the Security IC Platform is appropriately re-defined for the present TOE.

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

79 If the Security IC Platform makes use of an optional Package in BSI-CC-PP-0084-2014 [11] and if such Package is relevant for the present TOE the ST author shall appropriately incorporate the respective Objectives of that Package in the ST and adapt the related rationale accordingly.

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

81 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.

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

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

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

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

4.3 Security Objective Rationale

84 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 taken over to the present PP as well as the Threats, Organisational Security Policies and Assumptions that are additionally defined or redefined in the present PP. 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.

85 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 PP are addressed by the respective Security Objectives. Please refer for the further details to the related justification provided in BSI-CC-PP-0084-2014 [11]. In addition, in view of the present PP 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
(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

Table 9: Security Objective Rationale related to the IC platform

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

- 'IC Development' (Phase 2) and 'IC Manufacturing' (Phase 3) are covered as development and manufacturing of the Security IC Platform and therefore of the TOE as well.

[9] Re-defined Assumption, see section 3.4

[10] Re-defined Assumption, see section 3.4

- ‘IC Packaging’ (Phase 4) may be part of the development and manufacturing environment or the operational environment of the Security IC Platform. Even if it is part of the operational environment of the Security IC Platform addressed by OE.Process-Sec-IC it will be part of the development and manufacturing environment of the present TOE and covered by the SAR ALC_DVS.2.
- ‘Composite Product Integration’ / ‘Smart Card Product Finishing’ (Phase 5) is addressed by OE.Process-Sec-IC but it is part of the development and manufacturing environment of the present TOE and covered by the SAR ALC_DVS.2.
- ‘Personalisation’ / ‘Smart Card Personalisation’ (Phase 6) up to the delivery of the smart card to the end-user is addressed by A.Process-Sec-IC and A.Process-Sec-SC and covered by OE.Process-Sec-SC.

87 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 **A.Resp-ObjS** that assumes all User Data and TSF Data of the TOE are treated in the object system as defined for its specific application context. The Security Objective for the Operational Environment **OE.Resp-ObjS** requires the object system to be defined as required by the security needs of the specific application context.

88 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, the present PP claims conformance to BSI-CC-PP-0084-2014 [11]. The Security Objectives, Assumptions, Organisational Security Policies (OSPs) 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.

89 The present PP defines new Threats and Assumptions for the TOE in comparison to the Security IC Platform as TOE defined in BSI-CC-PP-0084-2014 and 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

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

91 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.

92 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.

93 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.

94 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.

95 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.

96 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.

97 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.

98 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.

99 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.

100 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.

101 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

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

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

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

5.1 Definition of the Family FIA_API Authentication Proof of Identity

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

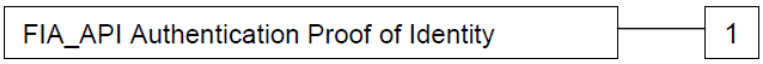
104 *Application note 3:* The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the extended family FIA_API from point of view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

FIA_API Authentication Proof of Identity

Family Behaviour

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

Component levelling



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

Management:	The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.
Audit:	There are no actions defined to be auditable.
FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FIA_API.1.1	The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment:*object, authorised user or role*] to an external entity.

5.2 Definition of the Family FPT_EMS TOE emanation

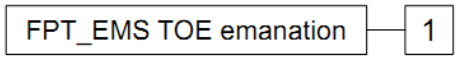
107 The family FPT_EMS (TOE emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT Security Functional Requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena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

FPT_EMS TOE emanation

Family Behaviour

108 This family defines requirements to mitigate intelligible emanations.

Component levelling



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

FPT_EMS.1.1	Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data
FPT_EMS.1.2	Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data
Management:	There are no management activities foreseen.
Audit:	There are no actions defined to be auditable.

FPT_EMS.1	**Emanation of TSF and User data**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMS.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

5.3 Definition of the Family FPT_ITE TSF image export

110 The family FPT_ITE (TSF image export) of the class FPT (Protection of the TSF) is defined here to describe the IT Security Functional Requirements of the TOE. This family defines rules for the export of TOE implementation fingerprints and of TSF Data in order to allow the verification of the correct implementation of the IC Dedicated Software and the COS of the TOE and the TSF Data of the smart card.

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

112 The export of all non-confidential TSF Data, e.g. data security attributes of subjects and objects and public authentication verification data like public keys, provides the ability to verify their correctness e.g. against an object system specification. The exported data must be correct, but do not need protection of confidentiality or integrity if the export is performed in a protected environment.

113 This family describes the functional requirements for the export of TOE implementation fingerprints and for the unprotected export of TSF Data not being addressed by any other component of CC Part 2 [2].

FPT_ITE TSF image export

Family Behaviour

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

Component levelling

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

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

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

FPT_ITE.1	**Export of TOE implementation fingerprint**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_ITE.1.1	The TOE shall export fingerprint of TOE implementation given the following conditions [assignment: *conditions for export*].
FPT_ITE.1.2	The TSF shall use [assignment: *list of generation rules to be applied by TSF*] for the exported data.
FPT_ITE.2	**Export of TSF data**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_ITE.2.1	The TOE shall export [assignment: *list of types of TSF data*] given the following conditions [assignment: *conditions for export*].
FPT_ITE.2.2	The TSF shall use [assignment: *list of encoding rules to be applied by TSF*] for the exported data.

6 Security Requirements

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

118 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 PP.

119 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 a interpretation refinement is given. In such a case a extra paragraph starting with "Refinement" is given.

120 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made [selection:] and are *italicised*.[11]

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

122 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.

123 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

124 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.

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

6.1.1 Overview

125 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:

Security Functional Groups	Security Functional Requirements concerned
Protection against Malfunctions	FRU_FLT.2/SICP, FPT_FLS.1/SICP
Protection against Abuse of Functionality	FMT_LIM.1/SICP, FMT_LIM.2/SICP, FAU_SAS.1/SICP
Protection against Physical Manipulation and Probing	FDP_SDC.1/SICP, FDP_SDI.2/SICP, FPT_PHP.3/SICP
Protection against Leakage	FDP_ITT.1/SICP, FPT_ITT.1/SICP, FDP_IFC.1/SICP
Generation of Random Numbers	FCS_RNG.1/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
Cryptographic Functions (section 6.1.7)	FCS_RNG.1, FCS_COP.1/SHA, FCS_COP.1/COS.AES, FCS_COP.1/COS.CMAC, FCS_CKM.1/AES.SM, FCS_CKM.1/ELC, FCS_COP.1/COS.RSA.S, FCS_COP.1/COS.ECDSA.V, FCS_COP.1/COS.ECDSA.S, FCS_COP.1/COS.RSA, FCS_COP.1/COS.ELC, FCS_CKM.4
Protection of communication (section 6.1.8)	FTP_ITC.1/TC

Table 12: Security functional groups vs. SFRs

126 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

127 The security attributes of human users are stored in password objects (cf. [21] for details). The human user selects the password object by *pwIdentifier* and therefore the role gained by the subject acting for this human user after successful authentication. The role is a set of access rights defined by the access control rules of the objects containing this *pwIdentifier*. The *secret* is used to verify the authentication attempt of the human user providing the authentication verification data. The security attributes *transportStatus, lifeCycleStatus* and *flagEnabled* stored in the password object define the status of the role associated with the password. E.g. if the *transportStatus* is equal to *Leer-PIN* or *Transport-PIN* the user is enforced to define his or her own password and making this password and this role effective (by changing the *transportStatus* to *regularPassword*). The multi-reference password shares the *secret* with the password identified by *pwReference*. It allows enforcing re-authentication for access and limitation of authentication state to specific objects and makes password management easier by using the same secret for different roles. The security attributes *interfaceDependentAccessRules, startRetryCounter, retryCounter, minimumLength* and *maximumLength* are defined for the *secret*. The PUC defined for the *secret* is intended for password management and the authorisation gained by successful authentication is limited to the command RESET RETRY COUNTER for reset of the *retryCounter* and setting a new *secret.*

128 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*	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

User type	Authentication reference data and security attributes	Comments
	startRetryCounter *retryCounter* *minimumLength* *maximumLength*	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 *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 (P1='00'), 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.

User type	Authentication reference data and security attributes	Comments
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.
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

129 The security attributes of devices depend on the authentication mechanism and the authentication reference data. A device may be associated with a symmetric cryptographic authentication key with a specific *keyIdentifier* and therefore the role gained by the subject acting for this device after successful authentication. The role is defined by the access control rules of the objects containing this *keyIdentifier*. A device may be also associated with a certificate containing the public key as authentication reference data and the card holder authorisation (*CHA*) in case of RSA-based CVC (if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the

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

TOE) or the card holder authorisation template (*CHAT*) in case of ELC-based CVC. The authentication protocol comprise the verification of the certificate by means of the root public key and command PSO VERIFY CERTIFICATE and by means of the public key contained in the successful verified certificate and the command EXTERNAL AUTHENTICATE. The subject acting for this device gets the role of the *CHA* (if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE) or *CHAT* which is referenced in the access control rules of the objects. The security attribute *lifeCycleStatus* is defined for persistently stored keys only.

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.
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* (*CHA*) for RSA keys (if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE) or	The following command is used by the TOE to authenticate a device: EXTERNAL AUTHENTICATE with *algID* equal to *rsaRoleCheck* (if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE) or *elcRoleCheck.* The following commands are used by the TOE to manage the authentication reference data: PSO VERIFY CERTIFICATE, ACTIVATE, DEACTIVATE, DELETE and TERMINATE.

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

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

User type	Authentication reference data and security attributes	Comments
	Certificate Holder Authorisation Template (CHAT) for ECC keys Security attributes in the certificate *Certificate Profile Identifier (CPI)* *Certification Authority Reference (CAR)* *Object Identifier (OID)*	
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

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

Subject type	Authentication verification data and security attributes	Operations
TSF	**Private authentication key** Authentication verification data *privateKey* Security attributes *keyIdentifier* *setAlgorithmIdentifier* with *algorithmIdentifier* *lifeCycleStatus*	The following commands are used by the TOE to authenticate themselves to an external device: INTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE.
TSF	**Secure messaging channel key** 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

131 The COS specification associates a subject with a *logical channel* and its *channelContext* (cf. [21], section 12). The TOE may support one subject respective logical channel or more than one independent subject or logical channel respectively, cf. section 10 Package Logical Channel. The *channelContext* comprises security attributes of the subject summarized in the following table.

Security attribute	**Elements**	**Comments**
interface		The TOE detects whether the communication uses contact-based interface (value set to *kontaktbehaftet*), or contactless interface (value set to *kontaktlos*)[16]. If the TOE does not support contactless communication the TOE shall behave as *interfaceDependentAccess Rules* is permanently set to "*kontaktbehaftet"*.
currentFolder		Identifier of the (unique) current folder.
	seIdentifier	Security environment selected by means of the command MANAGE SECURITY ENVIRONMENT[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.
	internalAuthenticate	*keyReference* and *algorithmIdentifier* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for authentication of the TSF itself by means of the command INTERNAL AUTHENTICATE.
	verifyCertificate	*keyReference* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for PSO VERIFY

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

[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
		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 (if the Package Crypto Box is supported by the TOE).
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 and PSO DECIPHER and PSO COMPUTE CRYPTOGRAPHIC CHECKSUM, PSO VERIFY CRYPTOGRAPHIC CHECKSUM (if the Package Crypto Box is supported by the TOE).
	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

Security attribute	Elements	Comments
		the session keys and if asymmetric key was used the *accessRight* associated with this key. The *keyIdentifier* may reference to the authentication reference data used for PACE[18] (if PACE is supported by the TOE).
	accessRulesSessionkeys	Access control rules associated with trusted channel support.
globalPasswordList	(*pwReference*, *securityStatusEvaluation-Counter*)	List of 0, 1, 2, 3 or 4 elements containing results of successful human user authentication with password in MF: *pwReference* and *securityStatusEvaluationCounter*.
dfSpecificPasswordList	(*pwReference*, *securityStatusEvaluation-Counter*)	List of 0, 1, 2, 3 or 4 elements containing results of successful human user authentication with password for each DF: *pwReference* and *securityStatusEvaluationCounter*.
globalSecurityList	*CHA* or *keyIdentifier*	List of 0, 1, 2 or 3 elements containing results of successful device authentication with authentication reference data in MF: *CHA* as reference to the role gained by authentication based on certificate (if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE) or *keyIdentifier* as reference to the used symmetric authentication key or *keyIdentifier* generated by successful authentication with PACE protocol (if PACE is supported by the TOE).
dfSpecificSecurityList	*CHA* or *keyIdentifier*	List of 0, 1, 2 or 3 elements containing results of successful device authentication with authentication reference data for each DF: *CHA* as reference to the role gained by authentication based on certificate (if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE) or *keyIdentifier* as reference to symmetric authentication key or *keyIdentifier* generated by successful authentication with PACE protocol (if PACE is supported by the TOE).
bitSecurityList		List of CHAT gained by successful authentication with CVC based on ECC. The effective access rights are the

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

Security attribute	Elements	Comments
		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.*
securityStatus-EvaluationCounter	*startSsec*	Must contain all values of *startSsec* and may be *empty.*

Table 17: Security attributes of a subject

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

Object type	Security attributes	Operations
Object system	*applicationPublicKeyList* *persistentCache* *pointInTime*	PSO VERIFY CERTIFICATE
Folder (8.3.1)	*accessRules:* *lifeCycleStatus* *shareable*[19] *interfaceDependentAccessRules* *children*	SELECT ACTIVATE DEACTIVATE DELETE FINGERPRINT GET RANDOM[20] 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 shortFileIdentifier* *lifeCycleStatus* *shareable*[21] *accessRules:* *interfaceDependentAccessRules*	SELECT ACTIVATE DEACTIVATE DELETE TERMINATE

[19] Available with Package Logical Channel

[20] Only available with Package Logical Channel

[21] Available with Package Logical Channel

Object type	Security attributes	Operations
	flagTransactionMode *flagChecksum*	
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 for Elementary File: *recordList* *maximumNumberOfRecords* *maximumRecordLength* *flagRecordLifeCycleStatus*	Additionally for Elementary File: ACTIVATE RECORD APPEND RECORD DELETE RECORD DEACTIVATE RECORD ERASE RECORD READ RECORD SEARCH RECORD SET LOGICAL EOF UPDATE RECORD
Regular Password (PIN) (8.4)	*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 (MR-PIN) (8.5)	*lifeCycleStatus* *pwdIdentifier* *accessRules:* *interfaceDependentAccessRules* *startSsecList* *flagEnabled* *passwordReference* Attributes used together with *referred password (PIN):* *secret: PIN* *minimumLength* *maximumLength*	Identical to Regular Password

Object type	Security attributes	Operations
	startRetryCounter *retryCounter* *transportStatus* *PUC* *pukUsage* channel specific: *securityStatusEvaluationCounter*	
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
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	Additionally for Public Asymmetric Key: *publicRsaKey: oid* or *publicElcKey:*	Additionally for Public Asymmetric Key: PSO VERIFY

Object type	Security attributes	Operations
(8.6.4.2)	*oid* *CHAT* *expirationDate: date*	CERTIFICATE, PSO VERIFY DIGITAL SIGNATURE
Public Asymmetric Key for authentication (8.6.4.3)	Additionally for Public Asymmetric Key: *publicRsaKey: oid* or *publicElcKey: oid* *CHA (if applicable for the TOE) / 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: *publicRsaKey: oid* *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 Authorisation (CHA (if applicable for the TOE) / CHAT)* *Object Identifier (OID)* *signature*	

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

133 The TOE must support Access control lists for

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

134 and may support Access control lists for

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

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

136 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]

137 The TOE access control rule contains

- command defined by CLA, 0 or 1 parameter P1, and 0 or 1 parameter P2,
- values of the *lifeCycleStatus* and *interfaceDependentAccessRules* indicating the set of access control rules to be applied,
- access control condition defined as Boolean expression with Boolean operators AND and OR of Boolean elements of the following types *ALWAYS*, *NEVER*, *PWD*(*pwIdentifier*), *AUT*(*keyReference*), *AUT*(*CHA*) (if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE), *AUT*(*CHAT*) and secure messaging conditions (cf. [21], section 10.2 for details).

138 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 provides the Boolean value FALSE. The other Boolean elements provide the Boolean value TRUE if the value in the access control list match its corresponding security attribute of the subject and provides the Boolean value FALSE is they do not match.

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

Operation	**SFR**	**Section**
ACTIVATE	FMT_SMF.1, FMT_MSA.1/Life	14.2.1
ACTIVATE RECORD	FMT_SMF.1, FMT_MSA.1/SEF	14.4.1
APPEND RECORD	FDP_ACC.1/SEF, FDP_ACF.1/SEF	14.4.2
CHANGE REFERENCE DATA	FIA_UAU.5, FIA_USB.1, FMT_SMF.1, FMT_MTD.1/PIN, FMT_MSA.1/PIN, FIA_AFL.1/PIN	14.6.1
CREATE	This command is optional and therefore not addressed in the SFRs of this PP.	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,	14.2.4

[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
	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*	
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 optional and therefore not addressed in the SFRs of this PP.	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*, *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[23], *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 optional and therefore not addressed in the SFRs of this PP.	14.5.1
GET PIN STATUS	FMT_SMF.1, FMT_MSA.1/PIN	14.6.4
GET RANDOM[24]	*FCS_RNG.1/GR*	10.4
GET RESPONSE	This command is optional and therefore not addressed in the SFRs of this PP.	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[25], FCS_COP.1/COS.RSA.S,	14.7.4

[23] If Package Crypto Box is supported by the TOE

[24] If Package Logical Channel is supported by the TOE

Operation	SFR	Section
	FCS_COP.1/COS.ECDSA.S, *FCS_COP.1/RSA.CVC.S*, *FCS_COP.1/CB.AES*, *FCS_COP.1/CB.CMAC*	
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[26]	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]	This command is optional and therefore not addressed in the SFRs of this PP.	-
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
PSO TRANSCIPHER USING ELC	FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3, FCS_COP.1/COS.RSA,	14.8.6.3

[25] If Package Crypto Box is supported by the TOE

[26] if Package Crypto Box is supported by the TOE

Operation	SFR	Section
	FCS_COP.1/COS.ELC	
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*	14.8.7
PSO VERIFY CRYPTOGRAPHIC CHECKSUM[27]	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 optional and therefore not addressed in the SFRs of this PP.	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 optional and therefore not addressed in the SFRs of this PP.	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 optional and therefore not addressed in the SFRs of this PP.	14.4.9

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

141 *Application note 4:* An implementation has to support the data types and the limits for the data types given in [21] exactly. If an implementation of COS supports additional values / types or extends limits it must be guaranteed that no Security Objective can be undermined. A justification

[27] if Package Crypto Box is supported by the TOE

for each additional difference and why it does not undermine a Security Objective has to be given from the developer.

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

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

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

144 All SFRs from section 6.1 ”Security Functional Requirements for the TOE” of BSI-CC-PP-0084-2014 are part of this PP. On each SFR of BSI-CC-PP-0014-2014 an iteration operation is performed. For the iteration operation, the suffix “/SICP” (short for: Secure Integrated Chip Platform) is added to the respective SFR name in BSI-CC-PP-0084-2014.

145 The complete list of the SFRs taken over from BSI-CC-PP-0084-2014 follows. For further descriptions, details, and interpretations refer to section 6.1 in BSI-CC-PP-0084-2014 [11].

- 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

146 **Table 20** maps the SFR name in the present PP to the SFR name in BSI-CC-PP-0084-2014 [11]. This approach allows an easy and unambiguous identification which SFR was taken over from the BSI-CC-PP-0084-2014 into this Protection Profile and which SFR is defined newly in the present PP.

SFR name	SFR name in [11]	Reference to paragraph in [11]
FRU_FLT.2/SICP	FRU_FLT.2	151
FPT_FLS.1/SICP	FPT_FLS.1	152
FMT_LIM.1/SICP	FMT_LIM.1	161
FMT_LIM.2/SICP	FMT_LIM.2	162
FAU_SAS.1/SICP	FAU_SAS.1	163
FDP_SDC.1/SICP	FDP_SDC.1	168
FDP_SDI.2/SICP	FDP_SDI.2	169
FPT_PHP.3/SICP	FPT_PHP.3	170
FDP_ITT.1/SICP	FDP_ITT.1	173
FPT_ITT.1/SICP	FPT_ITT.1	174
FDP_IFC.1/SICP	FDP_IFC.1	175
FCS_RNG.1/SICP	FCS_RNG.1	178

Table 20: Mapping between SFR names in this PP and SFR names in BSI-CC-PP-0084-2014 [11]

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

148 If the Security IC Platform makes use of an optional Package in BSI-CC-PP-0084-2014 [11] and if such Package is relevant for the present TOE the ST author shall appropriately incorporate the respective SFRs of that Package in the ST and adapt the related rationale and dependency analysis accordingly.

6.1.4 General Protection of User Data and TSF Data

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

FDP_RIP.1	Subset residual information protection
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: password objects, secret cryptographic keys, private cryptographic keys, session keys, [assignment: *other data objects*][28].

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

150 *Application note 7:* The author of the Security Target may want to use iterations of FDP_RIP.1 in order to distinguish between data, which must be deleted already upon deallocation and those which can be deleted upon allocation. It is recommended to delete secret/private cryptographic keys and all passwords upon deallocation. For secret User Data deletion upon allocation should be sufficient (depending on the resistance of the concrete TOE against physical attacks). Note that the COS specification allows management of applications during operational use. Therefore it is theoretically possible that a newly created object uses memory areas, which belonged to another object before. Therefore the COS must ensure that contents of the deleted objects are not accessible by reading the new object. The open assign operation may be "none".

151 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 [assignment: *integrity errors*] on all objects, based on the following attributes: (1) key objects, (2) PIN objects, (3) *affectedObject.flagTransactionMode=TRUE*, (4) [assignment: *other user data attributes*][29].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*].

152 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, (2) failure detected by TSF according to FPT_TST.1[30].

153 The TOE shall meet the requirement "FPT_EMS.1 (FPT_EMS.1)" as specified below (CC Part 2 extended).

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

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

FPT_EMS.1	Emanation of TSF and User data
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to 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) [assignment: *list of additional types of TSF data*][31] and the following user data (1) Private asymmetric keys, (2) Symmetric keys, (3) [assignment: *list of additional types of user data*][32].
FPT_EMS.1.2	The TSF shall ensure any user[33] are unable to use the following interface circuit interfaces[34] to gain access to the following TSF data (1) Regular password, (2) Multi-Reference password, (3) PUC, (4) Session keys, (5) Symmetric authentication keys, (6) Private authentication keys, (7) [assignment: *list of additional types of TSF data*][35] and the following user data (1) Private asymmetric keys, (2) Symmetric keys, (3) [assignment: *list of additional types of user data*][36].

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

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

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

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

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

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

154 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)[37] 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"[38] when interpreting the TSF data from another trusted IT product.

155 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][39].
FPT_ITE.1.2	The TSF shall use [selection: *SHA-256 based fingerprint of the TOE implementation*, *SHA-384 based fingerprint of the TOE implementation*, *SHA-512 based fingerprint of the TOE implementation*, *CMAC based fingerprint of the TOE implementation using [selection: AES-128, AES-192, AES-256] with cryptographic key size [selection: 128 bit, 192 bit, 256 bit] that meet the following standard [selection: FIPS180-4 [37], NIST SP800-38B [36]]*][40] for the exported data.

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

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

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

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

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

157 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) [assignment: *list of all TOE specific security attributes not described in COS specification [21]*][41] 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[42].
FPT_ITE.2.2	The TSF shall use [assignment: *list of encoding rules to be applied by TSF*] for the exported data.

158 *Application note 9*: The public TSF Data addressed as TSF Data in bullet (1) in the element FPT_ITE.2.1 covers at least all root public key and other public keys used as authentication reference data persistent stored in the object system (cf. *applicationPublicKeyList* and *persistentCache*) and exported by command LIST PUBLIC KEY (cf. [21], *persistentPublicKeyList* in [21] and [27], *applicationPublicKeyList* and *persistentCache* in [21]). The bullet (2) in the element FPT_ITE.2.1 covers all security attributes of the object system (cf. [21], (N019.900), [27], objectLocator 'E0') and of all objects of object types listed in **Table 18** and all TOE specific security attributes and parameters (except secrets). The COS specification [21] identifies optional functionality the TOE may support. The TOE (as COS, wrapper, translation table (if applicable), and guidance documentation) must support the user to find **all** objects and to export **all** security attributes of these objects. Note that while MF, DF and EF are hierarchically structured the Application and Application Dedicated File are directly referenced which may require special methods to find all objects in the object system. Note that the *listOfApplication* as security attribute of the object system contains at least one *applicationIdentifier* of each Application or Application Dedicated File (cf. [27]). The exported data shall be encoded by the wrapper to allow interpretation of the TSF Data. The encoding rules shall meet the requirements of the Technical Guideline BSI TR-03143 [20] describing the verification tool used for examination of the object system against the specification of the object system.

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

FPT_TST.1	TSF testing
Hierarchical to:	No other components.

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

42 [assignment: *conditions for export*]

Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up[43] to demonstrate the correct operation of the TSF[44].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[45].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of TSF[46].

6.1.5 Authentication

160 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*[47].

161 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[48] unsuccessful authentication attempts occur related to consecutive failed human user authentication for the PIN via VERIFY, ENABLE VERIFICATION REQUIREMENT, DISABLE VERIFICATION REQUIREMENT or CHANGE REFERENCE DATA command[49].
FIA_AFL.1.2/PIN	When the defined number of unsuccessful authentication attempts has been met[50], the TSF shall block the password for authentication until successful unblock using command RESET RETRY COUNTER

[43] [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]*]

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

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

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

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

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

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

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

(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[51].

162 *Application note 10:* The component FIA_AFL.1/PIN addresses the human user authentication by means of a password. The configurable positive integer of unsuccessful authentication attempts is defined in the password objects of the object system."Consecutive failed authentication attemps" are counted separately for each PIN and interrupted by successful authentication attempt for this PIN, i.e. the PIN object has a *retryCounter* wich is initially set to *startRetryCounter*, decremented by each failed authentication attempt and reset to *startRetryCounter* by successful authentication with the PIN or be successful execution of the command RESET RETRY COUNTER. The command RESET RETRY COUNTER (CLA,INS,P1)=(00,2C,02) and (CLA,INS,P1)=(00,2C,03) unblock the PIN without presenting unblocking code PUC of this password object. In order to prevent bypass of the human user authentication defined by the PIN or PUC the object system shall define access control to this command as required by the security needs of the specific application context, cf. OE.Resp-ObjS.

163 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[52] ~~unsuccessful~~[53] authentication attempts occur related to usage of a password unblocking code using the RESET RETRY COUNTER command[54].
FIA_AFL.1.2/PUC	When the defined number of ~~unsuccessful~~[55] authentication attempts has been met[56], the TSF shall [assignment: *list of actions, which at least includes: block the password unblocking code*][57].

164 *Application note 11:* The component FIA_AFL.1/PUC addresses the human user authentication by means of a PUC. The configurable positive integer of usage of password unblocking code is defined in the password objects of the object system.

51 [assignment: *list of actions*]

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

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

54 [assignment: *list of authentication events*]

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

56 [selection: *met, surpassed*]

57 [assignment: *list of actions*]

165 *Application note 12:* The command RESET RETRY COUNTER can be used to change a password or reset a retry counter. In certain cases, for example for digital signature applications, the usage of the command RESET RETRY COUNTER must be restricted to the ability to reset a retry counter only.

166 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: *pwdIdentifier* in *globalPasswordList* and *pwdIdentifier* in *dfSpecificPasswordList*, b. with Multi-Reference password: *pwIdentifier* in *globalPasswordList* and *pwIdentifier* in *dfSpecificPasswordList*, (2) for Device: authentication state gained a. 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[58].

167 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, (2) [selection: *GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, SELECT*], (3) commands with access control rule ALWAYS for the current life cycle status and depending on the interface, (4) [assignment: *list of additional TSF mediated actions*][59]

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

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.

168 *Application note 13:* ATR means Cold ATR and Warm ATR (cf. COS specification [21], (N019.900)b). The TOE may or may not define TOE specific access control rules for the commands GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT and SELECT, cf. COS specification [21], (N022.810). If the TOE does not define access control limitation for a command then the TOE shall allow the access for anybody (ALWAYS) and the ST author shall list the command in the element FIA_UAU.1.1.

169 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) [assignment: *additional identified authentication mechanism(s)*][60].

170 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,

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

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

(5) the execution of the MUTUAL AUTHENTICATE command,

(6) the execution of the GENERAL AUTHENTICATE command,

(7) a secure messaging channel,

(8) a trusted channel[61]

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) [assignment: *additional rules describing how the multiple authentication mechanisms provide authentication*][62].

171 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[63]** 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[64].

172 *Application note 14*: The entities establishing a secure messaging channel respective a trusted channel authenticate each other and agree symmetric session keys. The sender of a command authenticates its message by MAC calculation for the command (cf. PSO COMPUTE CRYPTOGRAPHIC CHECKSUM using SK4TC, cf. section 7 Package Crypto Box) and the receiver of the commands verifies the authentication by MAC verification of commands (using SK4SM). The receiver of the commands authenticates its message by MAC calculation (using SK4SM) and the sender of a command verifies the authentication by MAC verification of responses (cf. PSO VERIFY CRYPTOGRAPHIC CHECKSUM using SK4TC). If secure messaging is used with encryption the re-authentication includes the encrypted padding in the plaintext as authentication attempt of

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

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

63 Refinement identifying the concrete user

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

the message sender (cf. PSO ENCIPHER for commands) and the reciever (cf. secure messaging for responses) and verification of the correct padding as authentication verification by the message receiver (cf. secure messaging for received commands and PSO DECIPHER for received responses). The specification [21] states in section 13.1.2 item (N031.600): This re-authentication is controlled by the external entity (e.g. the connector in the eHealth environment). If no Secure Messaging is indicated in the CLA byte (see [ISO7816-4] Clause 5.1.1) and SessionkeyContext.flagSessionEnabled has the value SK4SM, then the security status of the key that was involved in the negotiation of the session keys MUST be deleted by means of clearSessionKeys(...).” Furthermore item (N031.700) states that the security status of the key that was involved in the negotiation of the session keys MUST be deleted by means of clearSessionKeys(...) if the check of the command CMAC (cf. FCS_COP.1/COS.CMAC) or Retail-MAC (cf. FCS_COP.1/COS.RMAC) fails. The TOE does not execute any command with incorrect message authentication code. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on a MAC, whether it was sent by the successfully authenticated communication partner. The TOE does not execute any command with incorrect MAC. Therefore, the TOE re-authenticates the communication partner connected, if a secure messaging error occurred, and accepts only those commands received from the initially communication partner.

173 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) [selection: *GET CHALLENGE*, *MANAGE CHANNEL*, *MANAGE SECURITY ENVIRONMENT*, *SELECT*], (3) commands with access control rule ALWAYS for the current life cycle status and depending on the interface, (4) [assignment: list of TSF mediated actions] [65] 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.

174 *Application note 15:* The TOE may or may not define TOE specific access control rules for the commands GET CHALLENGE, MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT and SELECT, cf. COS specification [21], (N022.810). If the TOE does not define access control limitation for these commands then the TOE shall allow the access for anybody (ALWAYS) and the ST author shall list the command in the element FIA_UID.1.1.

175 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)).

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

FIA_API.1	Authentication Proof of Identity
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide ~~a~~ (1) INTERNAL AUTHENTICATE, (2) MUTUAL AUTHENTICATE, (3) GENERAL AUTHENTICATE[66] to prove the identity of the TSF itself[67] to an external entity.

176 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 (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) [assignment: *additional authorised identified roles*][68].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

177 *Application note 16*: The Protection Profile BSI-CC-PP-0084-2014 does not explicitly define role because roles are linked to life cycle of the chip not addressed by SFR. Therefore the present PP defines the role "World" relevant for all parts of the TOE (e.g. physical protection) and roles for COS related SFR. The ST may add developer specific roles, e. g. for TSF Data export according to FPT_ITE.1.

178 *Application note 17*: Human users authenticate themselves by identifying the password or Multi-reference password and providing authentication verification data to be matched to the secret of the password object or PUC depending on the command used. The role gained by authorisation with a password is defined in the security attributes of the objects and related to identified commands. The authorisation status is valid for the same level and in the level below in the file

66 [assignment: *authentication mechanism*]

67 [assignment: *object, authorised user or rule*].

68 [assignment: *object, authorised identified roles*].

hierarchy as the password object is stored. The role gained by authentication with a symmetric key is defined in the security attributes of the objects and related to identified commands. The assignment may assign additional role like the role defined for authentication by means of PACE protocol (if PACE is supported by the TOE) or "none".

179 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), (5) for Device the Role authenticated by symmetric key: *keyIdentifier* and Authentication Context[69].
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[70].
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

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

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

or the context specific Multi-Reference password.

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

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

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

a. EXTERNAL AUTHENTICATE with symmetric or public keys,

b. MUTUAL AUTHENTICATE with symmetric or public keys,

c. GENERAL AUTHENTICATE with mutual ELC authentication and

d. GENERAL AUTHENTICATE for asynchronous secure messaging.

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

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

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

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

(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) [assignment: *further rules for the changing of attributes*][71].

180 *Application note 18:* Note that the security attributes of the user are defined by the authentication reference data. The user may chose security attributes of the subjects *interface* in the power on session and *seIdentifier* by execution of the command MANAGE SECURITY ENVIRONMENT for the current directory. The initial authentication state is set when the command SELECT is executed and the *newFile* is a folder (cf. [21], clause (N076.100) and (N048.200)).

6.1.6 Access Control

181 *Application note 19:* This section defines SFR for access control on User Data in the object system. The SFR FDP_ACF.1/MF_DF, FDP_ACF.1/EF, FDP_ACF.1/TEF, FDP_ACF.1/SEF and FDP_ACF.1/KEY describe the security attributes of the subject gaining access to these objects. The COS specification [21] describes the attributes of logical channels (i.e. subjects in CC terminology) which is valid for the core of COS including all Packages. The *globalSecurityList* and *dfSpecificSecurityList* contain all *keyIdentifier* used for successful device authentications, i.e. the list may be empty, may contain a CHA (if the RSA-based CVC functionality according to Option_RSA_CVC in [21] is supported by the TOE), a key identifier of a symmetric authentication key or CAN (in form of the *keyIdentifier* of the derived key) used with PACE if PACE is supported by the TOE. Because of this common structure there is no need for separate SFR in Package Contactless.

182 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[72] on (1) the subjects *logical channel* bind to users a. World, b. Human User, c. Device, d. Human User and Device, e. [assignment: *list of further subjects*], (2) the objects a. all executable code implemented by the TOE, b. MF,

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

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

c. Application,

d. Dedicated File,

e. Application Dedicated File,

f. persistent stored public keys,

g. [assignment*: list of further objects*],

(3) the operation by the following commands

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. [assignment*: all other operations applicable to MF and DF*][73].

183 *Application note 20*: Note that the commands ACTIVATE, DEACTIVATE and, TERMINATE DF for current file applicable to MF, DF, Application and Application Dedicated File manage the security life cycle attributes. Therefore access control to theses commands are described by FMT_MSA.1/Life. The object "all executable code implemented by the TOE" includes IC Dedicated Support Software, the Card Operating System and application specific code loaded on the smart card by command LOAD CODE or any other means (including related configuration data).

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

FDP_ACF.1/ MF_DF	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ MF_DF	The TSF shall enforce the access control MF_DF SFP[74] to objects based on the following (1) the subjects *logical channel* with security attributes a. *interface*, b. *globalPasswordList*, c. *globalSecurityList*, d. *dfSpecificPasswordList*,

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

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

e. *dfSpecificSecurityList*,

f. *bitSecurityList*,

g. *SessionkeyContext*,

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

(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. [assignment: *list of further objects listed in FDP_ACC.1.1/MF_DF with their security attributes*][75].

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

(2) GET CHALLENGE is [selection: *ALWAYS allowed*, *[assignment*: *supported access control rules]*].

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

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

(5) A subject is allowed to DELETE objects in the current folder MF

[75] [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*]

if the security attributes *interface*, *globalPasswordList*, *globalSecurityList* and *SessionkeyContext* of the subject meet the access rules for the command DELETE of the MF dependent on *lifeCycleStatus, seIdentifier* and *interfaceDependentAccessRules*.

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

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

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

(9) [assignment*: further list of subjects, objects, and operations among subjects and objects covered by the SFP*][76].

FDP_ACF.1.3/ MF_DF	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[77].
FDP_ACF.1.4/ MF_DF	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment*: rules, based on security attributes, that explicitly deny access of subjects to objects*].

185 *Application note 21:* The object system defines sets of access control rules depending on the life cycle status, security environment and the used interface (i.e. contact-based or contactless interface). The security environment may be chosen for the current folder by means of the command MANAGE SECURITY ENVIRONMENT. The command SELECT is therefore pre-requisite for many other commands. The access control rule defines for each command, which is defined by CLA, INS, P1 and P2 and acceptable for the type of the object, the necessary security state, which is reached by successful authentication of human user and devices, to allow the access to the selected object. Note that the command FINGERPRINT processes the data representing the TOE implementation like User Data (i.e. hash value calculation, no execution or interpretation as code) and is developer specific. Therefore, the ST author shall describe the TOE specific access control rules for these commands. The ST author shall perform the open operations whereby "none" is allowed.

186 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.

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

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

Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/EF	The TSF shall enforce the access control EF SFP[78] on

(1) the subjects *logical channel* bind to users
   a. World,
   b. Human User,
   c. Device,
   d. Human User and Device,
   e. [assignment: *list of further subjects*],

(2) the objects
   a. EF,
   b. Transparent EF,
   c. Structured EF,
   d. [assignment*: list of further objects*],

(3) the operation by the following commands
   a. SELECT,
   b. DELETE of the current file,
   c. [assignment*: further operations*][79].

187 *Application note 22*: Note that the commands ACTIVATE, DEACTIVATE and, TERMINATE DF for current file applicable to EF, Transparent EF and Structured EF manage the security life cycle attributes. Therefore access control to 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.

188 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[80] to objects based on the following

(1) the subjects *logical channel* with security attributes

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

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

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

a. *interface*,
b. *globalPasswordList*,
c. *globalSecurityList*,
d. *dfSpecificPasswordList*,
e. *dfSpecificSecurityList*,
f. *bitSecurityList*,
g. *SessionkeyContext*,
h. [assignment*: further subjects listed in FDP_ACC.1.1/EF*],

(2) the objects
a. EF with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules* of the EF, and [selection*: transaction mode, checksum*],
b. [assignment: *list of further objects listed in FDP_ACC.1.1/EF with their security attributes*][81].

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 [selection: *ALWAYS allowed*, *[assignment*: *supported access control rules]*].
(2) A subject is allowed to DELETE the current EF if the security attributes *interface*, *globalPasswordList*, *globalSecurityList*, *dfSpecificPasswordList*, *dfSpecificSecurityList* and *SessionkeyContext* of the subject meet the access rules for the command DELETE of this object dependent on *lifeCycleStatus*, *interfaceDependentAccessRules* and *seIdentifier* of the current folder.
(3) [assignment: *further list of subjects, objects, and operations among subjects and objects covered by the SFP*][82].

FDP_ACF.1.3/EF The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[83].

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

189 *Application note 23*: The EF stands here for transparent EF and structured EF, which access control is further refined by FDP_ACF.1/TEF and FDP_ACF.1/SEF. The selection of "transaction mode" (*flagTransactionMode*) and "checksum" (*flagChecksum*) may be empty because they are optional in the COS specification [21].

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

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

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

190 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[84] on

(1) the subjects *logical channel* bind to users
   a. World,
   b. Human User,
   c. Device,
   d. Human User and Device,
   e. [assignment: further *subjects*],

(2) the objects
   a. Transparent EF,
   b. [assignment*: list of further objects*],

(3) the operation by the following commands
   a. ERASE BINARY,
   b. READ BINARY,
   c. SET LOGICAL EOF,
   d. UPDATE BINARY,
   e. WRITE BINARY,
   f. [assignment*: further operation*][85].

191 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[86] to objects based on the following

(1) the subjects *logical channel* with security attributes
   a. *interface*,

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

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

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

b. *globalPasswordList*,

c. *globalSecurityList*,

d. *dfSpecificPasswordList*,

e. *dfSpecificSecurityList*,

f. *bitSecurityList*,

g. *SessionkeyContext*,

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

(2) the objects

a. with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules* of the current Transparent EF, and [selection*: transaction mode*, *checksum*],

b. [assignment: *list of further objects listed in FDP_ACC.1.1/TEF*][87].

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 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) [assignment: *further list of subjects, objects, and operations among subjects and objects covered by the SFP*][88].

FDP_ACF.1.3/TEF The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[89].

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 [assignment*: additional rules, based on security attributes, that explicitly deny access of subjects to objects*][90].

192 *Application note 24*: The selection of "transaction mode" (*flagTransactionMode*) and "checksum" (*flagChecksum*) may be empty because they are optional in the COS specification [21]. If the checksum of the data to be read by READ BINARY is malicious the TOE must append a warning when exporting. Exporting of malicious data should be taken into account by the evaluator during evaluation of class AVA: vulnerability assessment.

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

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

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

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

193 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[91] on (1) the subjects *logical channel* bind to users a. World, b. Human User c. Device d. Human User and Device, e. [assignment: further *subjects*], (2) the objects a. record in Structured EF b. [assignment*: list of further objects*], (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. [assignment*: further operation*][92].

194 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.

195 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[93] to objects based on the following

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

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

(1) the subjects *logical channel* with security attributes

a. *interface*,

b. *globalPasswordList*,

c. *globalSecurityList*,

d. *dfSpecificPasswordList*,

e. *dfSpecificSecurityList*,

f. *bitSecurityList*,

g. *SessionkeyContext*,

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

(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. [assignment: *list of further objects listed in FDP_ACC.1.1/SEF*][94].

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) [assignment: *further list of subjects, objects, and operations among subjects and objects covered by the SFP*][95].

FDP_ACF.1.3/SEF The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.[96].

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 [assignment*: additional rules, based on security attributes, that explicitly deny access of subjects to objects*][97].

---

93 [assignment: *access control SFP*]

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

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

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

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

196 *Application note 25*: Keys can be TSF or User Data. As SFR FDP_ACC.1/KEY and FDP_ACF.1/KEY address protection of User Data the keys defined in these SFR as objects are user keys only. Keys used for authentication are TSF Data and are therefore not in the scope of these two SFR. Please note that the PSO ENCIPHER, PSO DECIPHER, PSO COMPUTE CRYPTOGRAPHIC CHECKSUM, and PSO VERIFY CRYPTOGRAPHIC CHECKSUM are used with the SK4TC for trusted channel. If these commands are used in the context trusted channel the key used is TSF Data and not User Data. Therefore the SFR FDP_ACC.1/KEY and FDP_ACF.1/KEY are not applicable on the commands used for trusted channel. The commands PSO COMPUTE CRYPTOGRAPHIC CHECKSUM, and PSO VERIFY CRYPTOGRAPHIC CHECKSUM are required if the TOE supports the Package Crypto Box.

197 *Application note 26*: If the checksum of the record to be read by READ RECORD is malicious the TOE must append a warning when exporting. Exporting of malicious data should be taken into account by the evaluator during evaluation of class AVA: vulnerability assessment.

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

FDP_ACC.1/KEY	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/KEY	The TSF shall enforce the access control key SFP[98] on (1) the subjects *logical channel* bind to users a. World, b. Human User c. Device d. Human User and Device, e. [assignment: further *subjects*], (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. [assignment*: list of further objects*], (3) the operation by the following commands a. DELETE for private, public and symmetric key objects, b. MANAGE SECURITY ENVIRONMENT,

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

c. GENERATE ASYMMETRIC KEY PAIR,

d. PSO COMPUTE DIGITAL SIGNATURE,

e. PSO VERIFY DIGITAL SIGNATURE,

f. PSO VERIFY CERTIFICATE,

g. PSO ENCIPHER,

h. PSO DECIPHER,

i. PSO TRANSCIPHER,

j. PSO COMPUTE CRYPTOGRAPHIC CHECKSUM if supported by the TOE,

k. PSO VERIFY CRYPTOGRAPHIC CHECKSUM if supported by the TOE,

l. [assignment*: further operation*][99].

199 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[100] 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. [*assignment: further subjects listed in FDP_ACC.1.1/KEY*],

(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,

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

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

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,

g. [assignment: *list of further objects listed in FDP_ACC.1.1/KEY*][101].

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 [selection: *ALWAYS allowed*, *[assignment*: *supported access control rules]*] in cases defined in FDP_ACF.1.4/KEY.

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

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

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

a. the security attributes *interface*, *globalPasswordList*, *globalSecurityList*, *dfSpecificPasswordList*, *dfSpecificSecurityList* and *SessionkeyContext* of the subject meet the access rules for the command PSO VERIFY CERTIFICATE of the signature public key to be used for

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

verification of the signature of the CVC dependent on *seIdentifier* of the *current folder, lifeCycleStatus, key type* and *interfaceDependentAccessRules*,

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

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

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

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

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

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

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

lifeCycleStatus, the *key type* and *interfaceDependentAccessRules*.

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

(12) [assignment: *further list of subjects, objects, and operations among subjects and objects covered by the SFP*][102].

FDP_ACF.1.3/KEY The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[103].

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) [assignment*: rules, based on security attributes, that explicitly deny access of subjects to objects*][104].

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

(4) Management of access control security attributes by means of the

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

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

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

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) [assignment: *list of further management functions to be provided by the TSF*][105].

201 *Application note 27*: The Protection Profile BSI-CC-PP-0084-2014 [11] describes initialisation and personalisation as management functions. The ST author shall assign the COS commands dedicated for these management functions.

202 *Application note 28*: LOAD APPLICATION creates new objects together with their TSF Data (cf. FMT_MSA.1/Life). In case of folders this includes authentication reference data as passwords and public keys. CREATE is an optional command. The ST author should add it to the commands for the Life Cycle Management listed in FMT_SMF.1 and FMT_MSA.1/Life if implemented.

203 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[106] to restrict the ability to (1) create[107] **all** security attributes of the new object DF, Application, Application Dedicated File, EF, TEF and SEF[108] to subjects allowed to execute the command LOAD APPLICATION for the MF, DF, Application, Application Dedicated File where the new object is created[109],

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

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

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

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

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

(2) **change[110] the security attributes of the object MF, DF, Application, Application Dedicated File, EF, TEF and SEF[111] by means of the command LOAD APPLICATION to [selection*: none, subjects allowed to execute the command LOAD APPLICATION for the MF, DF, Application, Application Dedicated File where the object is updated*]**[112]**,**

(3) **change[113] the security attributes *lifeCycleStatus* to „*Operational state (active)*“[114] to subjects allowed to execute the command ACTIVATE for the selected object[115],**

(4) **change[116] the security attributes *lifeCycleStatus* to „*Operational state (deactivated)*“[117] to subjects allowed to execute the command DEACTIVATE for the selected object[118],**

(5) **change[119] the security attributes *lifeCycleStatus* to „*Termination state*”[120] to subjects allowed to execute the command TERMINATE for the selected EF, the key object or the password object[121],**

(6) **change[122] the security attributes *lifeCycleStatus* to „*Termination state*”[123] to subjects allowed to execute the command TERMINATE DF for the selected DF, Application or Application Dedicated File[124],**

(7) **change[125] the security attributes *lifeCycleStatus* to „*Termination state*”[126] to subjects allowed to execute the command TERMINATE CARD USAGE[127],**

(8) **query[128] the security attributes *lifeCycleStatus* by means of the command SELECT[129] to [selection: *ALWAYS allowed,***

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

111 [assignment: *list of security attributes*]

112 [assignment: *the authorised identified roles*]

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

114 [assignment: *list of security attributes*]

115 [assignment: *the authorised identified roles*]

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

117 [assignment: *list of security attributes*]

118 [assignment: *the authorised identified roles*]

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

120 [assignment: *list of security attributes*]

121 [assignment: *the authorised identified roles*]

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

123 [assignment: *list of security attributes*]

124 [assignment: *the authorised identified roles*]

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

126 [assignment: *list of security attributes*]

127 [assignment: *the authorised identified roles*]

[assignment: supported access control rules] **[130],**

(9) **delete[131] all security attributes of the selected object[132] to subjects allowed to execute the command DELETE for the selected object[133] to [assignment: *list of further security attributes with the authorised identified roles*].**

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.

204 *Application note 29*: The refinements repeat the structure of the element in order to avoid iteration of the same SFR. The command LOAD APPLICATION allows to create new objects and may allow update of objects MF, DF, Application, Application Dedicated File and their security attributes (cf. [21], (N039.300)). The ST author shall perform the selection in FMT_MSA.1.1/Life, clause (2) in order to indicate possible security implications of changes in the TSF Data of existing objects.

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

FMT_MSA.1/SEF	Management of security attributes
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or 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[134] to restrict the ability to (1) change[135] the security attributes *lifeCycleStatus* of the selected record to „*Operational state (active)*"[136] to subjects allowed to execute the command ACTIVATE RECORD[137], (2) **change[138] the security attributes *lifeCycleStatus* of the**

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

129 [assignment: *list of security attributes*]

130 [assignment: *the authorised identified roles*]

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

132 [assignment: *list of security attributes*]

133 [assignment: *the authorised identified roles*]

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

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

136 [assignment: *list of security attributes*]

137 [assignment: *the authorised identified roles*]

selected record to „*Operational state (deactivated)*“[139] to subjects allowed to execute the command DEACTIVATE RECORD[140],

(3) **delete[141] all security attributes of the selected record[142] to subjects allowed to execute the command DELETE RECORD[143],**

(4) **[assignment: *list of further security attributes with the authorised identified roles*].**

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.

206 *Application note 30*: 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.

207 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
	FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the the access control MF_DF SFP, access control EF SFP, access rule TEF SFP, access rule SEF SFP and access control key SFP[144] to provide restrictive[145] default values for security attributes that are used to enforce the SFP.
	After reset the security attributes of the subject are set as follows:
	(1) *currentFolder* is *root*,
	(2) *keyReferenceList, globalSecurityList, globalPasswordList, dfSpecificSecurityList, dfSpecificPasswordList* and *bitSecurityList* are empty,

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

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

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

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

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

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

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

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

(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[146] to specify alternative initial values to override the default values when an object or information is created.

208 *Application note 31*: The refinements provide rules for setting restrictive security attributes after reset.

209 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)[147] [148] to subjects successfully authenticated with the old *secret* of this password object[149],

(2) **set new *secret* and change *transportStatus* to *regularPassword* of the password objects with *transportStatus* equal to Leer-PIN[150] [151] to subjects allowed to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01)[152],**

(3) **set new *secret* of the password objects by means of the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,00)[153] [154] to subjects successfully authenticated with the PUC of this password object[155],**

(4) **set new *secret* of the password objects by means of the command RESET RETRY COUNTER with**

146 [assignment: *the authorised identified roles*]

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

148 [assignment: *other operations*]

149 [assignment: *the authorised identified roles*]

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

151 [assignment: *other operations*]

152 [assignment: *the authorised identified roles*]

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

154 [assignment: *other operations*]

155 [assignment: *the authorised identified roles*]

(CLA,INS,P1)=(00,2C,02)[156] [157] to subjects allowed to execute the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02)[158].

210 *Application note 32*: The TOE provides access control to the commands depending on the object system. The refinements repeat the structure of the element in order to avoid iteration of the same SFR. The commands CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01) and RESET RETRY COUNTER (CLA,INS,P1)=(00,2C,02) set a new password without need of authentication by PIN or PUC. In order to prevent bypass of the human user authentication defined by the PIN or PUC the object system shall define access control to this command as required by the security needs of the specific application context, cf. OE.Resp-ObjS.

211 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 rule TEF SFP, access rule SEF SFP and access control key SFP[159] to restrict the ability to (1) reset by means of the command VERIFY[160] [161] the security attributes retry counter of password objects[162] to subjects successfully authenticated with the secret of this password object[163], (2) **reset by means of the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[164] [165] the security attributes retry counter of password objects[166] to subjects successfully authenticated with the old secret of this password object[167],**

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

157 [assignment: other operations]

158 [assignment: *the authorised identified roles*]

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

160 [assignment: *other operations*]

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

162 [assignment: *list of security attributes*]

163 [assignment: *the authorised identified roles*]

164 [assignment: *other operations*]

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

166 [assignment: *list of security attributes*]

167 [assignment: *the authorised identified roles*]

(3) **change by means of the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[168] [169] 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)[170],**

(4) **change by means of the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01)[171] [172] 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)[173],**

(5) **reset by means of the command DISABLE VERIFICATION REQUIREMENT with (CLA,INS,P1)=(00,26,00)[174] [175] the security attributes retry counter of password objects[176] to subjects successfully authenticated with the old secret of this password object[177],**

(6) **reset by means of the command ENABLE VERIFICATION REQUIREMENT with (CLA,INS,P1)=(00,28,00)[178] [179] the security attributes retry counter of password objects[180] to subjects successfully authenticated with the old secret of this password object[181],**

(7) **reset by means of the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,00) or (CLA,INS,P1)=(00,2C,01)[182] [183] the security attributes retry counter of password objects[184] to subjects successfully authenticated with the PUC of this password object[185],**

---

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

169 [assignment: *other operations*]

170 [assignment: *the authorised identified roles*]

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

172 [assignment: *other operations*]

173 [assignment: *the authorised identified roles*]

174 [assignment: *other operations*]

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

176 [assignment: *list of security attributes*]

177 [assignment: *the authorised identified roles*]

178 [assignment: *other operations*]

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

180 [assignment: *list of security attributes*]

181 [assignment: *the authorised identified roles*]

182 [assignment: *other operations*]

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

184 [assignment: *list of security attributes*]

185 [assignment: *the authorised identified roles*]

(8) **reset by means of the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or (CLA,INS,P1)=(00,2C,03)[186] [187] the security attributes retry counter of password objects[188] to subjects allowed to execute the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or (CLA,INS,P1)=(00,2C,03)[189],**

(9) **query by means of the command GET PIN STATUS[190] [191] the security attributes *flagEnabled, retry counter, transportStatus*[192] to World[193],**

(10) **enable[194] the security attributes *flagEnabled* requiring authentication with the selected password[195] to subjects authenticated with password and allowed to execute the command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00'28,00)[196],**

(11) **enable[197] the security attributes *flagEnabled* requiring authentication with the selected password[198] to subjects allowed to execute the command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,28,01)[199]**,

(12) **disable[200] the security attributes *flagEnabled* requiring authentication with the selected password[201] to subjects authenticated with password and allowed to execute the command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,00)[202],**

(13) **disable[203] the security attributes *flagEnabled* requiring authentication with the selected password[204] to subjects**

186 [assignment: *other operations*]

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

188 [assignment: *list of security attributes*]

189 [assignment: *the authorised identified roles*]

190 [assignment: *other operations*]

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

192 [assignment: *list of security attributes*]

193 [assignment: *the authorised identified roles*]

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

195 [assignment: *list of security attributes*]

196 [assignment: *the authorised identified roles*]

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

198 [assignment: *list of security attributes*]

199 [assignment: *the authorised identified roles*]

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

201 [assignment: *list of security attributes*]

202 [assignment: *the authorised identified roles*]

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

204 [assignment: *list of security attributes*]

allowed to execute the command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,01)[205].

212 *Application note 33*: The TOE provides access control to the commands depending on the object system. The refinements repeat the structure of the element in order to avoid iteration of the same SFR. The command DISABLE VERIFICATION REQUIREMENT can be used to disable the need to perform successful authentication via the selected password or Multi-Reference password, i.e. any authentication attempt will be successful. The command ENABLE VERIFICATION REQUIREMENT can be used to enable the need to perform an authentication. The access rights to execute these commands can be limited to specific authenticated subjects. For example: the execution of DISABLE VERIFICATION REQUIREMENT should not be allowed for signing applications. The command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,01) allows to disable the verification requirement with the PIN. The command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,28,01) allows anybody to enable the verification requirement with the PIN. The commands RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or (CLA,INS,P1)=(00,2C,03) allows to reset the RESET RETRY COUNTER without authentication with PUC. In order to prevent bypass of the human user authentication defined by the PIN the object system shall define access control to these commands as required by the security needs of the specific application context, cf. OE.Resp-ObjS.

213 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[206] the root public keys to roles authorised to execute this command[207], (2) **import by means of the command PSO VERIFY CERTIFICATE[208] the root public keys to roles authorised to execute this command[209],** (3) **import by means of the command PSO VERIFY CERTIFICATE[210] the certificates as device authentication reference data to roles authorised to execute this command[211],** (4) **select by means of the command MANAGE SECURITY ENVIRONMENT[212] the device authentication reference data to**

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

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

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

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

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

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

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

[selection: *World, roles authorised to execute this command*][213].

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.

214 *Application note 34*: The TOE provides access control to the commands depending on the object system. The refinements repeat the structure of the element in order to avoid iteration of the same SFR. If root public keys are imported according to clause (2) this public key will be stored in the *persistentPublicKeyList* or the *persistentCache* of the object system.

215 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[214] to restrict the ability to query[215] [216] the security attributes access control rights set for the key[217] to meet the access rules of command GET SECURITY STATUS KEY of the object dependent on *lifeCycleStatus, seIdentifier* and *interfaceDependentAccessRules* [218].

216 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

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

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

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

[215] [assignment: *other operations*]

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

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

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

(1) export TSF data according to FPT_ITE.2[219] the

a. public authentication reference data,

b. security attributes for objects of the object system

to [assignment*: list of security attributes of subjects*][220],

(2) export TSF data according to FPT_ITE.2[221] the [assignment: *list of all TOE specific security attributes not described in COS specification [21]*][222] [223] to [assignment*: list of security attributes of subjects*][224],

(3) export[225] 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. [assignment: *list of types of TSF data*],

and the following user data

a. Private keys of the user,

b. Symmetric keys of the user,

c. [assignment: *list of types of user data*][226]

to nobody[227].

6.1.7 Cryptographic Functions

217 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],

---

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

220 [assignment: *the authorised identified roles*]

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

222 [assignment: *list of TSF data*]

223 [assignment: other operations]

224 [assignment: *the authorised identified roles*]

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

226 [assignment: *list of TSF data*]

227 [assignment: *the authorised identified roles*]

(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].

218 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.

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

FCS_RNG.1	Random number generation
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: deterministic, hybrid deterministic, physical, hybrid physical][228] random number generator **of RNG class [selection: *DRG.3, DRG.4, PTG.2, PTG.3*] ([5], [6])** that implements: [assignment: *list of security capabilities* ***of the selected RNG class***].
FCS_RNG.1.2	The TSF shall provide random numbers that meet [assignment: ~~*a*~~ *defined quality metric* ***of the selected RNG class***][229].

220 *Application note 35*: This SFR requires the TOE to generate random numbers used for key generation according to TR-03116-1 [19] section 3.5, requiring RNG classes identified in the selection in element FCS_RNG.1.1 and recommending RNG of class PTG.3. 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 implementation of the PACE protocol requires RNG of class PTG.3 (cf. [19]). The COS specification [21] requires to implement RNG for

- the command GET CHALLENGE,
- the command GET RANDOM if Package Logical Channel is supported[230],
- the authentication protocols as required by FIA_UAU.4,
- the key agreement for secure messaging

according to TR-03116-1 [19] section 3.4. The selection in the element FCS_RNG.1.1 includes RNG of classes DRG.3 and DRG.4. The quality metric assigned in element FCS_RNG.1.2 shall be chosen to resist attacks with high attack potential.

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

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

[230] cf. section for the Package Logical Channel

221 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
FCS_COP.1.1/SHA	The TSF shall perform hashing[231] in accordance with a specified cryptographic algorithm (1) SHA-1, (2) SHA-256, (3) SHA-384, (4) SHA-512[232] and cryptographic key sizes none[233] that meet the following: TR-03116-1 [19], FIPS 180-4 [37][234].

222 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) encryption and decryption with card internal key for command GENERAL AUTHENTICATE, (3) encryption and decryption for secure messaging[235] in accordance with a specified cryptographic algorithm AES in CBC

231 [assignment: *list of cryptographic operations*]

232 [assignment: *cryptographic algorithm*]

233 [assignment: *cryptographic key sizes*]

234 [assignment: *list of standards*]

235 [assignment: *list of cryptographic operations*]

	mode[236] and cryptographic key sizes 128 bit, 192 bit, 256 bit[237] that meet the following: TR-03116-1 [19], COS specification [21], FIPS 197 [33][238].

223 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 for AES as specified in sec. 4.3.3.2 in [17][239] and specified cryptographic key sizes 128 bit, 192 bit and 256 bit[240] that meet the following: TR-03111 [17], COS specification [21], FIPS 197 [33][241].

224 *Application note 36*: The Key Generation FCS_CKM.1/AES.SM is done during MUTUAL AUTHENTICATE and GENERAL AUTHENTICATE with establishment of secure messaging (with Package Crypto Box also for trusted channel during commands EXTERNAL AUTHENTICATE and INTERNAL AUTHENTICATE).

225 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,

236 [assignment: *cryptographic algorithm*]

237 [assignment: *cryptographic key sizes*]

238 [assignment: *list of standards*]

239 [assignment: *cryptographic key generation algorithm*]

240 [assignment: *cryptographic key sizes*]

241 [assignment: *list of standards*]

(2) computation and verification of cryptographic checksum for secure messaging[242]

in accordance with a specified cryptographic algorithm CMAC[243] and cryptographic key sizes 128 bit, 192 bit and 256 bit[244] that meet the following: TR-03116-1 [19], COS specification [21], NIST SP 800-38B [36][245].

226 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 [assignment: *cryptographic key generation algorithm*] **with COS standard curves**[246] and specified cryptographic key sizes 256 bit, 384 bit and 512 bit[247] that meet the following: TR-03111 [17], COS specification [21][248].

227 *Application note 37*: The COS specification [21] requires the TOE to support elliptic curves listed in COS specification [21], section 6.5 (refered as COS standard curves in this PP) and to implement the command GENERATE ASYMMETRIC KEY PAIR for the generation of ELC key pairs. The TOE should support the generation of asymmetric key pairs for the following operations:

- qualified electronic signatures,
- authentication of external entities,
- document cipher key decipherment.

228 The ST author shall perform the missing operation in the element FCS_CKM.1/ELC according to the implemented key generation algorithm.

229 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.

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

[243] [assignment: *cryptographic algorithm*]

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

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

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

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

[248] [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.RSA.S	The TSF shall perform digital signature generation for commands (1) PSO COMPUTE DIGITAL SIGNATURE, (2) INTERNAL AUTHENTICATE[249] 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) [250], and cryptographic key sizes 2048 bit and 3072 bit modulus length[251] that meet the following: TR-03116-1 [19], COS specification [21], [31], [34][252].

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

FCS_COP.1/COS.ECDSA.V	Cryptographic operation – ECDSA signature verification
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or 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 import of ELC keys for commands (1) PSO VERIFY CERTIFICATE, (2) PSO VERIFY DIGITAL SIGNATURE, (3) EXTERNAL AUTHENTICATE[253] in accordance with a specified cryptographic algorithm ECDSA with COS standard curves using (1) SHA-256,

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

[250] [assignment: *cryptographic algorithm*]

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

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

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

(2) SHA-384,

(3) SHA-512[254]

and cryptographic key sizes 256 bits, 384 bits, 512 bits[255] that meet the following: TR-03111 [17], TR-03116-1 [19], COS specification [21], [40][256].

231 *Application note 38*: The command PSO VERIFY CERTIFICATE may store the imported public keys for ELC temporarily in the *volatileCache* or permanently in the *persistentCache* or *applicationPublicKeyList*. These keys may be used as authentication reference data for asymmetric key based device authentication (cf. FIA_UAU.5) or User Data.

232 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 commands (1) PSO COMPUTE DIGITAL SIGNATURE, (2) INTERNAL AUTHENTICATE[257] in accordance with a specified cryptographic algorithm ECDSA with COS standard curves using (1) SHA-256, (2) SHA-384, (3) SHA-512[258] and cryptographic key sizes 256 bits, 384 bits, 512 bits[259] that meet the following: TR-03111 [17], TR-03116-1 [19], COS specification [21], [40][260].

254 [assignment: *cryptographic algorithm*]

255 [assignment: *cryptographic key sizes*]

256 [assignment: *list of standards*]

257 [assignment: *list of cryptographic operations*]

258 [assignment: *cryptographic algorithm*]

259 [assignment: *cryptographic key sizes*]

260 [assignment: *list of standards*]

233 *Application note 39*: 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
  - RSA ISO9796-2 DS2 with SHA-256 (see FCS_COP.1/COS.RSA.S)

234 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) [261] in accordance with a specified cryptographic algorithm (1) for encryption: a. RSAES-PKCS1-v1_5_Encrypt ([34] section 7.2.1), b. RSA-OAEP-Encrypt ([34] section 7.1.1), (2) for decryption: a. RSAES-PKCS1-v1_5_Decrypt ([34] section 7.2.2), b. RSA-OAEP-Decrypt ([34] section 7.1.2) [262]

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

[262] [assignment: *cryptographic algorithm*]

	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[263] that meet the following: TR-03116-1 [19], COS specification [21], [34][264].

235 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) [265] in accordance with a specified cryptographic algorithm (1) for encryption ELC encryption, (2) for decryption ELC decryption[266] 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[267] that meet the following: TR-03111 [17], TR-03116-1 [19], and COS specification [21][268].

236 *Application note 40*: The TOE can support or reject the command PSO HASH (following standard [30]) and ENVELOPE (following standard [29]). If the command is supported the ST author is asked to add a SFR FCS_COP.1/CB_HASH specifying the supported hash algorithms.

263 [assignment: *cryptographic key sizes*]

264 [assignment: *list of standards*]

265 [assignment: *list of cryptographic operations*]

266 [assignment: *cryptographic algorithm*]

267 [assignment: *cryptographic key sizes*]

268 [assignment: *list of standards*]

237 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 [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

238 *Application note 41*: The TOE shall destroy the encryption session keys and the message authentication keys for secure messaging after reset or termination of secure messaging session (trusted channel) or reaching fail secure state according to FPT_FLS.1. The TOE shall clear the memory area of any session keys before starting a new communication with an external entity in a new after-reset-session as required by FDP_RIP.1. Explicit deletion of a secret using the DELETE command should also be taken into account by the ST author.

6.1.8 Protection of communication

239 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[269] to initiate communication via the trusted channel.
FTP_ITC.1.3/TC	The TSF shall initiate communication via the trusted channel for none[270].

240 *Application note 42*: The TOE responds only to commands establishing secure messaging channels.

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

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

6.2 Security Assurance Requirements for the TOE

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

Security Target evaluation (Class ASE)

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

Assurance Level 4 (EAL4)

243 and augmented by taking the following components:

ALC_DVS.2 (Development security)

ATE_DPT.2 (Test depth)

AVA_VAN.5 (Advanced methodical vulnerability analysis).

244 The Security Assurance Requirements are:

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

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

Table 21: TOE Security Assurance Requirements

6.2.1 Refinements of the TOE Security Assurance Requirements

245 In BSI-CC-PP-0084-2014 [11] specific refinements of the TOE Security Assurance Requirements are set up. As the present Protection Profile 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 section where these refinements in BSI-CC-PP-0084-2014 [11] are specified are listed in **Table 22**. The ST author is asked to refer for more details to the respective sections in BSI-CC-PP-0084-2014 [11].

246 For all other SFRs the TOE Security Assurance Requirements from Common Criteria Part 3 [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 the present Protection Profile. According to Common Criteria Part 1 [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)"
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)"

Refinements regarding	Reference to [11]
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

247 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

248 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.

249 The COS specification [21] allows implementation of optional features and commands. The following refinement for ADV_ARC.1.5C defines specific evidence required for these optional features and commands if implemented by the TOE and not being part of the TSF.

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

6.2.3 Refinements to ADV_FSP.4 Complete functional specification

250 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.

251 *Application note 43:* 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

252 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**.

253 *Application note 44:* 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

254 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.

255 *Application note 45*: The wrapper will be used to interact with the smart card for the export of all public TSF Data of all objects in an object system according to "Export of TSF data (FPT_ITE.2)". Because the COS specification [21] identifies optional functionality the TOE may support the guidance documentation shall describe the method of use of the TOE (as COS, wrapper) to find all objects in the object system and to export all security attributes of these objects.

6.2.6 Refinements to ATE_FUN.1 Functional tests

256 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 [22], eHPC [23], SMC-B [24], gSMC-K [25] or gSMC-KT [26].

257 *Application note 46*: 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

258 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 [22], eHPC [23], SMC-B [24], gSMC-K [25] and gSMC-KT [26].

259 *Application note 47*: The evaluator should agree the typical uses cases with the certification body in order to define an effective test approach and to use synergy for appropiate test effort. The agreed test cases support comparable test effort for TSF defined in the main part of this PP and the optional Packages included in the security target.

6.3 Security Requirements Rationale

260 This section comprises three parts:

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

6.3.1 Security Functional Requirements Rationale

261 Table 2 in BSI-CC-PP-0084-2014 [11], section 6.3.1 “Rationale for the security functional requirements” gives an overview, how the Security Functional Requirements that are taken over in the present PP 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].

262 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
FAU_SAS.1/SICP	X							
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

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

263 As stated in section 2.4, this PP 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.

264 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					

	O.Integrity	O.Confidentiality	O.Resp-COS	O.TSFDataExport	O.Authentication	O.AccessControl	O.KeyManagement	O.Crypto	O.SecureMessaging
FPT_ITE.1				X					
FPT_ITE.2				X					
FPT_TST.1	X	X	X						
FIA_SOS.1					X				
FIA_AFL.1/PIN					X				
FIA_AFL.1/PUC					X				
FIA_ATD.1					X				
FIA_UAU.1					X				
FIA_UAU.4					X				
FIA_UAU.5					X				
FIA_UAU.6					X				
FIA_UID.1					X				
FIA_API.1					X				
FMT_SMR.1					X	X			
FIA_USB.1					X	X			
FDP_ACC.1/MF_DF						X			
FDP_ACF.1/MF_DF						X			
FDP_ACC.1/EF						X			
FDP_ACF.1/EF						X			
FDP_ACC.1/TEF						X			
FDP_ACF.1/TEF						X			
FDP_ACC.1/SEF						X			
FDP_ACF.1/SEF						X			
FDP_ACC.1/KEY						X	X		
FDP_ACF.1/KEY						X	X		
FMT_MSA.3						X			
FMT_SMF.1						X			
FMT_MSA.1/Life					X	X	X		
FMT_MSA.1/SEF						X			

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

Table 24: Mapping between Security Objectives for the TOE and SFRs

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

266 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 error 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.

267 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.

268 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.

269 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 TOE implementation by the SFR FPT_ITE.1. For Card Verifiable Certificates (CVC), the SFR FPT_TDC.1 requires the consistent interpretation when shared between the TSF and another trusted IT product.

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

- FIA_SOS.1 requires that the TSF enforces the length of the secret of the password objects.
- FIA_AFL.1/PIN requires that the TSF detects repeated unsuccessful authentication attempts and blocks the password authentication when the number of unsuccessful authentication attempts reaches a defined number.
- FIA_AFL.1/PUC requires that the TSF detects repeated unsuccessful authentication attempts for the password unblocking function and performs appropriate actions when the number of unsuccessful authentication attempts reaches a defined number.
- FIA_ATD.1 requires that the TSF maintains dedicated security attributes belonging to individual users.
- FIA_UAU.1 requires the processing of dedicated actions before a user is authenticated. Any other actions shall require user authentication.
- FIA_UAU.4 requires the prevention of reuse of authentication data.
- FIA_UAU.5 requires the TSF to support user authentication by providing dedicated commands. Multiple authentication mechanisms like password based and key based authentication are required.
- FIA_UAU.6 requires the TSF to support re-authentication of message senders using a secure messaging channel.
- FIA_UID.1 requires the processing of dedicated actions before a user is identified. Any other actions shall require user identification.

- FIA_API.1 requires that the TSF provides dedicated commands to prove the identity of the TSF itself.
- FMT_SMR.1 requires that the TSF maintains roles and associates users with roles.
- FIA_USB.1 requires that the TSF associates dedicated security attributes with subjects acting on behalf of that user. Also, the TSF shall enforce rules governing changes of these security attributes by the implementation of commands that perform these changes.
- FMT_MSA.1/Life requires that the TSF enforces the access control policy to restrict the ability to manage life cycle relevant security attributes like *lifeCycleStatus*. For that purpose the SFR requires management functions to implement these operations.
- FMT_MTD.1/PIN requires that the TSF restricts the ability to change password objects by the implementation of dedicated commands and management functions.
- FMT_MSA.1/PIN requires that the TSF enforces the access control policy to restrict the ability to change, enable and disable and optionally perform further operations of security attributes for password objects. For that purpose the SFR requires management functions to implement these operations.
- FMT_MTD.1/Auth requires that the TSF restricts the ability to import device authentication reference data by the implementation of dedicated commands and management functions.
- FMT_MSA.1/Auth requires that the TSF enforces the access control policy to restrict the ability to read security attributes for the device authentication reference data. For that purpose the SFR requires management functions to implement this operation.

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

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

- FDP_ACF.1/TEF requires that the TSF enforce an access control policy to restrict operations on transparent EF objects based on a set of rules defined in the SFR. Also, the TSF is required to deny access to transparent EF objects in case of "Termination state" of the TOE life cycle.
- FDP_ACC.1/SEF requires that the TSF enforces an access control policy to restrict operations on structured EF objects performed by subjects of the TOE.
- FDP_ACF.1/SEF requires that the TSF enforce an access control policy to restrict operations on structured EF objects based on a set of rules defined in the SFR. Also, the TSF is required to deny access to structured EF objects in case of "Termination state" of the TOE life cycle.
- FDP_ACC.1/KEY requires that the TSF enforces an access control policy to restrict operations on dedicated key objects performed by subjects of the TOE.
- FDP_ACF.1/KEY requires that the TSF enforce an access control policy to restrict operations on dedicated key objects based on a set of rules defined in the SFR. Also, the TSF is required to deny access to dedicated key objects in case of "Termination state" of the TOE life cycle.
- FMT_MSA.3 requires that the TSF enforces an access control policy that provides restrictive default values for the used security attributes. Alternative default values for these security attributes shall only be allowed for dedicated authorised roles.
- FMT_SMF.1 requires that the TSF implements dedicated management functions that are given in the SFR.
- FMT_MSA.1/Life requires that the TSF enforces the access control policy to restrict the ability to manage life cycle relevant security attributes like *lifeCycleStatus*. For that purpose the SFR requires management functions to implement these operations.
- FMT_MSA.1/SEF requires that the TSF enforces the access control policy to restrict the ability to manage of security attributes of records. For that purpose the SFR requires management functions to implement these operations.
- FMT_MTD.1/PIN requires that the TSF restricts the ability to change password objects by the implementation of dedicated commands and management functions.
- FMT_MSA.1/PIN requires that the TSF enforces the access control policy to restrict the ability to read, change, enable, disable and optionally perform further operations of security attributes for password objects. For that purpose the SFR requires management functions to implement these operations.
- FMT_MTD.1/Auth requires that the TSF restricts the ability to import device authentication reference data by the implementation of dedicated commands and management functions.
- FMT_MSA.1/Auth requires that the TSF enforces the access control policy to restrict the ability to read security attributes for the device authentication reference data. For that purpose the SFR requires management functions to implement this operation.
- FMT_MTD.1/NE restricts the ability to export sensitive TSF Data to dedicated roles, some sensitive User Data like private authentication keys are not allowed to be exported at all.

272 The Security Objective **O.KeyManagement** "Generation and import of keys" requires the ability of the TSF to secure generation, import, distribution, access control and destruction of

cryptographic keys. Also, the TSF is required to support the import and export of public keys. This Security Objective is addressed by the following SFRs:

- FCS_RNG.1 requires that the TSF provides a random number generator of a specific class used for generation of keys.
- FCS_CKM.1/AES.SM and FCS_CKM.1/ELC require that the TSF generates cryptographic keys with specific key generation algorithms as stated in the SFRs. The mentioned SFRs are needed to fulfil different requirements of the intended usage of the cryptographic keys.
- FCS_CKM.4 requires that the TSF destroys cryptographic keys in accordance with a given specific key destruction method.
- FDP_ACC.1/KEY and FDP_ACF.1/KEY control access to the key management and the cryptographic operations using keys.
- FMT_MSA.1/Life requires restriction of the management of security attributes of the keys to subjects authorised for specific commands.

273 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_COP.1/SHA requires that the TSF provides different hashing algorithms that are referenced in the SFR.
- FCS_COP.1/COS.AES requires that the TSF provides decryption and encryption using AES with different key sizes.
- FCS_COP.1/COS.CMAC requires that the TSF provides computation and verification of cryptographic checksums using the CMAC algorithm.
- FCS_COP.1/COS.RSA.S requires that the TSF provides the generation of digital signatures based on the RSA algorithm and different modulus lengths.
- FCS_COP.1/COS.ECDSA.S requires that the TSF provides the generation of digital signatures based on the ECDSA and different hash algorithms and different key sizes.
- FCS_COP.1/COS.ECDSA.V requires that the TSF provides the verification of digital signatures based on the ECDSA and different hash algorithms and different key sizes.
- FCS_COP.1/COS.RSA requires that the TSF provides encryption and decryption capabilities based on RSA algorithms with different modulus lengths.
- FCS_COP.1/COS.ELC requires that the TSF provides encryption and decryption capabilities based on ELC algorithms with different key sizes.
- FCS_CKM.1/AES.SM and FCS_CKM.1/ELC require that the TSF generates cryptographic keys with specific key generation algorithms as stated in the SFRs. The mentioned SFRs are needed to fulfil different requirements of the intended usage of the cryptographic keys.

274 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

275 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].

276 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.

277 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.

278 The following table lists the required dependencies of the SFRs of this PP 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

SFR	dependent on	fulfilled by
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
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	FDP_ACC.1/KEY,

SFR	dependent on	fulfilled by
	control, FMT_MSA.3 Static attribute initialisation	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, FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY, FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/NE	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FMT_SMR.1, FMT_SMF.1

SFR	dependent on	fulfilled by
FCS_RNG.1	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/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 generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/AES.SM, FCS_CKM.4
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* in the case that the TOE provides RSA key generation functionality, i.e. Package RSA Key Generation is applied. Otherwise, dependency on FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1 is not applicable as neither key import nor key generation by the TOE for RSA key pairs / private keys

SFR	dependent on	fulfilled by
		are relevant for the operational phase. 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* in the case that the TOE provides RSA key generation functionality, i.e. Package RSA Key Generation is applied. Otherwise, dependency on FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1 is not applicable as neither key import nor key generation by the TOE for RSA key pairs / private keys are relevant for the operational phase. 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	FCS_CKM.1/AES.SM, *FCS_CKM.1/RSA* in the case that the TOE provides RSA

SFR	dependent on	fulfilled by
	with security attributes, or FCS_CKM.1 Cryptographic key generation]	key generation functionality, i.e. Package RSA Key Generation is applied, FCS_CKM.1/ELC
FTP_ITC.1/TC	No dependencies.	n. a.

Table 25: Dependencies of the SFRs

6.3.3 Security Assurance Requirements Rationale

279 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.

280 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.

281 The selection of the component ATE_DPT.2 provides a higher assurance than the pre-defined EAL4 Package due to requiring the functional testing of SFR-enforcing modules. The functional testing of SFR-enforcing modules is due to the TOE building a smart card platform with very broad and powerful security functionality but without object system. An augmentation with ATE_DPT.2 only for the SFR specified in BSI-CC-PP-0084-2014 [11] would have been sufficient to fulfil the conformance, but this would contradict the intention of BSI-CC-PP-0084-2014. Therefore the augmentation with ATE_DPT.2 is required for the complete Protection Profile.

282 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.

283 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.

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

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

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

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

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

Table 26: SAR Dependencies

7 Package Crypto Box

287 The COS may support optionally additional cryptographic functionality according to [21]. This section defines the Package Crypto Box to be used by the ST author if the TOE provides this security functionality.

7.1 TOE Overview for Package Crypto Box

288 In addition to the TOE definition given in section 1.2.1 “TOE definition and operational usage” the TOE is equipped with further cryptographic functionality.

7.2 Security Problem Definition for Package Crypto Box

7.2.1 Assets and External Entities

Assets

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

Subjects and external entities

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

7.2.2 Threats

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

7.2.3 Organisational Security Policies

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

7.2.4 Assumptions

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

7.3 Security Objectives for Package Crypto Box

294 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.

295 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.

296 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.

297 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.

7.4 Security Requirements for Package Crypto Box

298 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 27: Authentication data of the devices and security attributes

299 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 verification 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 referenced in keyReferenceList.macCalculation and keyReferenceList.dataEncipher*	The commands PSO COMPUTE CRYPTOGRAPHIC CHECKSUM and PSO ENCIPHER are used to generate commands received by the authenticated PICC with secure messaging.

Table 28: Authentication data of the COS with Package Crypto Box

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

301 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**[271] 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 [272].

302 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)).

[271] Refinement identifying the concrete user

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

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[273] to prove the identity of the TSF itself[274] to an external entity.

303 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.
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[275].
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[276].
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) [assignment: *further rules for the changing of attributes*][277].

304 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

[273] [assignment: *authentication mechanism*]

[274] [assignment: *object, authorised user or rule*].

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

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

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

	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, (4) decryption with card internal key for command EXTERNAL AUTHENTICATE, (5) encryption with card internal key for command INTERNAL AUTHENTICATE[278] in accordance with a specified cryptographic algorithm AES in CBC mode[279] and cryptographic key sizes 128 bit, 192 bit, 256 bit[280] that meet the following: TR-03116-1 [19], COS specification [21], FIPS 197 [33][281].

305 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,

278 [assignment: *list of cryptographic operations*]

279 [assignment: *cryptographic algorithm*]

280 [assignment: *cryptographic key sizes*]

281 [assignment: *list of standards*]

(3) verification of cryptographic checksum for command EXTERNAL AUTHENTICATE[282]

in accordance with a specified cryptographic algorithm CMAC[283] and cryptographic key sizes 128 bit, 192 bit and 256 bit[284] that meet the following: TR-03116-1 [19], COS specification [21], [36][285].

306 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[286] in accordance with a specified cryptographic algorithm (1) for encryption: a. RSAES-PKCS1-v1_5-Encrypt ([34] section 7.2.1), b. RSA-OAEP-Encrypt ([34] section 7.1.1), (2) for decryption: a. RSAES-PKCS1-v1_5-Decrypt ([34] section 7.2.2), b. RSA-OAEP-Decrypt ([34] section 7.1.2) [287] 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[288] that meet the following: PKCS #1 [34][289].

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

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

[283] [assignment: *cryptographic algorithm*]

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

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

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

[287] [assignment: *cryptographic algorithm*]

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

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

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[290] in accordance with a specified cryptographic algorithm ELC encryption with COS standard curves[291] and cryptographic key sizes 256 bits, 384 bits, 512 bits[292] that meet the following: TR-03111 [17], section 4.3.1, 4.3.3 and 5.3.1.2[293].

7.5 Security Requirements Rationale for Package Crypto Box

308 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 29: Mapping between Security Objectives for the TOE and SFRs for Package Crypto Box

290 [assignment: *list of cryptographic operations*]

291 [assignment: *cryptographic algorithm*]

292 [assignment: *cryptographic key sizes*]

293 [assignment: *list of standards*]

309 **Table 29** 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.

310 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.
- 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.

311 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.

312 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 30** should be taken as extension of **Table 25** and **Table 44** (if applicable) in order to cover all dependencies. In particular, **Table 30** 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	FCS_CKM.1/AES.SM, FCS_CKM.4

SFR	dependent on	fulfilled by
	with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	
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.4 Cryptographic key destruction	FCS_CKM.1/ELC, FCS_CKM.4
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* in the case that the TOE provides RSA key generation functionality, i.e. Package RSA Key Generation is applied. Otherwise, dependency on FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1 is not applicable as neither key import nor key generation by the TOE for RSA key pairs / private keys are relevant for the operational phase. FCS_CKM.4
Hint: *FCS_CKM.1/RSA* in the case that 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 44**: FCS_COP.1/CB.RSA

Table 30: Dependencies of the SFRs for Package Crypto Box

8 Package Contactless

313 The COS may support optionally 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 to be used by the ST author if the TOE provides this security functionality.

314 The TSF for the Proximity Coupling Devices (PCD) is described in the Package PACE for Proximity Coupling Device in section 9. Both Packages describe TSF for different roles in the PACE protocol. E.g. the human user sends the CAN to the smart card terminal (as PCD) and the smart card terminal sends the CAN to the gSMC-KT (as TOE with Package PACE for Proximity Coupling Device) running the PACE protocol in PCD role. The terminal communicates with a contactless smart card (as PICC), which is a sample of the TOE but with Package Contactless and running the PACE protocol in PICC role.

8.1 TOE Overview for Package Contactless

315 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

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

Security Attributes of Users and Subjects

317 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.

318 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).

User type	Definition
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 31: User type for Package Contactless

8.2.2 Threats

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

8.2.3 Organisational Security Policies

320 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

321 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

322 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.

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

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

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.

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

OE.PACE_Terminal **PACE support by contactless terminal**

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

325 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

326 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.
TOE as PICC	SK4SM referenced in *macKey* and *SSCmac*	SK4SM is used to generate MAC for command responses.

Table 32: Authentication data of the COS for Package Contactless

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

328 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 31** even if the Package Contactless is not included.

329 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 [selection: ~~***physical, non-physical true, deterministic,***~~ *hybrid deterministic, hybrid physical*][294] random number generator **of RNG class [selection: *DRG.4, PTG.3*] ([5], [6]) for PACE protocol** that implements: [assignment: *list of security capabilities* ***of the selected RNG class***].
FCS_RNG.1.2/ PACE	The TSF provide random ~~numbers~~ **[selection: *bits, octets of bits, numbers [assignment: format of the numbers]*]** that meet [assignment: ~~*a*~~ *defined quality metric* ***of the selected RNG class***].

330 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
FCS_COP.1.1/PACE.PICC.ENC	The TSF shall perform decryption and encryption for secure messaging[295] in accordance with a specified cryptographic algorithm AES in CBC mode[296] and cryptographic key sizes **[selection: *128 bit, 192 bit, 256 bit*]**[297] that meet the following: TR-03110 [16], COS specification [21][298].

331 *Application note 48*: 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.

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

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

295 [assignment: *list of cryptographic operations*]

296 [assignment: *cryptographic algorithm*]

297 [assignment: *cryptographic key sizes*]

298 [assignment: *list of standards*]

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[299] in accordance with a specified cryptographic algorithm CMAC[300] and cryptographic key sizes **[selection: *128 bit, 192 bit, 256 bit*]**[301] that meet the following: TR-03110 [16], COS specification [21][302].

333 *Application note 49*: 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.

334 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 **[selection: *Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [17] using the protocol* [selection: *id-PACE-ECDH-GM-AES-CBC-CMAC-128 with brainpoolP256r1, id-PACE-ECDH-GM-AES-CBC-CMAC-192 with brainpoolP384r1, id-PACE-ECDH-GM-AES-CBC-CMAC-256 with brainpoolP512r1*]]**[303] and specified cryptographic key sizes **[selection: *256 bit, 384 bit, 512 bit*]**[304] that meet the following: TR-03110 [16], TR-03111 [17][305].

299 [assignment: *list of cryptographic operations*]

300 [assignment: *cryptographic algorithm*]

301 [assignment: *cryptographic key sizes*]

302 [assignment: *list of standards*]

303 [assignment: *cryptographic key generation algorithm*]

304 [assignment: *cryptographic key sizes*]

305 [assignment: *list of standards*]

335 *Application note 50*: The TOE exchanges a shared secret with the external entity during the PACE protocol, see [16]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [33]) or on the ECDH compliant to TR-03111 [17] (i.e. the elliptic curve cryptographic algorithm ECKA). The shared secret is used for deriving the AES session keys for message encryption and message authentication according to [16] for the TSF as required by FCS_COP.1/PACE.PICC.ENC and FCS_COP.1/PACE.PICC.MAC. FCS_CKM.1/DH.PACE.PICC implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to TR-03110 [16].

336 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 [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

337 *Application note 51*: The TOE shall destroy the encryption session keys and the message authentication keys for PACE protocol after reset or termination of the secure messaging (or trusted channel) session or reaching fail secure state according to FPT_FLS.1. The TOE shall clear the memory area of any session keys before starting a new communication with an external entity in a new after-reset-session as required by FDP_RIP.1.

338 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) [assignment: *list of TSF-mediated actions*][306] 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

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

PACE	allowing any other TSF-mediated actions on behalf of that user.

339 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) [assignment: *list of TSF-mediated actions*][307] 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.

340 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][308].

341 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 [20] using

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

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

command GENERAL AUTHENTICATE,

(2) secure messaging in MAC-ENC mode using PACE session keys according to [20], section 13, and [16], Part 3, in PICC role[309]

to support user authentication.

FIA_UAU.5.2/ PACE.PICC	The TSF shall authenticate any user's claimed identity according to the 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[310].

342 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[311].

343 *Application note 52*: 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).

344 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*,

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

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

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

(2) *SK4SM referenced* in *macKey and SSCmac*[312].

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[313].
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)[314].

345 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*][315] the following objects: (1) session keys (immediately after closing related communication session),

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

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

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

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

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

(3) [assignment: *list of additional objects*][316].

346 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[317] to transmit and receive[318] user data in a manner protected from unauthorised disclosure.

347 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[319] to transmit and receive[320] user data in a manner protected from modification, deletion, insertion, and replay[321] errors.
FDP_UIT.1.2/ PACE	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, and replay[322] has occurred.

316 [assignment: *list of objects*]

317 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

318 [selection: *transmit, receive*]

319 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

320 [selection: *transmit, receive*]

321 [selection: *modification, deletion, insertion, replay*]

322 [selection: *modification, deletion, insertion, replay*]

348 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[323] 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[324].

349 *Application note 53*: 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.

350 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) [assignment: *additional authorised identified roles*][325].
FMT_SMR.1.2/ PACE.PICC	The TSF shall be able to associate users with roles.

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

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

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

325 [assignment: *the authorised identified roles*]

FMT_MTD.1/ PACE.PICC	Management of TSF data – PACE/PICC
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/ PACE.PICC	The TSF shall restrict the ability to read[326] [327] the (1) SCCO used for PACE protocol in PICC role, (2) session keys of secure messaging channel established using PACE protocol in PICC role[328] to none[329].

352 *Application note 54*: The refinement 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.

353 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[330] given the following conditions (1) conditions as defined in FPT_ITE.2.1, (2) no export of the SCCO[331].
FPT_ITE.2.2/ PACE	The TSF shall use [assignment: *list of encoding rules to be applied by TSF*] for the exported data.

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

326 [assignment: *other operations*]

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

328 [assignment: *list of TSF data*]

329 [assignment: *the authorised identified roles*]

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

331 [assignment: *conditions for export*]

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[332].

355 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 [assignment: *types of emissions*] in excess of [assignment: *specified limits*] 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) [assignment: *list of additional types of TSF data*][333] and [assignment: *list of types of user data*].
FPT_EMS.1.2/ PACE.PICC	The TSF shall ensure any users[334] are unable to use the following interface the contactless interface and circuit contacts[335] 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) [assignment: *list of additional types of TSF data*][336]

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

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

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

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

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

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

8.5 Security Requirements Rationale for Package Contactless

356 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
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 33: Mapping between Security Objectives for the TOE and SFRs for Package Contactless

357 **Table 33** 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.

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

359 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.

360 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.

361 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.

362 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.

363 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 physical random number generator of class DRG.4 or PTG.3.

364 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.

365 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.

366 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 34** 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.

SFR	dependent on	fulfilled by
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
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.

SFR	dependent on	fulfilled by
FTP_ITC.1/PACE	No dependencies.	n. a.

Table 34: Dependencies of the SFRs for Package Contactless

9 Package PACE for Proximity Coupling Device

367 The COS may support optionally additional functionality for contactless communication of Proximity Coupling Devices (PCD, named also “terminal” in the following) using the terminal part of the PACE protocol according to [21]. This section defines the Package PACE for Proximity Coupling Device to be used by the ST author if the TOE provides this security functionality.

368 The TSF for the Proximity Integrated Circuit Chip (PICC) is described in the Package Contactless in section 8.

9.1 TOE Overview for Package PACE for Proximity Coupling Device

369 This Package describes additional TSF supporting the contactless communication of a terminal in PCD role with the smart card (PICC) using PACE. The TOE is part of the terminal and provides the cryptographic functions for the terminal through its contact-based interface. The terminal implements the contactless interface to PICC.

9.2 Security Problem Definition for Package PACE for Proximity Coupling Device

9.2.1 Assets and External Entities

Assets

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

Security Attributes of Users and Subjects

371 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. When the TOE is running the PCD role of the PACE protocol the subject gains security attributes defining the authentication state of the external user communicating through the trusted channel established after successful authentication. This authentication state is identified in the response code of the trusted channel commands PSO DECIPHER and PSO VERIFY CRYPTOGRAPHIC CHECKSUM.

372 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	An external device communicating with the TOE through the contactless interface and successfully authenticated by the PACE

User type	Definition
PACE protocol in PICC role	protocol in PICC role.

Table 35: User type for Package PACE for Proximity Coupling Device

9.2.2 Threats

373 There are no additional Threats for the Package PACE for Proximity Coupling Device beyond the Threats already defined in section 3.2.

9.2.3 Organisational Security Policies

374 There are no additional Organisational Security Policies for the Package PACE for Proximity Coupling Device beyond the Organisational Security Policies already defined in section 3.3.

9.2.4 Assumptions

375 There are no additional Assumptions for the Package PACE for Proximity Coupling Device beyond the Assumptions already defined in section 3.4.

9.3 Security Objectives for Package PACE for Proximity Coupling Device

376 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 PACE for Proximity Coupling Device. Therefore the Security Objective Rationale (section 4.3) is supplemented as well.

377 The TOE shall fulfil the Security Objective “Protection of contactless communication with PACE/PCD (O.PACE_Terminal)” as specified below.

O.PACE_Terminal **Protection of contactless communication with PACE/PCD**

The TOE supports the terminal part of the PACE protocol in order to protect the confidentiality and the integrity of data communicated through the contactless interface of the terminal.

378 The operational environment of the TOE shall fulfil the Security Objective “PACE/PICC support by contactless chip (OE.PACE_Chip)” as specified below.

OE.PACE_Chip **PACE/PICC support by contactless chip**

The external device communicating through its contactless interface using PACE shall support the chip part of the PACE protocol.

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

9.4 Security Requirements for Package PACE for Proximity Coupling Device

380 In addition to the authentication reference data of the devices listed in **Table 15** the following table defines for the TOE with Package PACE for Proximity Coupling Device the authentication reference data of the user in PICC role and the authentication verification data used by the TSF itself (cf. FIA_API.1) in PCD role.

User type / Subject type	**Authentication data and security attributes**	**Operations**
Device as PICC	**Card Access Number (CAN)** Authentication verification data Card Access Number (CAN) provided to the TOE ENC and MAC session keys SK4TC generated running PACE Security attributes *flagSessionEnabled* (equal SK4TC) *negotiationKeyInformation* SK4TC referenced in *keyReferenceList.macCalculation* and *keyReferenceList.dataEncipher*	The command GENERAL AUTHENTICATE with (CLA,INS,P1,P2)=(‘x0’,’86’,’00’,’00’) is used by the TOE running the PACE protocol role as PCD to authenticate the external device running the PACE protocol role as PICC. Note that the commands PSO VERIFY CRYPTOGRAPHIC CHECKSUM and PSO DECIPHER supported by the TOE with Package Crypto Box are used to authenticate the responses received after establishment of session keys SK4TC.
TOE acting for human user as PCD	SK4TC referenced in *keyReferenceList.macCalculation* and *keyReferenceList.dataEncipher*	The commands PSO COMPUTE CRYPTOGRAPHIC CHECKSUM and PSO ENCIPHER are used to generate commands received by the authenticated PICC with secure messaging.

Table 36: Authentication data of the COS with Package PACE for Proximity Coupling Device

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

382 The TOE shall meet the requirement “Cryptographic operation – PACE secure messaging encryption (FCS_COP.1/PACE.PCD.ENC)” as specified below.

FCS_COP.1/ PACE.PCD.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
FCS_COP.1.1/PACE.PCD.ENC	The TSF shall perform decryption and encryption for trusted channel[337] in accordance with a specified cryptographic algorithm AES in CBC mode[338] and cryptographic key sizes **[selection: *128 bit, 192 bit, 256 bit*]**[339] that meet the following: TR-03110 [16], COS specification [21][340].

383 *Application note 55*: 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.PCD.

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

FCS_COP.1/ PACE.PCD.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.PCD.MAC	The TSF shall perform MAC calculation for trusted channel[341] in accordance with a specified cryptographic algorithm CMAC[342] and cryptographic key sizes **[selection: *128 bit, 192 bit, 256 bit*]**[343] that meet the following: TR-03110 [16], COS specification [21][344].

385 *Application note 56*: 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.PCD.

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

FCS_CKM.1/ DH.PACE.PCD	Cryptographic key generation – DH by PACE/PCD

337 [assignment: *list of cryptographic operations*]

338 [assignment: *cryptographic algorithm*]

339 [assignment: *cryptographic key sizes*]

340 [assignment: *list of standards*]

341 [assignment: *list of cryptographic operations*]

342 [assignment: *cryptographic algorithm*]

343 [assignment: *cryptographic key sizes*]

344 [assignment: *list of standards*]

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.PCD	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[selection: *Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [17] using the protocol* [selection: *id-PACE-ECDH-GM-AES-CBC-CMAC-128_PCD with brainpoolP256r1, id-PACE-ECDH-GM-AES-CBC-CMAC-192_PCD with brainpoolP384r1, id-PACE-ECDH-GM-AES-CBC-CMAC-256_PCD with brainpoolP512r1*]]**[345] and specified cryptographic key sizes **[selection: *256 bit, 384 bit, 512 bit*]**[346] that meet the following: TR-03110 [16], TR-03111 [17][347].

387 *Application note 57*: The TOE exchanges a shared secret with the external entity during the PACE protocol, see [16]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [33]) or on the ECDH compliant to TR-03111 [17] (i.e. the elliptic curve cryptographic algorithm ECKA). The shared secret is used for deriving the AES session keys for message encryption and message authentication according to [16] for the TSF as required by, FCS_COP.1/ PACE.PCD.ENC, and FCS_COP.1/PACE.PCD.MAC. FCS_CKM.1/DH.PACE.PCD implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to TR-03110 [16].

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

FCS_CKM.4/ PACE.PCD	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.PCD	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

389 *Application note 58*: The TOE shall destroy the encryption session keys and the message authentication keys for PACE protocol after reset or termination of the secure messaging (or trusted channel) session or reaching fail secure state according to FPT_FLS.1. The TOE shall clear the memory area of any session keys before starting a new communication with an external entity in a new after-reset-session as required by FDP_RIP.1.

345 [assignment: *cryptographic key generation algorithm*]

346 [assignment: *cryptographic key sizes*]

347 [assignment: *list of standards*]

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

FIA_UAU.5/ PACE.PCD	Multiple authentication mechanisms – PACE/PCD
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1/ PACE.PCD	The TSF shall provide (1) PACE protocol in PCD role according to [16] and [20] using command GENERAL AUTHENTICATE, (2) trusted channel using PACE session keys according to [20], section 13, and [16], Part 3, in PCD role[348] to support user authentication.
FIA_UAU.5.2/ PACE.PCD	The TSF shall authenticate any user's claimed identity according to the the PACE protocol as PCD is used for authentication of devices using PACE protocol in PICC role and trusted channel in MAC-ENC mode using PACE session keys is used and messages received in commands PSO VERIFY CRYPTOGRAPHIC CHECKSUM and PSO DECIPHER[349].

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

FIA_UAU.6/ PACE.PCD	Re-authenticating – PACE/PCD
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1/ PACE.PCD	The TSF shall re-authenticate the user under the conditions after successful run of the PACE protocol as PCD each message received in commands PSO VERIFY CRYPTOGRAPHIC CHECKSUM and PSO DECIPHER shall be verified as being sent by the authenticated PICC[350].

392 *Application note 59*: The PACE protocol as PCD specified in [26] starts trusted channel used for all commands and responses exchanged after successful PACE authentication. The TOE decrypts and verifies each response whether it was sent by the successfully authenticated chip to the terminal (see FCS_COP.1/PACE.PCD.ENC and FCS_COP.1/PACE.PCD.MAC for further details). The TOE executes these verifications only on demand of the terminal. Therefore, the TOE re-authenticates the chip connected, if a trusted channel error occurred, and accepts only those responses received from the initially authenticated chip (see FIA_UAU.5/PACE.PCD).

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

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

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

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

FIA_USB.1/ PACE.PCD	User-subject binding – PACE/PCD
Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1/ PACE/PCD	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 PICC role with SK4TC referenced in *keyReferenceList.macCalculation* and *keyReferenceList.dataEncipher*[351].
FIA_USB.1.2/ PACE.PCD	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[352].
FIA_USB.1.3/ PACE.PCD	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 successfully authenticated using PACE protocol in PICC role is set to "authenticated" and the authentication reference data SK4TC is stored in *keyReferenceList.macCalculation* and *keyReferenceList. dataEncipher*. (2) 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 gained using PACE protocol in PICC role and bound to the SK4TC is changed to "not authenticated" (i.e. the *keyReferenceList.macCalculation*, *keyReferenceList. dataEncipher* and the SK4TC are deleted)[353].

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

FDP_RIP.1/ PACE.PCD	Subset residual information protection – PACE/PCD
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1/ PACE.PCD	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*][354] the following objects: (1) trusted channel keys (immediately after closing related communication session), (2) any ephemeral secret having been generated during DH key exchange,

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

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

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

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

(3) [assignment: *list of additional objects*][355].

395 The TOE shall meet the requirement "TOE emanation – PACE/PCD (FPT_EMS.1/PACE.PCD)" as specified below (CC Part 2 extended).

FPT_EMS.1/ PACE.PCD	TOE emanation – PACE/PCD
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1/ PACE.PCD	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to (1) CAN, (2) PACE session keys, (3) any ephemeral secret having been generated during DH key exchange, (4) any object listed in FPT_EMS.1, (5) [assignment: *list of additional types of TSF data*][356] and [assignment: *list of types of user data*].
FPT_EMS.1.2/ PACE.PCD	The TSF shall ensure any users[357] are unable to use the following interface the contactless interface and circuit contacts[358] to gain access to (1) CAN, (2) PACE session keys, (3) any ephemeral secret having been generated during DH key exchange, (4) any object listed in FPT_EMS.1, (5) [assignment: *list of additional types of TSF data*][359] and [assignment: *list of types of user data*].

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

FTP_ITC.1/ PACE.PCD	Inter-TSF trusted channel – PACE/PCD
Hierarchical to:	No other components.

[355] [assignment: *list of objects*]

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

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

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

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

Dependencies:	No dependencies.
FTP_ITC.1.1/ PACE.PCD	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.PCD	The TSF shall permit another trusted IT product[360] to initiate communication via the trusted channel.
FTP_ITC.1.3/ PACE.PCD	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for data exchange between the TOE and the external user after successful establishing the trusted channel by means of PACE[361].

397 *Application note 60*: The trusted IT product is the terminal. In FTP_ITC.1.3/PACE.PCD, 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 the terminal and shutdown the trusted channel after integrity violation of the received data for decryption or MAC verification.

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

FMT_SMR.1/ PACE.PCD	Security roles – PACE/PCD
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1/ PACE.PCD	The TSF shall maintain the roles (1) the roles defined in FMT_SMR.1, (2) PACE authenticated PICC, (3) [assignment: *additional authorised identified roles*][362].
FMT_SMR.1.2/ PACE/PCD	The TSF shall be able to associate users with roles.

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

FMT_MTD.1/ PACE.PCD	Management of TSF data – PACE/PCD
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/	The TSF shall restrict the ability to

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

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

362 [assignment: *the authorised identified roles*]

PACE.PCD

(1) read[363] [364] the keys of trusted channel established using PACE protocol in PCD role[365] to none[366],

(2) define[367] [368] the CAN used for PACE protocol in PCD role to everybody[369].

400 *Application note 61*: The refinement defined an additional rule for managing the CAN in a special case of the PACE protocol (i.e. the PCD role). The derived session keys SM4SM and SM4TC shall be kept secret.

9.5 Security Requirements Rationale for Package PACE for Proximity Coupling Device

401 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 PACE for Proximity Coupling Device.

	O.Integrity	O.Confidentiality	O.Resp-COS	O.TSFDataExport	O.Authentication	O.AccessControl	O.KeyManagement	O.Crypto	O.PACE_Terminal
FCS_CKM.1/DH.PACE.PCD								X	X
FCS_CKM.4/PACE.PCD								X	X
FCS_COP.1/PACE.PCD.ENC								X	X
FCS_COP.1/ PACE.PCD.MAC								X	X
FDP_RIP.1/PACE.PCD		X							X
FPT_EMS.1/PACE.PICC		X			X				X
FIA_UAU.5/PACE.PCD					X				X
FIA_UAU.6/PACE.PCD					X				X
FIA_USB.1/PACE.PCD					X	X			X
FMT_MTD.1/PACE.PCD		X			X				X

[363] [assignment: *other operations*]

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

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

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

[367] [assignment: *other operations*]

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

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

	O.Integrity	O.Confidentiality	O.Resp-COS	O.TSFDataExport	O.Authentication	O.AccessControl	O.KeyManagement	O.Crypto	O.PACE_Terminal
FMT_SMR.1/PACE.PCD					X	X			X
FTP_ITC.1/PACE.PCD					X	X			X

Table 37: Mapping between Security Objectives for the TOE and SFRs for Package PACE for Proximity Coupling Device

402 **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.

403 All SFRs identified in the Package PACE for Proximity Coupling Device are implementing security functionality for the Security Objective **O.PACE_Terminal**.

404 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.PCD addresses this Security Objective as it requires that residual information regarding sensitive data in previously used resources will not be available after its usage. The SFR FMT_MTD.1/PACE.PCD requires to protect the confidentiality of the trusted channel keys against reading. The SFR FPT_EMS.1/PACE.PCD protect the confidential authentication data against compromise.

405 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_UAU.5/PACE.PCD requires the TSF to support the PACE protocol and secure messaging based on PACE trusted channel keys. Further, the TSF shall authenticate all users based on the PACE protocol.
- FIA_UAU.6/PACE.PCD requires the TSF to support re-authentication of users under dedicated conditions as given in the SFR.
- FPT_EMS.1/PACE.PCD 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.PCD requires that the TSF restricts the ability to change password objects by the implementation of dedicated commands and management functions.
- FTP_ITC.1/PACE.PCD 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.PCD requires that the TSF maintains roles and associates users with roles.

406 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:

- FMT_SMR.1/PACE.PCD requires that the TSF maintains roles and associates users with roles.
- FIA_USB.1/PACE.PCD 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.
- FTP_ITC.1/PACE.PCD 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.

407 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.PCD requires that the TSF generate cryptographic keys with the Diffie-Hellman-Protocol or ECDH.
- FCS_CKM.4/PACE.PCD requires that the TSF destroys cryptographic keys in accordance with a given specific key destruction method.
- FCS_COP.1/PACE.PCD.ENC requires that the TSF provides decryption and encryption using AES to be used for secure messaging.
- FCS_COP.1/PACE.PCD.MAC requires that the TSF provides computation and verification of cryptographic checksums using the CMAC algorithm to be used for secure messaging.

408 The Security Objective **O.PACE_Terminal** "Protection of contactless communication with PACE/PCD" requires the TOE support of the terminal part of the PACE protocol in order to protect the confidentiality and the integrity of data communicated through the contactless interface of the terminal. All SFRs, i.e. FCS_CKM.1/DH.PACE.PCD, FCS_CKM.4/PACE.PCD, FCS_COP.1/PACE.PCD.ENC, FCS_COP.1/PACE.PCD.MAC, FDP_RIP.1/PACE.PCD, FPT_EMS.1/PACE.PCD, FIA_UAU.5/PACE.PCD, FIA_UAU.6/PACE.PCD, FIA_USB.1/PACE.PCD, FMT_MTD.1/PACE.PCD, FMT_SMR.1/PACE.PCD, FTP_ITC.1/PACE.PCD, are defined to meet this Security Objective specific for the Package PACE for Proximity Coupling Device.

409 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
FCS_CKM.1/ DH.PACE.PCD	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation],	FCS_COP.1/PACE.PCD.ENC, FCS_COP.1/PACE.PCD.MAC, FCS_CKM.4/PACE.PCD

SFR	dependent on	fulfilled by
	FCS_CKM.4 Cryptographic key destruction	
FCS_CKM.4/ PACE.PCD	[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.PCD
FCS_COP.1/ PACE.PCD.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.PCD, FCS_CKM.4/PACE.PCD
FCS_COP.1/ PACE.PCD.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.PCD, FCS_CKM.4/PACE.PCD
FIA_UAU.5/PACE.PCD	No dependencies.	n. a.
FIA_UAU.6/PACE.PCD	No dependencies.	n. a.
FIA_USB.1/PACE.PCD	FIA_ATD.1 User attribute definition	FIA_ATD.1/PACE
FPT_EMS.1/PACE.PCD	No dependencies.	n. a.
FTP_ITC.1/PACE.PCD	No dependencies.	n. a.
FDP_RIP.1/PACE.PCD	No dependencies.	n. a.
FMT_SMR.1/PACE.PCD	FIA_UID.1 Timing of identification	FIA_UID.1/PACE
FMT_MTD.1/PACE.PCD	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FMT_SMR.1/PACE, FMT_SMF.1

Table 38: Dependencies of the SFRs for Package PACE for Proximity Coupling Device

10 Package Logical Channel

410 The COS may support optionally additional functionality for logical channels according to [21]. This section defines the Package Logical Channel to be used by the ST author if the TOE provides this security functionality.

10.1 TOE Overview for Package Logical Channel

411 In addition to the TOE definition given in section 1.2.1 “TOE definition and operational usage” the TOE is equipped with additional logic channels. The extension is purely functional. The command GET RANDOM is included in the option for logical channels in [21].

10.2 Security Problem Definition for Package Logical Channel

10.2.1 Assets and External Entities

Assets

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

Subjects and external entities

413 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

414 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

415 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.

416 *Application note 62:* The COS specification [21] describes the concept of logical channels in section 12.

10.2.4 Assumptions

417 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

418 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.

419 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.

420 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.

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

10.4 Security Requirements for Package Logical Channel

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

423 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.
FCS_RNG.1.1/GR	The TSF shall provide a physical[370] random number generator **of RNG class [selection: *PTG.2, PTG.3*] ([6]) for GET RANDOM** that implements: [assignment: *list of security capabilities* ***of the selected RNG class***].

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

FCS_RNG.1.2/GR	The TSF shall provide random ~~numbers~~ **[selection:** ***bits, octets of bits, numbers [assignment: format of the numbers]]*** that meet [assignment: ~~a~~ *defined quality metric* ***of the selected RNG class***].

424 *Application note 63*: If the TOE will provide random numbers by means of the command GET RANDOM for key generation of external devices like the connector (i.e. usage as gSMC-K) or the eHealth Card Terminals (i.e. usage as gSMC-KT) the provided random numbers shall meet TR-03116-1 [19] section 3.5. If the command GET RANDOM 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 this purpose.

425 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[371].
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: (1) If a new logical channel is opened the authentication state is "not authenticated" for all contexts within that logical channel[372].
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) [assignment: *rules for the changing of attributes*][373].

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

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

426 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[374] on (1) the subjects 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[375].

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

FDP_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[376] 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"[377].
FDP_ACF.1.2/LC	The TSF shall enforce the following rules to determine if an operation

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

374 [assignment: *access control SFP*]

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

376 [assignment: *access control SFP*]

377 [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*]

among controlled subjects and controlled objects is allowed:

(1) The command MANAGE CHANNEL is [selection: *ALWAYS allowed*, *[assignment*: *supported access control rules]*].

(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*[378].

FDP_ACF.1.3/LC The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[379].

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[380].

428 *Application note 64:* The COS specification [21] claims that the security attribute "shareable" is always TRUE.

429 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[381] to provide restrictive[382] 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,**

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

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

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

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

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

(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[383] 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

430 The following table provides an overview for Security Functional Requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen in the Package Logical Channel.

	O.Integrity	O.Confidentiality	O.Resp-COS	O.TSFDataExport	O.Authentication	O.AccessControl	O.KeyManagement	O.Crypto	O.SecureMessaging	O.LogicalChannel
FCS_RNG.1/GR										X
FIA_USB.1/LC						X				X
FDP_ACC.1/LC						X				X
FDP_ACF.1/LC						X				X
FMT_MSA.3/LC						X				X

Table 39: Mapping between Security Objectives for the TOE and SFRs for Package Logical Channel

431 **Table 39** 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.

432 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, 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.

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

- 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.

433 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 40** should be taken as extension of **Table 25** in order to cover all dependencies.

SFR	**dependent on**	**fulfilled by**
FCS_RNG.1/GR	No dependencies.	n. a.
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 40: Dependencies of the SFRs for Package Logical Channel

11 Package RSA CVC

434 The COS may support optionally additional cryptographic functionality for RSA that is related to Card Verifiable Certificates (CVC) according to Option_RSA_CVC in [21]. This section defines the Package RSA CVC to be used by the ST author if the TOE provides this security functionality.

11.1 TOE Overview for Package RSA CVC

435 In addition to the TOE definition given in section 1.2.1 "TOE definition and operational usage" the TOE is equipped with further cryptographic functionality for RSA related to CVCs according to Option_RSA_CVC in [21].

11.2 Security Problem Definition for Package RSA CVC

11.2.1 Assets and External Entities

Assets

436 The assets do not differ from the assets already defined in section 3.1. However, their scope is widened in view of the RSA-based CVC functionality according to Option_RSA_CVC in [21], i.e. the assets described in section 3.1 address and cover now as well the RSA-based CVC functionality.

Subjects and external entities

437 There are no additional external entities and subjects for the Package RSA CVC beyond those already defined in section 3.1. However, their scope is widened in view of the RSA-based CVC functionality according to Option_RSA_CVC in [21], i.e. the subjects and external entities described in section 3.1 address and cover now as well the RSA-based CVC functionality.

11.2.2 Threats

438 There are no additional Threats for the Package RSA CVC beyond the Threats already defined in section 3.2. However, their scope is widened in view of the RSA-based CVC functionality according to Option_RSA_CVC in [21], i.e. the Threats described in section 3.2 address and cover now as well the RSA-based CVC functionality.

11.2.3 Organisational Security Policies

439 There are no additional Organisational Security Policies for the Package RSA CVC beyond the Organisational Security Policies already defined in section 3.3. However, their scope is widened in view of the RSA-based CVC functionality according to Option_RSA_CVC in [21], i.e. the

Organisational Security Policies described in section 3.3 address and cover now as well the RSA-based CVC functionality.

11.2.4 Assumptions

440 There are no additional Assumptions for the Package RSA CVC beyond the Assumptions already defined in section 3.4. However, their scope is widened in view of the RSA-based CVC functionality according to Option_RSA_CVC in [21], i.e. the Assumptions described in section 3.4 address and cover now as well the RSA-based CVC functionality.

11.3 Security Objectives for Package RSA CVC

441 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 CVC beyond the Security Objectives already defined in sections 4.1 and 4.2. However, their scope is widened in view of the RSA-based CVC functionality according to Option_RSA_CVC in [21], i.e. the Security Objectives described in the sections 4.1 and 4.2 address and cover now as well the RSA-based CVC functionality.

11.4 Security Requirements for Package RSA CVC

442 All Security Functional Requirements (SFRs) for the TOE defined in section 6.1 are taken over to the Package RSA CVC. However, their scope is widened to the RSA-based CVC functionality according to Option_RSA_CVC 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 related RSA key objects and certificates (CVC), the handling of the CHA and the contents and handling of the security attributes *globalSecurityList* and *dfSpecificSecurityList*.

443 In addition, the TOE shall meet the following SFRs in order to address the additional cryptographic functionality related to the RSA-based CVC functionality according to Option_RSA_CVC in [21].

444 The TOE shall meet the requirement “Cryptographic operation – RSA signature-creation (FCS_COP.1/RSA.CVC.S)” as specified below.

FCS_COP.1/RSA.CVC.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/	The TSF shall perform digital signature generation for command

RSA.CVC.S	(1) INTERNAL AUTHENTICATE[384] in accordance with a specified cryptographic algorithm RSA ISO9796-2 DS1 with SHA-256[385] and cryptographic key sizes 2048 bit modulus length[386] that meet the following: TR-03116-1 [19], COS specification [21], [31], [34][387].

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

FCS_COP.1/RSA.CVC.V	Cryptographic operation – RSA signature verification
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ RSA.CVC.V	The TSF shall perform digital signature verification for import of RSA keys using the commands (1) PSO VERIFY CERTIFICATE, (2) EXTERNAL AUTHENTICATE[388] in accordance with a specified cryptographic algorithm RSA ISO9796-2 DS1[389] and cryptographic key sizes 2048 bit modulus length[390] that meet the following: TR-03116-1 [19], COS specification [21], [31] ,[34][391].

446 *Application note 65*: The command PSO VERIFY CERTIFICATE may store the imported public keys for RSA temporarily in the *volatileCache* or permanently in the *persistentCache* or *applicationPublicKeyList*. These keys may be used as authentication reference data for asymmetric key based device authentication (cf. FIA_UAU.5) or User Data.

11.5 Security Requirements Rationale for Package RSA CVC

447 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 CVC.

384 [assignment: *list of cryptographic operations*]

385 [assignment: *list of cryptographic operations*]

386 [assignment: *cryptographic key sizes*]

387 [assignment: *list of standards*]

388 [assignment: *list of cryptographic operations*]

389 [assignment: *cryptographic algorithm*]

390 [assignment: *cryptographic key sizes*]

391 [assignment: *list of standards*]

	O.Integrity	O.Confidentiality	O.Resp-COS	O.TSFDataExport	O.Authentication	O.AccessControl	O.KeyManagement	O.Crypto	O.SecureMessaging	O.TrustedChannel
FCS_COP.1/RSA.CVC.S								X		
FCS_COP.1/RSA.CVC.V								X		

Table 41: Mapping between Security Objectives for the TOE and SFRs for Package RSA CVC

448 **Table 41** 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.

449 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_COP.1/RSA.CVC.S requires that the TSF provides the generation of digital signatures based on the RSA algorithm in the framework of the RSA-based CVC functionality according to Option_RSA_CVC in [21].
- FCS_COP.1/RSA.CVC.V requires that the TSF provides the verification of digital signatures based on the RSA algorithm in the framework of the RSA-based CVC functionality according to Option_RSA_CVC in [21].

450 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 42** should be taken as extension of **Table 25** and **Table 44** (if applicable) in order to cover all dependencies. In particular, **Table 42** 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**
FCS_COP.1/RSA.CVC.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* in the case that the TOE provides RSA key generation functionality, i.e. Package RSA Key Generation is applied. Otherwise, dependency on FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1 is not applicable as neither key import nor key generation by the TOE for RSA key pairs / private keys are relevant for the operational phase.

SFR	dependent on	fulfilled by
		FCS_CKM.4
FCS_COP.1/RSA.CVC.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	*FCS_CKM.1/RSA* in the case that the TOE provides RSA key generation functionality, i.e. Package RSA Key Generation is applied. Otherwise, dependency on FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1 is not applicable as neither key import nor key generation by the TOE for RSA key pairs / private keys are relevant for the operational phase. FCS_CKM.4
Hint: *FCS_CKM.1/RSA* in the case that 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 44**: FCS_COP.1/RSA.CVC.S, FCS_COP.1/RSA.CVC.V

Table 42: Dependencies of the SFRs for Package RSA CVC

12 Package RSA Key Generation

451 The COS may support optionally additional cryptographic functionality related to RSA key generation according to Option_RSA_KeyGeneration in [21]. This section defines the Package RSA Key Generation to be used by the ST author if the TOE provides this security functionality.

12.1 TOE Overview for Package RSA Key Generation

452 In addition to the TOE definition given in section 1.2.1 “TOE definition and operational usage” the TOE is equipped with further cryptographic functionality related to RSA key generation by the TOE.

12.2 Security Problem Definition for Package RSA Key Generation

12.2.1 Assets and External Entities

Assets

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

Subjects and external entities

454 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.

12.2.2 Threats

455 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.

12.2.3 Organisational Security Policies

456 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.

12.2.4 Assumptions

457 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.

12.3 Security Objectives for Package RSA Key Generation

458 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.

12.4 Security Requirements for Package RSA Key Generation

459 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.

460 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].

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

FCS_CKM.1/RSA	Cryptographic key generation – RSA key generation
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or 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 [assignment: *cryptographic key generation algorithm*][392] and specified cryptographic key sizes 2048 bit and 3072 bit modulus length[393] that meet the following: TR-03116-1 [19][394].

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

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

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

462 *Application note 66*: The COS specification [21] specifies the command GENERATE ASYMMETRIC KEY PAIR for the generation of RSA key pairs as an option for the TOE implementation. The TOE may support the generation of asymmetric key pairs for the following operations:

- qualified electronic signatures,
- authentication of external entities,
- document cipher key decipherment.

463 The ST author shall perform the missing operation in the element FCS_CKM.1/RSA according to the implemented key generation algorithm.

12.5 Security Requirements Rationale for Package RSA Key Generation

464 The following table provides an overview for Security Functional Requirements coverage also giving an evidence for *sufficiency* and *necessity* of the SFRs chosen in the Package RSA Key Generation.

	O.Integrity	O.Confidentiality	O.Resp-COS	O.TSFDataExport	O.Authentication	O.AccessControl	O.KeyManagement	O.Crypto	O.SecureMessaging
FCS_CKM.1/RSA							X	X	

Table 43: Mapping between Security Objectives for the TOE and SFRs for Package RSA Key Generation

465 **Table 43** 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.

466 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.

467 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.

468 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 44** 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 *FCS_COP.1/CB.RSA* in the case that the TOE provides crypto box functionality, i.e. Package Crypto Box is applied. *FCS_COP.1/RSA.CVC.S*, *FCS_COP.1/RSA.CVC.V* in the case that the TOE provides RSA CVC functionality, i.e. Package RSA CVC is applied.

Table 44: Dependencies of the SFRs for Package RSA Key Generation

13 Annex: Composite Evaluation of Smart Cards as Signature Products based on COS Smart Card Platforms (Informative)

469 The TOE of the Protection Profile in hand may be used as smart card platform for signature products that are intended to be used as Secure Signature Creation Device (SSCD) or as part of a Signature Creation Application (SCA). The signature product as SSCD for qualified electronic signatures shall be evaluated and certified on base of the Common Criteria for its approval as signature product according to the so-called eIDAS regulation, refer to [43] and [44]. As being part of an SCA the evaluation and certification of the signature product is recommended in order to support the approval of the SCA as signature product in the sense of the eIDAS regulation [43] and [44].

470 Such an evaluation may be performed as composite evaluation [8] with a certified TOE conforming to the Protection Profile in hand as 'Certified Platform' and the object system of the signature product on top of this platform as 'Application'.

471 This informative annex provides information how security targets for such composite evaluation may be written, using the example of the electronic Health Card (eHC) and the electronic Health Professional Card (eHPC) as an SSCD as well as the device-specific Secure Module Cards of the Card Terminal (gSMC-KT) and of the Konnektor (gSMC-K) as part of an SCA. The discussion is based on the Protection Profiles [12], [13], [14] and [15] that prescribe security requirements for the SSCD.

472 Note that in the framework of the eIDAS regulation the approval of an SSCD as a signature product for qualified electronic signatures requires the SSCD to be conformant to a Protection Profile listed in [44].

13.1 Smart Cards as Secure Signature Creation Devices based on COS Smart Card Platforms (Informative)

473 The preparation of a smart card as SSCD includes the following steps:

(1) The personalisation as SSCD comprises the definition of the Signatory as authorised user of the signature creation data (SCD) in the SSCD, i.e. a private signature key.

(2) The initialisation of the SSCD comprises the loading of the signature key pair into the SSCD or the generation of such key pair by the SSCD itself. The SSCD shall implement the SCD and should implement the signature verification data (SVD), i.e. the public key e.g. for the verification of the digital signatures generated with the private key as self-test.

(3) The generation of the qualified certificate by the Certification Service Provider for qualified certificates (CSP-QC) comprises the generation of a certificate that contains the SVD which corresponds to the SCD under the control of the Signatory, the name of the Signatory or a pseudonym (which is to be identified as such) and an indication of the beginning and end of the validity period of the certificate. The qualified certificate shall be verifiable by means of the directory services of the CSP-QC. The CSP-QC should load related certificate info or the certificate itself into the SSCD for convenience of the Signatory.

474 The following sections assume that the eHC and the eHPC implement the MF and the DF.QES as defined in the object system specifications [22] for the eHC and [23] for the eHPC.[395]

475 The ST for the eHC and the eHPC as SSCD may claim conformance to the Protection Profile in hand and shall claim conformance to the appropriate SSCD Protection Profile according to the requirements in [44] depending on the method of initialisation and the method of use as SSCD.

13.1.1 eHC as SSCD

476 The eHC is issued by the German health insurance companies to patients insured by them for the use of health care services. If wished by the patient as cardholder of the eHC such smart card shall be prepared by a CSP-QC as SSCD where the patient is the Signatory.

477 The object system specification of the eHC [22] already specifies in the DF.QES

(1) the user Signatory by means of the PIN object PIN.QES,

(2) the signature creation data as Pr.CH.QES.R2048 (mandatory) and Pr.CH.QES.R3072 and Pr.CH.QES.E384 (optional),

(3) the EF.C.CH.QES.R2048 and optional additional files for other certificates.

478 The role Signatory is different from the role cardholder defined by the regular password PIN.CH in the MF and the roles defined by the multi-reference passwords that reference to the secret of the PIN.CH.

479 The eHC may be initialised in three different ways:

(1) The CSP-QC may generate the signature key pair by the eHC and export the public key from the SSCD to the certificate-generation application in its trusted environment. In this case, the ST author should claim conformance to the Protection Profile [12] for Secure Signature Creation Devices with key generation.

(2) The CSP-QC may generate the signature key pair and load the private key as signature creation data into the SSCD. The CSP-QC will send the public key to the certificate-generation application in its trusted environment. In this case, the ST author should claim conformance to the Protection Profile [13] for Secure Signature Creation Devices with key import.

(3) The CSP-QC or the Signatory may generate the signature key pair by the eHC and export the public key from the SSCD to the certificate-generation application through a trusted channel after delivery of the smart card to the cardholder. In this case, the ST author should claim conformance to the Protection Profile [14] for Secure Signature Creation Devices with key generation and trusted communication with the certificate-generation application.

480 Note that the object system specification of the eHC [22] does not specify the access control rules for Pr.CH.QES.x and the command GENERATE ASYMMETRIC KEY PAIR and therefore allows for product and CSP-QC specific solutions.

[395] Note that the smart card platform, the MF and the DF.QES define the security features of the eHC and the eHPC in respect of the qualified electronic signature. The other parts of the object system must not affect this security functionality. The MF and the DF.QES specification are expected to be stable and independent of updates of the object system specifications.

481 The regular password PIN.QES shall be protected by setting the security attribute *transportStatus* to *Transport-PIN* in time of delivery of the eHC to the cardholder and before personalisation as SSCD and by changing the *transportStatus* to *regularPassword* by the Signatory. The security attribute "*SCD operational*" defined in the SSCD Protection Profiles [12] and [13] and referenced by conformance claim in [14] is implemented by means of the security attribute *transportStatus* of the PIN.QES, where the value *Transport-PIN* of the security attribute *transportStatus* meets the value "*no*" of the security attribute "*SCD operational*" and the value *Reguläres Passwort* of the security attribute *transportStatus* meets the value "*yes*" of the security attribute "*SCD operational*".

482 The access control rules of the signature creation data Pr.CH.QES.R2048, Pr.CH.QES.R3072 and Pr.CH.QES.E384 for the signature creation function by means of the command PSO COMPUTE DIGITAL SIGNATURE as defined in [22] meet the SFR FDP_ACF.1/Signature_Creation as defined in the SSCD Protection Profiles [12], [13] and [14].

13.1.2 eHPC as SSCD

483 The eHPC is issued as SSCD (mandatory). The eHPC supports

(1) local PIN entry, i.e. it is assumed that the PIN is entered at the same smart card terminal as the eHPC is used and is sent to the eHPC in clear text,

(2) remote PIN entry, i.e. the smart card terminal used as PIN entry device transmits the PIN through a trusted channel to the eHPC in another (or even the same) smart card terminal,

(3) single signature creation, i.e. creation of only one signature after authentication as Signatory,

(4) batch signature creation, i.e. creation of one or more signatures after authentication as Signatory.

484 The object system specification of the eHPC [23] already specifies in the DF.QES

(1) the user Signatory by means of the PIN object PIN.QES,

(2) the signature creation data as Pr.CH.QES.R2048 (mandatory) and Pr.CH.QES.R3072 and Pr.CH.QES.E384 (optional),

(3) the EF.C.CH.QES.R2048 and optional additional files for other certificates.

485 The role Signatory is different from the role cardholder defined by the regular password PIN.CH in the MF and the roles defined by the multi-reference passwords that reference to the secret of the PIN.CH.

486 The eHPC may be initialised in three different ways:

(1) The CSP-QC may generate the signature key pair by the eHPC and export the public key from the SSCD to the certificate-generation application in its trusted environment. In this case, the ST author should claim conformance to the Protection Profile [12] for Secure Signature Creation Devices with key generation.

(2) The CSP-QC may generate the signature key pair and load the private key as signature creation data into the SSCD. The CSP-QC will send the public key to the certificate-generation application in its trusted environment. In this case, the ST author should claim conformance to the Protection Profile [13] for Secure Signature Creation Devices with key import.

(3) The CSP-QC or the Signatory may generate the signature key pair by the eHPC and export the public key from the SSCD to the certificate-generation application through a trusted channel after delivery of the smart card to the cardholder. In this case, the ST author should claim conformance to the Protection Profile [14] for Secure Signature Creation Devices with key generation and trusted communication with the certificate-generation application.

487 Note that the object system specification of the eHPC [23] does not specify the access control rules for Pr.CH.QES.x and the command GENERATE ASYMMETRIC KEY PAIR but leave the access control rules up to the CSP-QS. Because of the mandatory initialisation of the eHPC as SSCD the case (3) is unlikely of practical use for the first SCD but may be considered for the update of the DF.QES with a new SCD and corresponding certificates.

488 The regular password PIN.QES shall be protected by setting the security attribute *transportStatus* to *Transport-PIN* in time of delivery of the eHPC to the cardholder and before personalisation as SSCD and by changing the *transportStatus* to *regularPassword* by the Signatory. The security attribute "*SCD operational*" defined in the SSCD Protection Profiles [12] and [13] and referenced by conformance claim in [14] is implemented by means of the security attribute *transportStatus* of the PIN.QES, where the value *Transport-PIN* of the security attribute *transportStatus* meets the value "*no*" of the security attribute "*SCD operational*" and the value *Reguläres Passwort* of the security attribute *transportStatus* meets the value "*yes*" of the security attribute "*SCD operational*".

489 The PIN authentication using a remote smart card terminal as PIN entry device requires the confidentiality protection of the PIN transmitted between this terminal and the eHPC. This confidentiality protection is enabled by the Konnektor controlling the mutual authentication between the gSMC-KT as PIN sender and the eHPC as PIN receiver and establishing a secure messaging channel between them. Note that the eHPC does not enforce secure messaging as PIN receiver for the PIN.QES because the eHPC supports both local PIN entry and remote PIN entry and cannot distinguish between them.

490 The access control rules for the single signature creation function with the signature creation data Pr.CH.QES.R2048, Pr.CH.QES.R3072 and Pr.CH.QES.E384 and the command PSO COMPUTE DIGITAL SIGNATURE as defined in [23] require successful authentication with PIN.QES only and meet the SFR FDP_ACF.1/Signature_Creation as defined in the SSCD Protection Profiles [12], [13] and [14].

491 The access control rules for the batch signature creation function with the signature creation data Pr.CH.QES.R2048, Pr.CH.QES.R3072 and Pr.CH.QES.E384 and the command PSO COMPUTE DIGITAL SIGNATURE as defined in [23] enforce

(1) successful authentication of the Signatory with PIN.QES, and

(2) successful device authentication, i.e. of the gSMC-K as representative of the SCA of the Konnektor and as sender of the data to be signed (DTBS) (cf. section 13.2.2, gSMC-K as part of the SCA of the Konnektor), and following secure messaging with protection of integrity and confidentiality.

492 The security requirements for the protected communication between the SSCD (with on-board key generation) and the SCA are defined in the Protection Profile [15] for Secure Signature Creation Devices with key generation and trusted communication with the signature creation application. For an SSCD with key import, the ST author may use the SFRs in an analogous way.

493 Note that the Protection Profile [15] requires the SSCD or human interface device (i.e. the smart card terminal) to initiate the trusted channel for the protection of the signature verification data

(i.e. confidentiality and integrity in case of PIN), cf. SFR FTP_ITC.1/VAD. Furthermore, the Protection Profile [15] requires the SSCD to detect manipulation and insertion of the DTBS received, cf. FDP_UIT.1/DTBS, and requires the establishment of a trusted channel between the SCA and the SSCD for signature creation, cf. FTP_ITC.1/DTBS. Therefore, the ST author **cannot** claim conformance to the Protection Profile [15] for the ST describing the eHCP as SSCD.

494 The ST author should instead of this describe more precise Security Objectives for the Operational Environment to address the usage of a trusted channel for remote PIN entry like this:

OE.TC_PIN	**Trusted channel for remote PIN entry** The PIN entry device shall authenticate itself as PIN sender and the TOE as PIN receiver, and shall send the PIN of the Signatory in a trusted channel to the TOE.

495 The ST author may describe more precise Security Objectives for the TOE and its operational environment and similar but not identical SFRs in order

(1) to allow for single signature creation without a trusted channel for the DTBS and

(2) to enforce the authentication and the transmission of the DTBS in the established trusted channel as access control condition for thr batch signature creation

496 like described in the following.

497 The objectives may be described like this:

O.BatchSignature	**Batch signature support** The TOE shall enforce the authentication of the SCA and the transmission of the DTBS in the established trusted channel as access control condition for the batch signature creation.
OE.BatchSignature	**Batch signature control** The SCA shall authenticate itself to the TOE and transmit the DTBS for the batch signature creation in the established trusted channel to the TOE.

498 The access control may be described like this:

FDP_ACC.1/BatchSign	Subset access control – Batch signature creation
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ BatchSign	The TSF shall enforce the Signature-creation SFP[396] on (1) subjects: a. signatory, b. signature creation application, (2) objects:

396 [assignment: *access control SFP*]

a. signature creation data PrK.HP.QES,

b. DTBS-representation,

(3) operations:

a. command PSO COMPUTE DIGITAL SIGNATURE[397].

499

FDP_ACF.1/BatchSign	Security attribute based access control – Batch signature creation
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ BatchSign	The TSF shall enforce the Signature-creation SFP[398] to objects based on the following: (1) subjects: a. human user with authentication state, b. signature creation application with authentication state, (2) objects: a. signature creation data PrK.HC.QES with security attribute *lifeCycleStatus* set to "*Operational state (active)*", b. DTBS-representation[399].
FDP_ACF.1.2/ BatchSign	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) the human user successfully authenticated with PIN.QES is allowed to create 1 signature using PrK.HP.QES with *lifeCycleStatus* set to *"Operational state (active)"* by means of the command PSO COMPUTE DIGITAL SIGNATURE in security environment #1, (2) the human user successfully authenticated with PIN.QES and using signature creation application successfully authenticated with CHA 'D2760000400033' with trusted channel to the TOE is allowed to create n signatures using PrK.HP.QES with *lifeCycleStatus* set to *"Operational state (active)"* by means of the command PSO COMPUTE DIGITAL SIGNATURE in security environment #2[400].

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

398 [assignment: *access control SFP*]

399 [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*]

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

FDP_ACF.1.3/ BatchSign	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[401].
FDP_ACF.1.4/ BatchSign	The TSF shall explicitly deny access of subjects to objects based on the rule: (1) to create signature without security attribute *lifeCycleStatus* of PrK.HP.QES set to "*Operational state (active)*", (2) to create more than one signature with PrK.HP.QES after successful authentication with PIN.QES by sending the DTBS-representation without secure messaging provided by signature creation application successfully authenticated with CHA 'D2760000400033'[402].

500 The secure messaging channel may be described like this:

FTP_ITC.1/ SM_BatchSig	Inter-TSF trusted channel – Secure Messaging for batch signature
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/SM_BatchSig	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/SM_BatchSig	The TSF shall permit the TSF[403] to initiate communication via the trusted channel.
FTP_ITC.1.3/SM_BatchSig	The TSF shall ~~**initiate**~~ **enforce**[404] communication via the trusted channel **with SK4SM** for receiving of commands from the SCA and sending responses to the SCA[405].

501 The selection in the element FTP_ITC.1.2/SM_BatchSig is based on the first command GET CHALLENGE sent to the TOE in order to initiate the mutual authentication protocol including the generation of the secure messaging keys SK4SM of the TSF (cf. [21], section 15.4.1).

502 The refinement in the element FTP_ITC.1.3/SM_BatchSig describes that the eHPC uses secure messaging with SK4SM. Note that the COS specification [21] distinguishes (simplified) between

(1) secure messaging for smart cards

(a) verifying the MAC of received commands and decrypting received data and

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

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

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

404 Refinement: The trusted IT product is the terminal. The word "initiate" is changed to 'enforce", as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforces the trusted channel.

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

(b) encrypting and MAC calculating the responses, and

(2) trusted channel for smart cards

(a) encrypting the data of commands and MAC calculating for the commands and

(b) MAC verification and decrypting the data of the responses.

503 The CC terminology summarizes the communication under the term “trusted channel”.

13.2 Smart Cards as Part of Signature Creation Applications based on COS Smart Card Platforms (Informative)

13.2.1 gSMC-KT as part of the electronic Health Card Terminal

504 The electronic Health Card Terminal (eHCT) may be used as PIN entry device for the PIN.QES of the Signatory to be sent to the SSCD eHPC. In this case, the eHCT is part of the SCA. The eHCT may use the gSMC-KT for

- protection of confidentiality and integrity of the PIN.QES by sending the PIN commands through a trusted channel,
- protected storage of asymmetric key material and other security critical data in the DF.KT used for establishing the TLS channel between the eHCT and the Konnektor as described in the Technical Guideline for batch signature creation [18].

505 The security functionality of the trusted channel used by the gSMC-KT is already described in section 7 for the Package Crypto Box.

506 The private key for the authentication as PIN sender to the SSCD eHPC is the key PrK.SMC.AUTD_RPS_CVC.E256 (optionally PrK.SMC.AUTD_RPS_CVC.E384) for the gSMC-KT stored in the MF. The authentication reference data are the certificate C.SMC.AUTD_RPS_CVC.E256 (optionally C.SMC.AUTD_RPS_CVC.E384) for the gSMC-KT stored also in the MF. The establishment of the trusted channel between the eHPC and the gSMC-KT is controlled by the Konnektor. The ST author may describe the SFR for this trusted channel provided by the gSMC-KT by means of the component FTP_ITC.1.

507 The trusted channel provided by the gSMC-KT may be described like this:

FTP_ITC.1/ TC_PIN	Inter-TSF trusted channel – Trusted channel for batch signature
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/TC_PIN	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_PIN	The TSF shall permit another trusted IT product[406] to initiate communication via the trusted channel.
FTP_ITC.1.3/TC_PIN	The TSF shall ~~**initiate**~~ **enforce**[407] communication via the trusted channel **with SK4TC** for sending of PIN commands to the SSCD and receiving responses from the SSCD[408].

13.2.2 gSMC-K as part of the SCA of the Konnektor

508 The Konnektor implements an SCA and includes for this purpose a gSMC-K for

- protection of confidentiality and integrity of the DTBS by means of a trusted channel for sending the signature creation commands and receiving the digital signature for batch signature creation by the eHPC (cf. section 13.1.2, eHPC as SSCD),
- protected storage of asymmetric key material and other security critical data in the DF.SAK used for establishing the TLS channel between the eHCT and the Konnektor as described in the Technical Guideline for batch signature creation [18].

509 The security functionality of the trusted channel used by the gSMC-K is already described in section 7 for the Package Crypto Box.

510 The private key for the authentication of the gSMC-K as SCA is the key PrK.SAK.AUTD_CVC.E256 (alternatively PrK.SAK.AUTD_CVC.E384) for the gSMC-K stored in the DF.SAK. The authentication reference data are the certificate C.SAK.AUTD_CVC.E256 (optionally C.SAK.AUTD_CVC.E384) stored also in the DF.SAK. The establishment of the trusted channel between the eHPC and the gSMC-K is controlled by the SCA. The ST author may describe the SFR for this trusted channel by means of the component FTP_ITC.1.

511 The trusted channel provided by the gSMC-K may be described like this:

FTP_ITC.1/ TC_BatchSig	Inter-TSF trusted channel – Trusted channel for batch signature
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/TC_BatchSig	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_BatchSig	The TSF shall permit another trusted IT product[409] to initiate communication via the trusted channel.
FTP_ITC.1.3/TC_BatchSig	The TSF shall ~~**initiate**~~ **enforce**[410] communication via the trusted channel **with SK4TC** for sending of commands to the SSCD and

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

407 Refinement: The trusted IT product is the terminal. The word “initiate” is changed to ‘enforce”, as the TOE is a passive device that can not initiate the communication. All the communication is initiated by the Terminal, and the TOE enforces the trusted channel.

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

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

receiving responses from the SSCD[411].

[410] Refinement: The trusted IT product is the terminal. The word “initiate” is changed to ‘enforce”, as the TOE is a passive device that can not initiate the communication. All the communication is initiated by the Terminal, and the TOE enforces the trusted channel.

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

14 Acronyms

512 The terminology and abbreviations of Common Criteria Version 3.1 Revision 5 [1], [2], [3] and the specification [21] apply.

Acronyms	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 1.2.1)
eHC	electronic Health Card (elektronische Gesundheitskarte)
eHCT	electronic Health Card Terminal
eHPC	electronic Health Professional Card (elektronischer Heilberufsausweis)
eIDAS	electronic IDentification, Authentication and trust Services
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 (as defined in [16] Part 2)
PICC	Proximity Integrated Circuit Chip (as defined in [16] Part 2)
PKI	Public Key Infrastructure
PP	Protection Profile
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCD	Signature Creation Data

Acronyms	Term
SEF	Structured Elementary File
SFP	Security Function Policy
SFR	Security Functional Requirement
SICP	Secure Integrated Chip Platform
SMC-B	Secure Module Card Type B
SPD	Security Problem Definition
SSCD	Secure Signature Creation Device
SVD	Signature Verification Data
ST	Security Target
TEF	Transparent Elementary File
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

15 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, April 2017

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

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

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

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

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

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

[8] Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, Version 1.5, October 2017, JIL

[9] Joint Interpretation Library – The Application of CC to Integrated Circuits, February 2009, Version 3.0, 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] EN 419211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation, developed by CEN/ISSS - Information Society Standardization System, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the certification reference BSI-CC-PP-0059-2009-MA-02

[13] EN 419211-3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import, developed by CEN/ISSS - Information Society Standardization System, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the certification reference BSI-CC-PP-0075-2012-MA-01

[14] EN 419211-4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application, developed by CEN/ISSS - Information Society Standardization System, registered

and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the certification reference BSI-CC-PP-0071-2012-MA-01

[15] EN 419211-5:2013 – Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application, developed by CEN/ISSS - Information Society Standardization System, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the certification reference BSI-CC-PP-0072-2012-MA-01

Technical Guidelines and Specifications

[16] Technical Guideline BSI TR-03110:

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

Technical Guideline BSI TR-03110-2: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 21 December 2016, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Technical Guideline BSI TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications, Version 2.21, 21 December 2016, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[17] Technical Guideline BSI TR-03111: Elliptic Curve Cryptography, Version 2.0, 28.06.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

[19] Technische Richtlinie BSI TR-03116-1: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.19, 03.12.2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

[21] Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.11.0, 14.05.2018, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[22] Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem, Version 4.1.0, 18.12.2017, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[23] Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem, Version 4.1.0, 18.12.2017, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[24] Spezifikation der Secure Module Card SMC-B Objektsystem, Version 4.1.0, 18.12.2017, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[25] Spezifikation der gSMC-K Objektsystem, Version 3.10.0, 28.10.2016, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[26] Spezifikation gSMC-KT Objektsystem, Version 4.1.0, 18.12.2017, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[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 7816-9:2004 (2nd edition), Identification cards – Integrated circuit cards – Part 9: Commands for card management

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

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

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

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

[37] Federal Information Processing Standards Publication 180-4 (FIPS PUB 180-4), SECURE HASH STANDARD, 11 February 2011, 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 2005, ANSI

[40] American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 16 November 2005, ANSI

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

Other Sources

[42] ISO/IEC 14443-4:2016 (3rd edition), Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol

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

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

Additional references

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

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