Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Protection Profile

Card Operating System Generation 2 (PP COS G2)

Common Criteria

BSI-CC-PP-0082-V2

Approved by the
Federal Office for Information Security

Foreword

This Protection Profile 'Card Operating System (PP COS)' 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 [1], [2], [3], Revision 4.

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	Commentary
1.0	23rd August 2013	Final version for evaluation	
1.1	4th November 2013	Change FIA_AFL.1/PIN and FMT_MTD.1/PIN in order to comply with COS specification. GET RANDOM in Paket Logical Channel verschoben. FDP_SDI.2 aufgenommen.	
1.2	20th November 2013	Package PACE for Proximity Coupling Device added	
1.3	11th February 2014	update of the packages, commands FINGERPRINT and LIST PUBLIC KEY added, FDP_SDI.2 for objects with transaction protection, access control rule for PSO VERIFY CERTIFICATE added	
1.4	2nd April 2014	Clarification on antenna, update of the table 15 and package Crypto Box for trusted channel, FIA_SOS.1 added, update FIA_USB.1, FIA_API.1 is adapted to BSI-CC-PP-0084, access condition for command FINGERPRINT is adapted in FDP_ACF.1/MF_DF, adaption of refinement to ATE_FUN.1 and ATE_IND.2 due to optional packages and application, update of modul length of RSA in FCS_COP.1/COS.RSA.V, any subject is allowed to execute command PSO Verify Digital Signature.	
1.5	30th April 2014	Update due to BSI comments	
1.6	4th June 2014	RSA 3072 public key operation removed due to change of COS specification	
1.7	25 July 2014	Certification-ID, update of table 19.	
1.8	10 October 2014	References are updated, references to wrapper specification, BSI-CC-PP-0084 and JIL transition guide are 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	18th November 2014	Corrections due to BSI comments.	

Current Version: 1.9 (18th November 2014)

Contents

1 PP Introduction 7
1.1 PP reference 7
1.2 TOE Overview 7
1.2.1 TOE definition and operational usage 7
1.2.2 TOE major security features for operational use 8
1.2.3 TOE type 8
1.2.4 Non-TOE hardware/software/firmware 9
2 Conformance Claims 11
2.1 CC Conformance Claim 11
2.2 PP Claim 11
2.3 Package Claim 11
2.4 Conformance Claim Rationale 11
2.5 Conformance statement 12
3 Security Problem Definition 13
3.1 Assets and External Entities 13
3.2 Threats 14
3.3 Organisational Security Policies 16
3.4 Assumptions 17
4 Security Objectives 19
4.1 Security Objectives for the TOE 19
4.2 Security Objectives for Operational Environment 21
4.3 Security Objective Rationale 22
5 Extended Components Definition 27
5.1 Definition of the Family FCS_RNG Generation of Random Numbers 27
5.2 Definition of the Family FIA_API 28
5.3 Definition of the Family FPT_EMS TOE Emanation 28
5.4 Definition of the Family FPT_ITE TSF image export 29
6 Security Requirements 31
6.1 Security Functional Requirements for the TOE 31
6.1.1 Overview 32
6.1.2 Users, subjects and objects 33
6.1.3 Security Functional Requirements for the TOE taken over from BSI-CC-PP-0035-2007 47
6.1.4 General Protection of User data and TSF data 48
6.1.5 Authentication 53
6.1.6 Access Control 61

6.1.7 Cryptographic Functions 84
6.1.8 Protection of communication 94
6.2 Security Assurance Requirements for the TOE 94
6.2.1 Refinements of the TOE Assurance Requirements 96
6.2.2 Refinements to ADV_ARC.1 Security architecture description 97
6.2.3 Refinements to ADV_FSP.4 Complete functional specification 97
6.2.4 Refinement to ADV_IMP.1 97
6.2.5 Refinements to AGD_OPE.1 Operational user guidance 98
6.2.6 Refinements to ATE_FUN.1 Functional tests 98
6.2.7 Refinements to ATE_IND.2 Independent testing – sample 98
6.3 Security Requirements Rationale 99
6.3.1 Security Functional Requirements Rationale 99
6.3.2 Rationale for SFR's Dependencies 106
6.3.3 Security Assurance Requirements Rationale 111
7 Package Crypto Box 113
7.1 TOE Overview 113
7.2 Security Problem Definition 113
7.2.1 Assets and External Entities 113
7.2.2 Threats 113
7.2.3 Organisational Security Policies 113
7.2.4 Assumptions 113
7.3 Security Objectives 114
7.4 Security Requirements for Package Crypto Box 114
8 Package Contactless 123
8.1 TOE Overview 123
8.2 Security Problem Definition 123
8.2.1 Assets and External Entities 123
8.2.2 Threats 124
8.2.3 Organisational Security Policies 124
8.2.4 Assumptions 124
8.3 Security Objectives 124
8.4 Security Requirements for Package Contactless 125
8.5 Security Requirements rationale 134
9 Package PACE for Proximity Coupling Device 140
9.1 TOE Overview 140
9.2 Security Problem Definition 140
9.2.1 Assets and External Entities 140
9.2.2 Threats 141
9.2.3 Organisational Security Policies 141

9.2.4 Assumptions 141
9.3 Security Objectives 141
9.4 Security Requirements for Package PACE for Proximity Coupling Device 141
9.5 Security Requirements rationale 148
10 Package Logical Channel 152
10.1 TOE Overview 152
10.2 Security Problem Definition 152
10.2.1 Assets and External Entities 152
10.2.2 Threats 152
10.2.3 Organisational Security Policies 152
10.2.4 Assumptions 152
10.3 Security Objectives 153
10.4 Security Requirements for Package Logical Channel 153
10.5 Security Requirements rationale 156
11 Annex: Composite Evaluation of Smart Cards as Signature Products based on COS Smart Card Platforms (Informative) 159
11.1 Smart Cards as Secure Signature-creation Devices based COS (Informative) 159
11.1.1 eHC as SSCD 160
11.1.2 eHPC as SSCD 161
11.2 Smart Cards as Part of Signature-creation Application based on COS Smart Card Platforms (Informative) 166
11.2.1 gSMC-KT as part of Electronic Health Card Terminal 166
11.2.2 gSMC-K as part of the SCA of the Konnektor 167
12 Acronyms 168
13 Bibliography 170

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

2

Title:	Protection Profile 'Card Operating System Generation 2 (PP COS G2)'
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Editor(s):	T-Systems GEI GmbH
CC Version:	3.1 (Revision 4)
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 detail)
General Status:	final
Version Number:	1.9 as of 18th November 2014
Registration:	BSI-CC-PP-0082-V2
Keywords:	Gesundheitskarte, card operating system

1.2 TOE Overview

1.2.1 TOE definition and operational usage

3 The Target of Evaluation (TOE) addressed by the current protection profile is a smart card platform implementing the Card Operating System (COS) according [21] without any object system. The TOE shall comprise at least

i) the Security platform IC, 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],

iii) the wrapper for interpretation of exported TSF data,

iv) the associated guidance documentation.

4 The TOE includes all excutable code running on the Security platform IC, i. e. IC Dedicated Support Software, the Card Operating System, application specific code loaded on the smartcard by command LOAD CODE or any other means. The TSF of the TOE defined in a ST claiming conformance to this PP shall comprise all security functionality available after delivery of the TOE including vendor specific commands for initialization, personalization and operational usage allowed but not described in the specification of the COS [21]. This protection profile is written

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

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

based on COS specification [21] but also applicable to 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.

5 Note, if the TOE support 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.

6 The TOE does not include the object system, i. e. the application specific structures like the Master File (MF), the Applications, the Application Dedicated Files (ADF), the Dedicated Files (DF[3]), Elementary Files (EF) and internal security objects[4] including TSF data. The TOE and the application specific object system build an initialized smart card product like an electronic Health Card (eHC [22]), a Professional Health Card (eHPC [23]) or a Secure Module Card Type B (SMC-B [24]), K (SMC-K [25]) and KT (SMC-KT [26]).

1.2.2 TOE major security features for operational use

7 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

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

9 The export of non-confidential TSF data of the object systems supports verification of correct implementation of the object system of the smart card during manufacturing and test. The exported TSF data include all security attributes of the object system as a whole and of all objects but excludes any confidential authentication data. The wrapper provides communication interfaces between the COS and the verification tool (cf. [27]). 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 standardized format for export to the verification tool. The verification tool compares the response of the smart card with the object system definition. Details of the interface will be described in the BSI Technical Guidance TR-03143 „eHealth G2-COS Konsistenz-Prüftool“.

[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.

10 The typical life cycle phases for the current TOE type are IC and Smartcard embedded software development, manufacturing[5], smartcard product finishing[6], smartcard personalisation and, finally, smartcard end-usage as defined in [10]. The TOE should be delivered with completely installed COS. Any patches of the COS may be delivered to Smart Card Integrator for completion of COS installation. Any smartcard 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.

Operational use of the TOE is explicitly in the focus of current 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 current PP. A security evaluation /certification being conform with this PP will have to involve all life cycle phases into consideration to the extent as required by the assurance package chosen here for the TOE (see chap. 2.3 'Package Claim' below).

1.2.4 Non-TOE hardware/software/firmware

11 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 [43].

12 The specification [21] defines the options "Crypto Box", "Contactless", "PACE for Proximity Coupling Device", "Logical Channel", and "USB" which the TOE may implement. The PP takes account of these options in the following sections:

Option in [21]	Package	Remark
Option_Kryptobox	Crypto Box	Defines additional cryptographic SFR (see chapter 7).
Option_kontaktlose_ Schnittstelle	Contactless	Defines additional SFR for contactless interfaces of the smartcard, i.e. PICC part of PACE.
Option_PACE_PCD	PACE for Proximity Coupling Device	Defines additional SFR for support of contactless interfaces of the terminals, i.e. PCD part of PACE.
Option_logische_Kanäle	Logical Channel	Defines additional SFR for the support of logical channels (see chapter 9).
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 for the sake of completeness.

Table 1: Mapping between options and packages.

13 The Common Criteria for IT Security Evaluation, Version 3.1, Revision 4, defines a package as a set of SFR or SAR. This approach does not necessarily fit for description of extended TSF due to extended functionality of the TOE by means of packages. Therefore it was decided to provide an

[5] IC manufacturing, packaging and testing

[6] including installation of the object system

extension of the Security Problem Definition, the Security Objectives, and the Security Requirements as well as for the corresponding rationales for each defined package.

14 If the TOE implements one of these options the ST writer must integrate 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.

15 *Application note* 1*:* The ST writer must describe in the chapter Conformance Claim, section Package claim which package was chosen and in section Conformance Rationale how these package are integrated in the ST. Note the chosen packages may require support of commands or only special variants of the commands, cf. [21] for details.

16 *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 writer 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

17 This protection profile claims conformance to

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

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

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

as follows

- Part 2 extended,
- Part 3 conformant.

18 The

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

has to be taken into account.

2.2 PP Claim

19 This PP claims **strict** conformance to protection profile BSI-CC-PP-0035-2007 [11].

2.3 Package Claim

20 The current 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

21 This PP claims strict conformance to the BSI-CC-PP-0035-2007 [11].

22 From the Security Problem Definition (see section 3: “Security Problem Definition” [11]) of BSI-CC-PP-0035-2007 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-0035-2007. See section 3.2 and 3.3 for more details.

23 The assumptions A.Process-Sec-IC, A.Plat-Appl and A.Resp-Appl defined in the BSI-CC-PP-0035-2007 [11] address the operational environment of the Security IC, i.e. the COS part of the current TOE and the operational environment of the current TOE. The aspects of these assumptions are relevant for the COS part of the current TOE, address the development process of the COS and are evaluated according to composite evaluation approach [8]. Therefore these assumptions are now refined in order to address the assumptions about the operational environment of the current TOE (cf. chapter 3.4 for details).

24 The Security Objectives for the Security IC as defined in the BSI-CC-PP-0035-2007 O.Leak-Inherent, O.Phy-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced, O.Abuse-Func, O.Identification, O.RND are included as security objectives for the current TOE. Security Objectives for the Environment OE.Resp-Appl defined in the BSI-CC-PP-0035-2007 is split into the security objective O_Resp_Appl for the COS part of the TOE and OE.Resp-ObjS for the object system in the operational environment of the TOE. The security objective for the environment OE.Plat-Appl defined in the BSI-CC-PP-0035-2007 is ensured by the COS part of the TOE and verified in the composite evaluation process. It results in a similar security objective for the object system in the operational environment of the TOE OE.Plat-COS. OE.Process-Sec-IC defined in the BSI-CC-PP-0035-2007 is completely ensured by the assurance class ALC of the TOE up to Phase 5 and addressed by OE.Process-Card. See chapter 4 for more details.

25 All Security Functional Requirements with existing refinements are taken over from the BSI-CC-PP-0035-2007 into this PP by iterations indicated by "/SICP". Namely this are the following SFR: FRU_FLT.2/SICP, FPT_FLS.1/SICP, FMT_LIM.1/SICP, FMT_LIM.2/SICP, FAU_SAS.1/SICP, FPT_PHP.3/SICP, FDP_ITT.1/SICP, FPT_ITT.1/SICP, FDP_IFC.1/SICP, FCS_RNG.1/SCIP. See section 6.1 for more details.

26 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.

27 The refinements of the Security Assurance Requirements made in BSI-CC-PP-0035-2007 are taken over in this Protection Profile and must be applied to the Security platform IC.

28 As all important parts of the BSI-CC-PP-0035-2007 are referred in a way that these are part of this Protection Profile the rationales still hold. Please refer sections 4.3 and 6.3 for further details.

29 Therefore the strict conformance with the BSI-CC-PP-0035-2007 [11] is fulfilled by this Protection Profile.

30 Note: the BSI-CC-PP-0035-2007 [11] was updated by BSI-CC-PP-0084 [48]. The TOE may include Security platform IC certified conformant to BSI-CC-PP-0084 [48] if the transition guide [47] is taken into account and the ST provides appropriate rationale.

2.5 Conformance statement

31 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

32 As defined in section 1.2.1 the TOE is a smart card platform implementing the Card Operating System (COS) according [21] without any object system. In sense of the BSI-CC-PP-0035-2007 [11] the COS is User Data and Security IC Embedded Software.

33 In section 3.1 “Description of Assets” in the BSI-CC-PP-0035-2007 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.

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

- the User Data defined in the BSI-CC-PP-0035-2007 are User data or TSF Data in the context of the current PP,
- Security IC Embedded Software is part of the current TOE,
- the security services provided by the TOE for the Security IC Embedded Software are part of the current TSF and
- the random numbers produced by the IC platform are internally used by the TSF.

35 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

36 Note: elementary files (EF) may be stored in the MF, any DF, Application or Application Dedicated File. The place of an EF in the file hierarchy defines features of the User Data stored in the EF. User data does not affect the operation of the TSF (cf. CC part 1, para. 100). Cryptographic keys used by the TSF to verify authentication attempts of external entities (i.e. authentication reference data) including the verification of Card Verifiable Certificates (CVC) or

authenticate itself to external entities by generation of authentication verification data in a cryptographic protocol are TSF data (cf. Tables 13, 14 and 17)

37 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

38 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.

39 The following threats are defined in the BSI-CC-PP-0035-2007 [11]: T.Leak-Inherent, T.Phys-Probing, T.Malfunction, T.Phys-Manipulation, T.Leak-Forced, T.Abuse-Func, T.RND. All threats are part of this Protection Profile and taken over into this PP. Please refer BSI-CC-PP-0035-2007 for further descriptions and the details. Table 4 lists all threats taken over with the corresponding reference.

Threat name	Reference to paragraph in [11]	Short description
T.Leak-Inherent	78	Inherent Information Leakage
T.Phys-Probing	79	Physical Probing
T.Malfunction	80	Malfunction due to Environmental Stress
T.Phys-Manipulation	81	Physical Manipulation
T.Leak-Forced	82	Forced Information Leakage
T.Abuse-Func	83	Abuse of Functionality
T.RND	84	Deficiency of Random Numbers

Table 4: Overview of threats defined in BSI-CC-PP-0035-2007 [11] and taken over into this PP.

40 The TOE shall avert the threat "Forge of User or TSF data (T.Forge_Internal_Data)" as specified below.

[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 current security policy, whereby an attacker might 'capture' any subject role recognised by the TOE.

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.

41 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.

42 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 authorization. This threat comprises several attack scenarios e.g. the attacker may try circumvent the user authentication to use signing functionality without authorization. The attacker may try to alter the TSF data e.g. to extend the user rights after successful authentication.

43 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.

44 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.

45 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.

46 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

47 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.

48 The following OSP is defined in the BSI-CC-PP-0035-2007 [11]. That OSP is part of this Protection Profile and is taken over into this PP for the current TOE. Note the current PP includes the embedded software which is not a part of TOE defined in the BSI-CC-PP-0035-2007 [11]. Please refer BSI-CC-PP-0035-2007 for further descriptions and the details. Table 5 lists all OSP taken over with the corresponding reference.

OSP name	Short description	Reference to paragraph in [11]
P.Process-TOE	Protection during TOE Development and Production	86

Table 5: Overview of OSP defined in BSI-CC-PP-0035-2007 [11] and taken over into this PP.

3.4 Assumptions

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

50 The assumptions defined in the BSI-CC-PP-0035-2007 [11] address the operational environment of the Security IC, i.e. the COS part of the current TOE and the operational environment of the current TOE. The aspects of these assumptions, which are relevant for the COS part of the current TOE, address the development process of the current TOE and are evaluated according to composite evaluation approach [8]. Therefore these assumptions are now refined in order to address the assumptions about the operational environment of the current TOE. The Table 6 lists and maps these assumptions for the operational environment with the corresponding reference.

Assumptions defined in [11]	Reference to paragraph in [11]	Refined assumptions for the operational environment of the current TOE	Rationale of the changes
A.Process-Sec-IC	91	A.Process-Sec-SC	While the TOE of BSI-CC-PP-0035-2007 is delivered after Phase 3 IC manufactioring and Testing or Phase or Phase 4 IC Packaging the current TOE is delivered after Phase 5 Composite Product Integration before Phase 6 Personalisation. The protection during Phase 4 may and during Phase 5 shall be addressed by security of the development environment of the current TOE. Only protection during Personalisation is in responsibility of the operational environment.
A.Plat-Appl	93	removed	Usage of Hardware Platform as TOE of BSI-CC-PP-0035-2007 as addressed by A.Plat-Appl is covered by ADV class related to COS as part of the current TOE.
A.Resp-Appl	95	A.Resp-ObjS	The user data of the TOE of BSI-CC-PP-0035-2007 are the Security IC Embedded Software, i.e. the COS part of the TOE, the TSF data of the current TOE and the user data of the COS. The object system contains the TSF data and defines the security attributes of the user data of the current TOE.

Table 6: Overview of assumptions defined in BSI-CC-PP-0035-2007 [11] and implemented by the TOE.

51 The developer of applications for COS must ensure the appropriate “A.Process-Sec-SC (Protection during Personalisation)” after delivery of the TOE.

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

52 The developer of applications for 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, and the application notes, and (ii) findings of the TOE evaluation reports relevant for the COS as documented in the certification report.

53 The developer of applications for COS must ensure the appropriate “Treatment of User Data by the Object System (A.Resp-ObjS)” while developing the application.

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

4 Security Objectives

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

4.1 Security Objectives for the TOE

55 The following TOE security objectives address the protection provided by the TOE.

56 The following Security Objectives for the TOE are defined in the BSI-CC-PP-0035-2007 [11]. The Security Objectives for the TOE are part of this Protection Profile and are taken over into this PP. Please refer BSI-CC-PP-0035-2007 for further descriptions and the details. Table 6 lists all Security Objectives taken over with the corresponding reference.

Security Objectives name	Short description	Reference to paragraph in [11]
O.Leak-Inherent	Protection against Inherent Information Leakage	100
O.Phy-Probing	Protection against Physical Probing	101
O.Malfunction	Protection against Malfunctions	102
O.Phys-Manipulation	Protection against Physical Manipulation	103
O.Leak-Forced	Protection against Forced Information Leakage	104
O.Abuse-Func	Protection against Abuse of Functionality	105
O.Identification	TOE Identification	106
O.RND	Random Numbers	107

Table 7: Overview of Security Objectives for the TOE defined in BSI-CC-PP-0035-2007 [11] and taken over into this PP.

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

58 The TOE shall provide “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.

59 The TOE shall provide “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.

60 The TOE shall provide a “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.

61 The TOE shall provide “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.

62 The TOE shall provide “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.

63 The TOE shall provide “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.

64 The TOE shall provide “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.

65 The TOE shall provide “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.

66 The TOE shall provide a “Secure messaging (O.SecureMessaging)” as specified below.

O.SecureMessaging **Secure messaging**

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

4.2 Security Objectives for Operational Environment

67 This section describes the security objectives for the operational environment enforced by the Security IC Embedded Software.

68 The following security objectives for the operational environment of the security IC are defined in the BSI-CC-PP-0035-2007 [11]. The operational environment of the Security IC as TOE in the BSI-CC-PP-0035-2007 comprises the COS part of the current TOE and the operational environment of the current TOE. Therefore these security objectives of the operational environment are split and refined. The aspects relevant for the COS part of the current TOE shall be fulfilled in the development process of the COS and evaluated according to composite evaluation approach [8]. The remaining aspects of the security objectives for the operational environment defined in the BSI-CC-PP-0035-2007 are addressed in new security objectives for the operational environment of the current PP. The table 8 lists and maps these security objectives for the operational environment with the corresponding reference.

Security Objectives for the operational environment defined in [11]	Reference to paragraph in [11]	Refined security objectives for the operational environment of the current TOE	Rationale of the changes
OE.Plat-Appl	109	removed	OE.Plat-Appl requires the Security IC Embedded Software to meet the guidance documents of the Security IC. The Security IC Embedded Software is part of the current TOE. This requirement shall be fulfilled in the development process of the TOE.
OE.Resp-Appl	110	OE.Resp-ObjS	OE.Resp-Appl requires the Security IC Embedded Software to treat the user data as required by the security needs of the specific application context. This objective shall be ensured by the TOE and the object system.

Security Objectives for the operational environment defined in [11]	Reference to paragraph in [11]	Refined security objectives for the operational environment of the current TOE	Rationale of the changes
OE.Process-Sec-IC	111	OE.Process-Card	The policy defined for the Security platform IC is extended to the current TOE.

Table 8: Overview of Security Objectives for the Operational Environment defined in BSI-CC-PP-0035-2007 [11] and taken over into this PP.

69 The Security IC Embedded Software shall provide "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) user guidance of the COS, (ii) application notes for the COS (iii) other guidance documents, and (iv) findings of the TOE evaluation reports relevant for applications developed for COS as referenced in the certification report.

70 The Security IC Embedded Software shall provide "Treatment of User Data (OE.Resp-ObjS)" as specified below

OE.Resp-ObjS **Treatment of User Data**

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

71 The operational environment of the TOE shall provide "Protection of Smartcard during Personalisation (OE.Process-Card)" as specified below

OE.Process-Card **Protection of Smartcard during Personalisation**

Security procedures shall be used after delivery of the TOE during Phase 6 Smartcard personalisation up to the delivery of the smartcard to the end-user in order to maintain confidentiality and integrity of the TOE and to prevent any theft, unauthorised personalization or unauthorised use.

4.3 Security Objective Rationale

72 Table 1 in BSI-CC-PP-0035-2007 [11] Section 4.4 "Security Objectives Rationale" gives an overview, how the assumptions, threats, and organisational security policies taken over are addressed by the objectives. Please refer that table and the text following after that table justifying this in detail for the further details.

73 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 are addressing the security

problem definition as given in the BSI-CC-PP-0035-2007 and the additional threats, organisational policies and assumptions defined in the current PP. It shows that all threats and OSPs are addressed by the security objectives for the TOE and for the TOE environment. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

	(SAR ALC for IC part of the TOE)	OE.Process-Sec-Card	(SAR ADV class for COS part of the TOE)	(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	(X)	(X)											
A.Process-Sec-SC		X											
A.Plat-Appl			(X)										
A.Resp-Appl				(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

74 The **A.Process-Sec-IC** assumes and **OE. Process-Sec-IC** requires that security procedures are used after delivery of the IC by the IC Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). Development and production of the Security IC is part of development and production of the TOE because it includes the Security IC. The **A.Process-Sec-SC** assumes and **OE.Process-Sec-Card** requires security procedures during Phase 6 Smartcard personalisation up to the delivery of the smartcard to the end-user. More precisely, the smartcard life cycle according to [10] (cf. also to BSI-CC-PP-0035-2007) are covered as follows.

- IC development (Phase 2) and IC manufacturing and testing (Phase3) are covered as development and manufacturing of the security ICand therefore of the TOE as well.

- IC packaging and testing (Phase 3) may be part of the development and manufacturing environment or the operational environment of the security IC. Even if it is part of the operational environment of the Security IC addressed by OE. Process-Sec-IC it will be part of the development and manufacturing environment of the current TOE and covered by the SAR ALC_DVS.2.

- IC packaging and testing (Phase 4) and Smartcard Packaging and finishing process (Phase 5) are addressed by OE. Process-Sec-IC but they are part of the development and manufacturing environment of the current TOE and covered by the SAR ALC_DVS.2.

- Snartcard personalisation (Phase 6) up to the delivery of the smartcard to the end-user is addressed by A.Process-Sec-IC and A.Process-Sec-SC and covered by OE.Process-Sec-Card.

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

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

77 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-0035-2007. As stated in section 2.4, this PP claims conformance to BSI-CC-PP-0035-2007 [11]. The objectives, assumptions, policies and threats as used in Table 9 are defined and handled in [11]. Hence, the rationale for these items and their correlation with Table 9 is given in [11] and not repeated here.

78 The current PP defines new threats and assumptions for the TOE extended to the the Security platform IC as TOE defined in BSI-CC-PP-0035-2007 and extends the policy P.Process-TOE to the current 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.Malicious_Application				X	X	X						
T.Misuse					X	X						
T.Crypto								X				
T.Intercept									X			
T.WrongRights			X									
A.Plat-COS										X		
A.Resp-ObjS											X	
P.Process-TOE												X

Table 10: Security Objective Rationale for the COS part of the TOE

79 A detailed justification required for *suitability* of the security objectives to coup with the security problem definition is given below.

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

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

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

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

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

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

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

87 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.

88 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.

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

5 Extended Components Definition

90 This protection profile uses components defined as extensions to Common Criteria part 2 [3]. The following extensions are taken from BSI-CC-PP-0035-2007 [11] chapter 5 "Extended Components Definition" and are part of this Protection Profile:

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

The Definition of the Family FCS_RNG already defined in BSI-CC-PP-0035-2007 is updated according to [6] and [7] by refinement of selection "hybrid" to "hybrid physical" and "hybrid deterministic". The families FIA_API, FPT_EMS and FPT_ITE are defined in the document on hand.

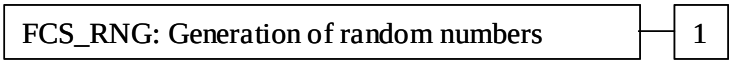
5.1 Definition of the Family FCS_RNG Generation of Random Numbers

91 This section describes the functional requirements for the generation of random numbers, which may be used as secrets for cryptographic purposes or authentication. The IT security functional requirements for a TOE are defined in an additional family (FCS_RNG) of the Class FCS (Cryptographic support).

Family Behaviour

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

Component levelling:



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

Management: There are no management activities foreseen.

Audit: There are no actions defined to be auditable

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

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

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

94 Note, this definition of FCS_RNG family is identical to the definition given in BSI-CC-PP-0035 but introduce additional RNG classes "hybrid physical" RNG and "hybrid deterministic" RNG according to [7].

5.2 Definition of the Family FIA_API

95 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.

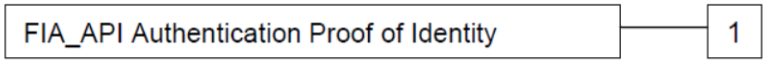
96 *Application note* 3: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the extended family FIA_API from point of view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

97 FIA_API Authentication Proof of Identity

Family Behaviour

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

Component levelling:



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

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

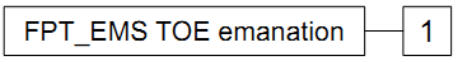
5.3 Definition of the Family FPT_EMS TOE Emanation

98 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].

Family Behaviour

99 This family defines requirements to mitigate intelligible emanations.

Component levelling:



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

Management:	There are no management activities foreseen.
Audit:	There are no actions defined to be auditable
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

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*].

5.4 Definition of the Family FPT_ITE TSF image export

Family Behaviour

101 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 export of TOE implementation fingerprints and of TSF data in order to allow verification of the correct implementation of the IC Dedicated Software and the COS of the TOE and the TSF data of the smartcard. The export of a fingerprint of the TOE implementation, e.g. a keyed hash value over all implemented executable code, provides the ability to compare the implemented executable code with the known intended executable code. The export of all non-confidential TSF data, e.g. data security attributes of subjects and objects and public authentication verification data like public keys, provides the ability to verify their correctness e.g. against a object system specification. The exported data must be correct, but do not need protection of confidentiality or integrity if the export is performed in a protected environment. This family describes the functional requirements for unprotected export of TSF data and export of TOE implementation fingerprints not being addressed by any other component of CC part 2 [2].

Component levelling:

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

103 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

104 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.

105 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.

106 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.

107 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*.[9]

108 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*.

109 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.

110 Some SFRs (including the potential exiting refinement) were taken over from the BSI-CC-PP-0035-2007. A list of all SFRs taken from BSI-CC-PP-0035-2007 [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

111 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.

[9] 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

112 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 security functional groups and allocated the functional requirements described in the following sections to them:

Security Functional Groups	Security Functional Requirements concerned
Protection against Malfunction	FRU_FLT.2/SICP, FPT_FLS.1/SICP
Protection against Abuse of Functionality	FMT_LIM.1/SICP, FMT_LIM.2/SICP, FAU_SAS.1/SICP
Protection against Physical Manipulation and Probing	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 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 159)	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.3TDES, FCS_COP.1/COS.RMAC, FCS_CKM.1/3TDES_SM, FCS_COP.1/COS.AES, FCS_CKM.1/AES.SM, FCS_CKM.1/RSA, FCS_CKM.1/ELC, FCS_COP.1/COS.CMAC, FCS_COP.1/COS.RSA.S, FCS_COP.1/COS.RSA.V, FCS_COP.1/COS.ECDSA.S, FCS_COP.1/COS.RSA, FCS_COP.1/COS.ELC, FCS_CKM.4
Protection of communication (section 6.1.8)	FTP_ITC.1/TC

Table 12: Security functional groups vs. SFRs

113 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

TSF Data	Definition
	TOE and to keep track of the Security IC'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

114 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 status to specific objects and makes password management easier by using the same secret for different roles. The security attributes *interfaceDependentAccessRules, startRetryCounter, retryCounter, minimumLength* and *maximumLength* are defined for the *secret*. The PUC defined for the *secret* is intended for password management and the authorization gained by successful authentication is limited to the command RESET RETRY COUNTER for reset of the *retryCounter* and setting a new *secret.*

115 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* *startRetryCounterf* *retryCounter* *minimumLength* *maximumLength*	The following command is used by the TOE to authenticate the human user and to reset the security attribute *retryCounter* by PIN: VERIFY. The following command is used by the TOE to manage the authentication reference data *secret* and the security attribute *retryCounter* with authentication of the human user by PIN: CHANGE REFERENCE DATA (P1='00'). The following commands are used by the TOE to manage the authentication reference data *secret* without authentication of the human user CHANGE REFERENCE DATA (P1='01') and RESET RETRY COUNTER (P1='02'). The following command is used by the TOE to manage the security attribute

User type	Authentication reference data and security attributes	Comments
		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[10], *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

116 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 authorization (*CHA*) in case of RSA-based CVC or the card holder authorization 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

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

for this device get the role of the *CHA* 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*[11] 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[12] *persistentCache, applicationPublicKeyList*[13] Security attributes of the user *Certificate Holder Reference* (*CHR*) *lifeCycleStatus,* *interfaceDependentAccessRules,* *Certificate Holder Authorization* (*CHA*) for RSA keys or *Certificate Holder Authorization Template (CHAT)* for elliptic curve keys Security attributes in the *certificate* *Certificate Profile Identifier (CPI)* *Certification Authority Reference (CAR)* *Object Identifier (OID)*	The following command is used by the TOE to authenticate a device EXTERNAL AUTHENTICATE with *algID* equal to *rsaRoleCheck* or *elcRoleCheck* The following commands are used by the TOE to manage the authentication reference data PSO VERIFY CERTIFICATE, ACTIVATE, DEACTIVATE, DELETE and TERMINATE.
Device	**Secure messaging channel key**	The TOE authenticates the sender of a

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

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

[13] The command PSO VERIFY CERTIFICATE may store the successful verified public key temporarily in the *volatileCache* or persistenly in the *applicationPublicKeyList* or the *persitentCache*. 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 *persitentCache*.

User type	Authentication reference data and security attributes	Comments
	Authentication reference data MAC session key SK4SM Security attributes of SK4SM *flagSessionEnabled* equal SK4SM, *Kmac* and *SSCmac*, *negotiationKeyInformation*.	received command using secure messaging.

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

117 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*, *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

118 The COS specification associates a subject with a *logical channel* and its *channelContext* (cf. [21], chapter 12). The TOE may support one subject respective logical channel or more than one independent subjects respective logical channels, cf. 9 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*)[14]. If the TOE does not support contactless communication the TOE shall behave as *interfaceDependentAccess*

[14] Note the COS specification [21] describes this security attribute in the context of access control rules in chapter 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”.

Security attribute	Elements	Comments
		Rules is permanently set to "*kontaktbehaftet*".
currentFolder		Identifier of the (unique) current folder
	seIdentifier	Security environment selected by means of command MANAGE SECURITY ENVIRONMENT[15]. 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 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 commands INTERNAL AUTHENTICATE.
	verifyCertificate	*keyReference* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for PSO VERIFY CERTIFICATE.
	signatureCreation	*keyReference* and *algorithmIdentifier* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for PSO COMPUTE DIGITAL SIGNATURE.
	dataDecipher	*keyReference* and *algorithmIdentifier* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for PSO DECIPHER or PSO TRANSCIPHER.
	dataEncipher	*keyReference* and *algorithmIdentifier* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for PSO ENCIPHER.
	macCalculation	*keyReference* and *algorithmIdentifier* of the key selected by means of the command MANAGE SECURITY ENVIRONMENT to be used for PSO COMPUTE CRYPTOGRAPHIC CHECKSUM and PSO VERIFY CRYPTOGRAPHIC CHECKSUM if package Crypto Box is supported.
SessionkeyContext		This list contains security attributes associated with secure messaging and trusted channels.
	flagSessionEnabled	Value *noSK* indicates no session key established.

[15] Note the COS specification [21] describes this security attribute in the informative chapter 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
		Value *SK4SM* indicates session keys established for receiving commands and sending responses. Value *SK4TC* indicates session keys established for PSO ENCIPHER, PSO DECIPHER and PSO COMPUTE CRYPTOGRAPHIC CHECKSUM, PSO VERIFY CRYPTOGRAPHIC CHECKSUM if package Crypto Box is supported.
	encKey and *SSCenc*	Key for encryption and decryption and its sequence counter.
	macKey and *SSCmac*	Key for MAC calculation and verification and its sequence counter.
	flagCmdEnc and *flagRspEnc*	Flags indicating encryption of data in commands respective responses.
	negotiationKeyInformation	*keyIdentifier* of the key used to generate the session keys and if asymmetric key was used the *accessRigth* associated with this key. The *keyIdentifier* may reference to the authentication reference data used for PACE[16] if PACE is supported by the TOE.
	accessRulesSession-keys	Access control rules associated with trusted channel support.
globalPasswordList	(*pwReference*, *securityStatusEvaluationCounter*)	List of 0, 1, 2, 3 or 4 elements containing results of successful human user authentication with password in MF: *pwReference* and *securityStatusEvaluationCounter*.
dfSpecificPasswordList	(*pwReference*, *securityStatusEvaluationCounter*)	List of 0, 1, 2, 3 or 4 elements containing results of successful human user authentication with password for each DF: *pwReference* and *securityStatusEvaluationCounter*.
globalSecurityList	*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 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* *CHA* as reference to the role gained by authentication based on certificate or *keyIdentifier* as reference to symmetric authentication key or *keyIdentifier* generated by

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

Security attribute	Elements	Comments
		successful authentication with PACE protocol if PACE is supported by the TOE.
bitSecurityList		List of CHAT gained by successful authentication with CVC based on ECC. The effective access rights are the intersection of access rights defined in CVC of the CVC chain up to the root.
Current file		Identifier of the (unique) current file from *currentFolder.children.*
securityStatusEvaluationCounter	*startSsec*	Must contain all values of *startSsec* and may be *empty.*

Table 17: Security attributes of a subject

119 The following tables provide an overview of the objects, operations and security attributes defined in the current 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*[17] *interfaceDependentAccessRules* *children*	SELECT ACTIVATE DEACTIVATE DELETE FINGERPRINT GET RANDOM[18] LOAD APPLICATION TERMINATE DF
Dedicated File (8.3.1.2)	Additionally to Folder: *fileIdentifier*	Identical to Folder
Application (8.3.1.1)	Additionally to Folder: *applicationIdentifier*	Identical to Folder
Application Dedicated File (8.3.1.3)	Additionally to Folder: *fileIdentifier* *applicationIdentifier* *children*	Identical to Folder
Elementary File (8.3.2)	*fileIdentifier* *list of shortFileIdentifier* *lifeCycleStatus* *shareable*[19] *accessRules:*	SELECT ACTIVATE DEACTIVATE DELETE TERMINATE

[17] Available with package logical channel

[18] Only available with package logical channel

[19] Available with package logical channel

Object type	Security attributes	Operations
	interfaceDependentAccessRules *flagTransactionMode* *flagChecksum*	
Transparent EF (8.3.2.1)	Additionally to Elementary File: *numberOfOctet* *positionLogicalEndOfFile* *body*	Additionally to Elementary File: ERASE BINARY READ BINARY UPDATE BINARY WRITE BINARY
Structured EF (8.3.2.2)	Additionally to Elementary File: *recordList* *maximumNumberOfRecords* *maximumRecordLength* *flagRecordLifeCycleStatus*	Additionally to Elementary File: ACTIVATE RECORD APPEND RECORD DELETE RECORD DEACTIVATE RECORD ERASE RECORD READ RECORD SEARCH RECORD SET LOGICAL EOF UPDATE RECORD
Regular Password (8.4) (PIN)	*lifeCycleStatus* *pwdIdentifier* *accessRules:* *interfaceDependentAccessRules* *secret: PIN* *minimumLength* *maximumLength* *startRetryCounter* *retryCounter* *transportStatus* *flagEnabled* *startSsecList* *PUC* *pukUsage* channel specific: *securityStatusEvaluationCounter*	ACTIVATE DEACTIVATE DELETE TERMINATE CHANGE REFERENCE DATA DISABLE VERIFICATION REQUIREMENT ENABLE VERIFICATION REQUIREMENT GET PIN STATUS RESET RETRY COUNTER VERIFY
Multi-reference Password (8.5) (MR-PIN)	*lifeCycleStatus* *pwdIdentifier* *accessRules:* *interfaceDependentAccessRules* *startSsecList* *flagEnabled* *passwordReference* Attributes used together with *referred password (PIN):* *secret: PIN* *minimumLength* *maximumLength* *startRetryCounter* *retryCounter*	Identical to Regular Password

Object type	Security attributes	Operations
	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 (8.6.4.2)	Additionally to Public Asymmetric Key: *publicRsaKey: oid* or *publicElcKey: oid* *CHAT* *expirationDate: date*	Additionally to Public Asymmetric Key: PSO VERIFY CERTIFICATE, PSO VERIFY DIGITAL SIGNATURE
Public Asymmetric Key	*publicRsaKey: oid* or *publicElcKey:*	Additionally to Public

Object type	Security attributes	Operations
for Authentication (8.6.4.3)	*oid* *CHA* *CHAT* *expirationDate: date*	Asymmetric Key: EXTERNAL AUTHENTICATE GENERAL AUTHENTICATE INTERNAL AUTHENTICATE
Public Asymmetric Key for Encryption (8.6.4.4)	Additionally to Public Asymmetric Key: *publicRsaKey: oid* *publicElcKey: oid*	Additionally to Public Asymmetric Key: PSO ENCIPHER
Card verifiable certificate (CVC) (7.1.1)	Certificate Profile Identifier (CPI) Certification Authority Reference (CAR) Certificate Holder Reference (CHR) Certificate Holder Autorisation (CHA) Object Identifier (OID) signature	

Table 18: Subjects, objects, operations and security attributes. The references refer to [21].

120 The TOE must support Access control lists for

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

and may support Access control lists for

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

121 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.

122 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.[20]

123 The TOE access control rule contains

- command defined by CLA, 0 or 1 parameter P1, and 0 or 1 parameter P2,

[20] 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.

- 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*), *AUT*(*CHAT*) and secure messaging conditions (cf. [21], chapter 10.2 for details).

Note 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.

124 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.

125 The following table gives an overview of the commands the COS has to implement and the related SFR. Please note that commands or special variants of commands may be required only if a specific package is supported by the TOE. The SFR defined in the main part of the PP are mandatory and printed in normal style. SFR 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 SFR in this PP.

Operation	SFR	Chapter
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, FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3, FMT_SMF.1, FMT_MSA.1/Life, FCS_CKM.4, *FIA_USB.1/LC*	14.2.4
DELETE RECORD	FDP_ACC.1/SEF, FDP_ACF.1/SEF, FMT_MSA.1/SEF	14.4.4
DISABLE VERIFICATION REQUIREMENT	FMT_SMF.1, FMT_MSA.1/PIN, FIA_AFL.1/PIN, FIA_USB.1	14.6.2
ENABLE VERIFICATION REQUIREMENT	FMT_SMF.1, FMT_MSA.1/PIN, FIA_AFL.1/PIN, FIA_USB.1	14.6.3
ENVELOPE	This command is optional and therefore not addressed in the SFRs of this PP.	14.9.1

Operation	SFR	Chapter
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.RSA.V, FCS_COP.1/COS.ECDSA.V, *FCS_COP.1/CB.3TDES, FCS_COP.1/CB.RMAC, FCS_COP.1/CB.AES, FCS_COP.1/CB.CMAC*	14.7.1
FINGERPRINT	FPT_ITE.1, FDP_ACF.1/MF_DF	14.9.2
GENERAL AUTHENTICATE	FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_API.1, FIA_USB.1, FCS_RNG.1, FCS_COP.1/COS.AES, FCS_CKM.1/AES.SM, *FIA_UAU.5/PACE, FIA_UAU.6/*PACE, *FIA_USB.1/PACE*	14.7.2
GENERATE ASYMMETRIC KEY PAIR	FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3, FMT_SMF.1, FCS_CKM.1/RSA, FCS_CKM.1/ELC	14.9.3
GET CHALLENGE	FCS_RNG.1	14.9.4
GET DATA	This command is 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[21]	*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, FCS_COP.1/COS.RSA.S, FCS_COP.1/COS.ECDSA.S, *FCS_COP.1/CB.3TDES, FCS_COP.1/CB.RMAC, FCS_COP.1/CB.AES, FCS_COP.1/CB.CMAC*	14.7.4
LOAD APPLICATION	FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF, FMT_SMF.1, FMT_MSA.1/Life	14.2.5
LIST PUBLIC KEY	FPT_ITE.2, FDP_ACC.1/MF_DF, FDP_ACF.1/MF_DF	14.9.7
MANAGE CHANNEL	FIA_UID.1, FIA_UAU.1, *FIA_USB.1/LC,* FMT_MSA.3	14.9.8
MANAGE SECURITY ENVIRONMENT	FIA_USB.1, FDP_ACC.1/KEY, FDP_ACF.1/KEY, FMT_MSA.3	14.9.9
MUTUAL AUTHENTICATE	FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_API.1, FIA_USB.1, FCS_RNG.1, FCS_CKM.1/AES.SM, *FCS_COP.1/CB.3TDES, FCS_COP.1/CB.RMAC, FCS_COP.1/CB.AES, FCS_COP.1/CB.CMAC*	14.7.1

[21] If package Logical Channel is supported

Operation	SFR	Chapter
PSO COMPUTE CRYPTOGRAPHIC CHECKSUM[22]	FDP_ACC.1/KEY, FDP_ACF.1/KEY, *FIA_API.1/CB*, *FCS_COP.1/CB.RMAC*, *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.3TDES*, *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.3TDES*, *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, FCS_COP.1/COS.ELC	14.8.6.3
PSO VERIFY CERTIFICATE	FMT_SMF.1, FMT_MTD.1/Auth, FCS_COP.1/COS.RSA.V, FCS_COP.1/COS.ECDSA.V, FDP_ACC.1/KEY, FDP_ACF.1/KEY	14.8.7
PSO VERIFY CRYPTOGRAPHIC CHECKSUM[23]	FDP_ACC.1/KEY, FDP_ACF.1/KEY, *FIA_USB.1/CB*, *FCS_COP.1/CB.RMAC* *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,	14.6.5

[22] if package Crypto Box is supported

[23] if package Crypto Box is supported

Operation	SFR	Chapter
	FMT_MTD.1/PIN, FMT_MSA.1/PIN	
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 SFR

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

127 *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.

128 *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-0035-2007

129 All SFRs from section 6.1 ”Security Functional Requirements for the TOE” of the BSI-CC-PP-0035-2007 are part of this PP. On all SFR of the BSI-CC-PP-0035-2007 an iteration operation is performed. For the iteration operation the suffix “/SICP” is added to the SFR name from BSI-CC-PP-0035-2007.

130 The complete list of the SFRs taken over from BSI-CC-PP-0035-2007 follows. For further descriptions, details, and interpretations refer section 6.1 in BSI-CC-PP-0035-2007 [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 capabilities
- FAU_SAS.1/SICP: Audit storage
- 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

131 Table 20 maps the SFR name in this PP to the SFR name in BSI-CC-PP-0035-2007 [11]. This approach allows an easy and unambiguous identification which SFR was taken over from the BSI-CC-PP-0035-2007 into this Protection Profile and which SFR is defined newly in this PP.

SFR name	SFR name in [11]	Reference to paragraph in [11]
FRU_FLT.2/SICP	FRU_FLT.2	140
FPT_FLS.1/SICP	FPT_FLS.1	141
FMT_LIM.1/SICP	FMT_LIM.1	150
FMT_LIM.2/SICP	FMT_LIM.2	151
FAU_SAS.1/SICP	FAU_SAS.1	152
FPT_PHP.3/SICP	FPT_PHP.3	156
FDP_ITT.1/SICP	FDP_ITT.1	159
FPT_ITT.1/SICP	FPT_ITT.1	160
FDP_IFC.1/SICP	FDP_IFC.1	161
FCS_RNG.1/SICP	FCS_RNG.1	164

Table 20: Mapping between SFR names in this PP and the SFR names in the BSI-CC-PP-0035-2007 [11]

132 In some cases security functional components have been added or refined. Please refer section for details. The refinements of the security functional are only being applied for the SFR for the TOE taken over from BSI-CC-PP-0035-2007 [11] (see Table 20).

6.1.4 General Protection of User data and TSF data

133 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*][24].

134 *Application note 7:* The writer of the Security Target may want to use iterations of FDP_RIP.1 in order to distinguish between data, which must be deleted already upon deallocation and those which can be deleted upon allocation. It is recommended to delete secret/private cryptographic keys and all passwords upon deallocation. For secret user data deletion upon allocation should be sufficient (depending on the resistance of the concrete TOE against physical attacks). 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".

135 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*][25].

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

136 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[26].

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

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

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

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

FPT_EMS.1	Emanation of TSF and User data
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit [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*][27] and the following user data (8) Private asymmetric keys, (9) Symmetric keys, (10) [assignment: *list of additional types of user data*][28].
FPT_EMS.1.2	The TSF shall ensure any user[29] are unable to use the following interface circuit interfaces[30] 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*][31] and the following user data (8) Private asymmetric keys, (9) Symmetric keys, (10) [assignment: *list of additional types of user data*][32].

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

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

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

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

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

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

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

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)[33] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use [21], chapter 7 "CV-Certificate" and [21], appendix H "CV-Certificate for ELC-keys"[34] when interpreting the TSF data from another trusted IT product.

139 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][35].
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: AES128, AES-192, AES-256] with cryptographic key size [selection: 128, 192, 256] bit that meet the following standard FIPS180-4 [37],NIST SP800-38B [36]*[36] for the exported data.

140 *Application note 8*: The command FINGERPRINT calculates a hash value or CMAC based fingerprint over the complete executable code actually implemented by the TOE. The TOE implementation includes IC Dedicated Support Software, the Card Operating System and application specific code loaded on the smartcard by command LOAD CODE or any other means. The hash function respective the CMAC based calculation uses the prefix send in the command FINGERPRINT for "fresh" fingerprints over all executable code, i.e. no precomputed values over fixed parts of the code only.

141 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.

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

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

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

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

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]*][37]

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[38].

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

142 *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 and guidance documentation) must support the user to find **all** objects and to export **all** security attributes of these objects. Note while MF, DF and EF are hierarchically structured the Application and Application Dedicated File are directly referenced which may require special methods to find all objects in the object system. Note the *listOfApplication* as security attribute of the object system contains at least one *applicationIdentifier* of each Application or Application Dedicated File (cf. [27]). The exported data shall be encoded by wrapper to allow interpretation of the TSF data. The encoding rules shall meet the requirements of the Technical Guidance TR-03143 describing the verification tool used for examination of the object system against the specification of the object system.

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

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

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

FPT_TST.1	TSF testing
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up[39] to demonstrate the correct operation of the TSF[40].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[41].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of TSF[42].

6.1.5 Authentication

144 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*[43].

145 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[44] 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[45].

[39] [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]*]

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

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

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

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

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

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

FIA_AFL.1.2/PIN	When the defined number of unsuccessful authentication attempts has been met[46], the TSF shall block the password for authentication until successful unblock using command RESET RETRY COUNTER (1) P1='00' or P1='01' with presenting unblocking code PUC of this password object, (2) P1='02' or P1='03' without presenting unblocking code PUC of this password object [47].

146 *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.

147 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[48] ~~unsuccessful~~[49] authentication attempts occur related to usage of a password unblocking code using the RESET RETRY COUNTER command[50].
FIA_AFL.1.2/PUC	When the defined number of ~~unsuccessful~~[51] authentication attempts has been met[52], the TSF shall [assignment: *list of actions, which at least includes: block the password unblocking code*][53].

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

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

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

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

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

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

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

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

148 *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.

149 *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.

150 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. 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[54].

151 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*][55] 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

54 [assignment: *list of security attributes*]

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

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

152 *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 than the TOE shall allow the access for anybody (ALWAYS) and the ST author shall list the command in the element FIA_UAU.1.1.

153 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)*][56].

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

FIA_UAU.5	Multiple authentication mechanisms
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide (1) the execution of the VERIFY command, (2) the execution of the CHANGE REFERENCE DATA command, (3) the execution of the RESET RETRY COUNTER command, (4) the execution of the EXTERNAL AUTHENTICATE command, (5) the execution of the MUTUAL AUTHENTICATE command, (6) the execution of the GENERAL AUTHENTICATE command, (7) a secure messaging channel, (8) a trusted channel[57] to support user authentication.

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

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

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 commands VERIFY, CHANGE REFERENCE DATA and RESET RETRY COUNTER, (2) key based authentication mechanisms shall be used for authenticating of devices by means of commands EXTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE and GENERAL AUTHENTICATE, (3) [assignment: *additional rules describing how the multiple authentication mechanisms provide authentication*][58].

155 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**[59] 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[60].

156 *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. Package Crypto Box) and the receiver of the commands verifies the authentication by MAC verification of commands (using SK4SM). The receiver of the commands authenticates its message by MAC calculation (using SK4SM) and the sender of a command verifies the authentication by MAC verification of responses (cf. PSO VERIFY CRYPTOGRAPHIC CHECKSUM using SK4TC). If secure messaging is used with encryption the re-authentication includes the encrypted padding in the plaintext as authentication attempt of the message sender (cf. PSO ENCIPHER for commands) and the reciever (cf. secure messaging for responses) and verification of the correct padding as authentication verification by the message receiver (cf. secure messaging for received commands and PSO DECIPHER for received responses). The specification [21] states in section 13.1.2 item (N031.600): This re-authentication is controlled by the external entity (e.g. the connector in the eHealth environment). If no Secure Messaging is indicated in the CLA byte (see [ISO7816-4] Clause 5.1.1) and SessionkeyContext.flagSessionEnabled has the value SK4SM, then the security status of the key that was involved in the negotiation of the session keys MUST be deleted by means of clearSessionKeys(...)." Furthermore item (N031.700) states that the security status of the key that was involved in the negotiation of the session keys MUST be deleted by means of clearSessionKeys(...) if the check of the command CMAC (cf. FCS_COP.1/COS.CMAC) or Retail-MAC (cf. FCS_COP.1/COS.RMAC) fails. The TOE does not execute any command with

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

[59] Refinement identifying the concrete user

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

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.

157 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] [61] 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.

158 *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.

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

FIA_API.1	Authentication Proof of Identity
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide ~~a~~ (1) INTERNAL AUTHENTICATE, (2) MUTUAL AUTHENTICATE, (3) GENERAL AUTHENTICATE [62] to prove the identity of the TSF itself [63] to an external entity.

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

FMT_SMR.1	Security roles

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

62 [assignment: *authentication mechanism*]

63 [assignment: *object, authorized user or rule*].

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*][64].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

161 *Application note 16*: The protection profile BSI-CC-PP-0035-2007 does not explicitly define role because roles are linked to life cycle of the chip not addressed by SFR. Therefore the current PP defines the role "World" relevant for all parts of the TOE (e.g. physical protection) and roles for COS related SFR. The ST may add developer specific roles, e. g. for TSF data export according to FPT_ITE.1/EXP.

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

163 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 : the Certificate Holder Authorisation (CHA) in the CVC,

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

(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[65].

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

(2) If the command SELECT is executed and the *newFile* is an folder the initial authentication state of the selected folder inherit the authentication state of the folder above up the root.[66]

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

(1) The authentication state is changed to "authenticated Human User" for the specific context when the Human User has successfully authenticated via one of the following procedures:
   a) VERIFY command using the context specific password or the context specific Multi-Reference password,
   b) If the security attribute *flagEnabled* of password object is set to *False* the authentication state for this specific password is changed to "authenticated Human User".
   c) If the security attribute *flagEnabled* of Multi-Reference password object is set to *False* the authentication state for this specific Multi-Reference password is changed to "authenticated Human User".

(2) The authentication state is changed to "authenticated Device" for the specific authentication context when a Device has successfully authenticated via one of the following procedures:
   a) EXTERNAL AUTHENTICATE with symmetric or public keys,
   b) MUTUAL AUTHENTICATE with symmetric or public keys,
   c) GENERAL AUTHENTICATE with mutual ELC authentication and
   d) GENERAL AUTHENTICATE for asynchronous secure messaging.

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

(4) All authentication contexts are lost and the authentication state

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

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

is set to “not authenticated” for all contexts if the TOE is reset.

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

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

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

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

(9) [assignment: *further rules for the changing of attributes*][67].

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

6.1.6 Access Control

165 *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, 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.

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

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

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[68] on (1) the subjects *logical channel* bind to users a. World, b. Human User, c. Device, d. Human User and Device, [assignment: *list of further subjects*], (2) the objects a. all executable code implemented by the TOE, b. MF, c. Application, d. Dedicated file, e. Application dedicated file, *f.* persistent stored public keys, g. [assignment*: list of further objects*], (3) the operation by command following a. command SELECT, b. create objects with command LOAD APPLICATION with and without command chaining, c. delete objects with command DELETE, d. read fingerprint with command FINGERPRINT, e. command LIST PUBLIC KEY, f. [assignment*: all other operations applicable to MF and DF*].[69]

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

168 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[70] to objects based on the following (1) the subject *logical channel* with security attributes

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

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

[70] [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/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*][71].

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

[71] [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*]

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*][72].

FDP_ACF.1.3/ MF_DF	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[73].
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*].

169 *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 command MANAGE SECURITY ENVIRONMENT. The command SELECT is therefore pre-requisite for many other commands. The access control rule defines for each command, which is defined by CLA, INS, P1 and P2 and acceptable for the type of the object, the necessary security state, which is reached by successful authentication of human user and devices, to allow the access to the selected object. Note the command FINGERPRINT process the data representing the TOE implementation like user data (i.e. hash value calculation, no execution or interpretation as code) and is developer specific. Therefore the ST writer shall describe the TOE specific access control rules for these commands. The ST writer shall perform the open operations where “none” is allowed.

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

FDP_ACC.1/EF	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control.
FDP_ACC.1.1/EF	The TSF shall enforce the access control EF SFP[74] on (1) the subjects *logical channel* bind to users

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

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

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

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 command following
a. SELECT,
b. DELETE of the current file,
c. [assignment*: further operations*][75].

171 *Application note 22*: Note the commands ACTIVATE, DEACTIVATE and, TERMINATE DF for current file applicable to EF, Transparent EF and Structured EF manage the security life cycle attributes. Therefore access control to theses commands are described by FMT_MSA.1/Life. The commands CREATE, GET DATA, GET RESPONSE and PUT DATA are optional. If implemented by the TOE these commands shall be added to the corresponding FDP_ACC.1 and FDP_ACF.1 SFR. 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.

172 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 rule EF SFP[76] to objects based on the following (1) the subject *logical channel* with security attributes a. *interface*, b. *globalPasswordList*, c. *globalSecurityList*, d. *dfSpecificPasswordList*, e. *dfSpecificSecurityList*, f. *bitSecurityList*, g. *SessionkeyContext*, h. [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 protection Mode, checksum*], b. [assignment: *list of further objects listed in*

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

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

FDP_ACC.1.1/EF with their security attributes][77].

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*][78].

FDP_ACF.1.3/EF — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[79].

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*].

173 *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 protection Mode" and "checksum" may be empty because they are optional in the COS specification [21].

174 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[80] 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*],

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

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

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

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

(3) the operation by the following command
   a. ERASE BINARY,
   b. READ BINARY,
   c. SET LOGICAL EOF,
   d. UPDATE BINARY,
   e. WRITE BINARY,
   f. [assignment*: further operation*][81].

175 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[82] 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*, a. [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 protection Mode, checksum*], b. [assignment: *list of further objects listed in FDP_ACC.1.1/TEF*][83].
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*

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

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

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

among subjects and objects covered by the SFP][84].

FDP_ACF.1.3/TEF	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[85].
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*][86].

176 *Application note 24*: The selection of "transaction protection Mode" and "checksum" 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.

177 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[87] 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 command following a. APPEND RECORD, b. ERASE RECORD, c. DELETE RECORD, d. READ RECORD, e. SEARCH RECORD, f. UPDATE RECORD, g. [assignment*: further operation*][88].

178 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.

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

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

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

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

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

179 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[89] 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*, a. [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*][90].
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*][91].
FDP_ACF.1.3/SEF	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.[92].
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*

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

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

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

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

explicitly deny access of subjects to objects][93].

180 *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

181 *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

182 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[94] 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 command following a. DELETE for private, public and symmetric key objects, b. MANAGE SECURITY ENVIRONMENT, c. GENERATE ASYMMETRIC KEY PAIR, d. PSO COMPUTE DIGITAL SIGNATURE, e. PSO VERIFY DIGITAL SIGNATURE, f. PSO VERIFY CERTIFICATE, g. PSO ENCIPHER, h. PSO DECIPHER,

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

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

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*][95].

183 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[96] 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, b. private asymmetric key used for user data with security attributes *seIdentifier* of the current folder, *lifeCycleStatus*, *keyAvailable* and *interfaceDependentAccessRules*, c. public asymmetric key for signature verification used for user data with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules*, d. public asymmetric key for encryption used for user data with security attributes *seIdentifier* of the current folder, *lifeCycleStatus* and *interfaceDependentAccessRules*, e. CVC with security attributes *certificate content* and *signature*, f. ephemeral keys used during Diffie-Hellmann key exchange g. [assignment: *list of further objects listed in FDP_ACC.1.1/KEY*][97].

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

96 [assignment: *access control SFP*]

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

FDP_ACF.1.2/KEY The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) MANAGE SECURITY ENVIRONMENT is [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 verification of the signature of the CVC dependent on *seIdentifier* of the *current folder*, *lifeCycleStatus*, *key type* and *interfaceDependentAccessRules*,

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

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

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

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

interfaceDependentAccessRules.

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

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

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

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

(12) [assignment: *further list of subjects, objects, and operations among subjects and objects covered by the SFP*][98].

FDP_ACF.1.3/KEY The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[99].

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

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

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

GENERATE ASYMMETRIC KEY PAIR with P1='80' or P1='84.

(2) [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*][100].

184 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) Initialization, (2) Personalization, (3) Life Cycle Management by means of 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 commands ACTIVATE, DEACTIVATE, ACTIVATE RECORD, DEACTIVATE RECORD, ENABLE VERIFICATION REQUIREMENT, DISABLE VERIFICATION REQUIREMENT, LOAD APPLICATION, (5) Management of password objects attributes by means of commands CHANGE REFERENCE DATA, RESET RETRY COUNTER, GET PIN STATUS, VERIFY, LOAD APPLICATION, (6) Management of device authentication reference data by means of commands PSO VERIFY CERTIFICATE, GET SECURITY STATUS KEY LOAD APPLICATION, (7) [assignment: *list of further management functions to be provided by the TSF*][101].

185 *Application note 27*: The protection profile BSI-CC-PP-0035-2007 [11] describes initialisation and personalisation as management functions. The ST author shall assign the COS commands dedicated for these management functions.

186 *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 writer should add it to the commands for the Life Cycle Management listed in FMT_SMF.1 and FMT_MSA.1/Life if implemented.

187 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]

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

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

	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[102] to restrict the ability to (1) create[103] **all** security attributes of the new object DF, Application, Application dedicated file, EF, TEF and SEF[104] to subjects allowed execution of command LOAD APPLICATION for the MF, DF, Application, Application dedicated file where the new object is created[105], (2) **change[106] security attributes of the object MF, DF, Application, Application dedicated file, EF, TEF and SEF[107] by means of command LOAD APPLICATION to [selection*: none, subjects allowed execution of command LOAD APPLICATION for the MF, DF, Application, Application dedicated file where the object is updated*]**[108]**,** (3) **change[109] the security attributes *lifeCycleStatus* to „*Operational state (active)*“[110] to subjects allowed execution of command ACTIVATE for the selected object[111],** (4) **change[112] the security attributes *lifeCycleStatus* to „*Operational state (deactivated)*“[113] to subjects allowed execution of command DEACTIVATE for the selected object[114],** (5) **change[115] the security attributes *lifeCycleStatus* to „*Termination state*”[116] to subjects allowed execution of command TERMINATE for the selected EF, the key object or the password object[117],** (6) **change[118] the security attributes *lifeCycleStatus* to „*Termination state*”[119] to subjects allowed execution of**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

command TERMINATE DF for the selected DF, Application or Application File[120],

(7) **change[121]the security attributes *lifeCycleStatus* to „*Termination state*"[122] to subjects allowed execution of command TERMINATE CARD USAGE[123],**

(8) **query[124]the security attributes *lifeCycleStatus* to by means of command SELECT[125] to [selection:*ALWAYS allowed, [assignment: supported access control rules]*][126],**

(9) **delete[127] all security attributes of the selected object[128] to subjects allowed execution of command DELETE for the selected object[129] 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.

188 *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 writer shall perform the selection in FMT_MSA.1.1/Life, clause (2) in order to indicate possible security implications of changes in the TSF data of existing objects.

189 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

119 [assignment: *list of security attributes*]

120 [assignment: *the authorised identified roles*]

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

122 [assignment: *list of security attributes*]

123 [assignment: *the authorised identified roles*]

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

125 [assignment: *list of security attributes*]

126 [assignment: *the authorised identified roles*]

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

128 [assignment: *list of security attributes*]

129 [assignment: *the authorised identified roles*]

FMT_MSA.1.1/SEF	The TSF shall enforce the access control SEF SFP[130] to restrict the ability to (1) change[131] the security attributes *lifeCycleStatus* of the selected record to „*Operational state (active)*“[132] to subjects allowed to execute the command ACTIVATE RECORD[133], (2) **change[134] the security attributes *lifeCycleStatus* of the selected record to „*Operational state (deactivated)*“[135] to subjects allowed to execute the command DEACTIVATE RECORD[136],** (3) **delete[137] all security attributes of the selected record[138] to subjects allowed to execute the command DELETE RECORD[139],** (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.**

190 *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.

191 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

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

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

132 [assignment: *list of security attributes*]

133 [assignment: *the authorised identified roles*]

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

135 [assignment: *list of security attributes*]

136 [assignment: *the authorised identified roles*]

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

138 [assignment: *list of security attributes*]

139 [assignment: *the authorised identified roles*]

control key SFP[140] to provide restrictive[141] default values for security attributes that are used to enforce the SFP.
After reset the security attributes of the subject are set as follows
(1) ***currentFolder*** **is** ***root,***
(2) ***keyReferenceList, globalSecurityList, globalPasswordList, dfSpecificSecurityList, dfSpecificPasswordList and bitSecurityList*** **are empty,**
(3) ***SessionkeyContext.flagSessionEnabled is set*** **to** ***noSK,***
(4) ***seIdentifier*** **is #1,**
(5) currentFile is undefined.

FMT_MSA.3.2 *The TSF* shall allow the subjects allowed to execute the command LOAD APPLICATION[142] to specify alternative initial values to override the default values when an object or information is created.

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

193 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 command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[143] [144] to subjects successful authenticated with the old *secret* of this password object[145], (2) **set new *secret* and change *transportStatus* to *regularPassword* of the password objects with *transportStatus* equal to Leer-PIN[146] [147] to subjects allowed to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01)[148],** (3) **set new *secret* of the password objects by means of command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,00)[149] [150] to subjects successful authenticated with the PUC of this**

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

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

142 [assignment: *the authorised identified roles*]

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

144 [assignment: *other operations*]

145 [assignment: *the authorised identified roles*]

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

147 [assignment: *other operations*]

148 [assignment: *the authorised identified roles*]

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

150 [assignment: *other operations*]

password object [151]

(4) **set new *secret* of the password objects by means of command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02)**[152] [153] **to subjects allowed to execute the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02)*[154]*.**

194 *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.

195 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[155] to restrict the ability to (1) reset by means of commands VERIFY[156] [157] the security attribute retry counter of password objects[158] to subjects successful authenticated with the secret of this password object*[159]*, (2) **reset by means of commands CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)**[160] [161] **the security attribute retry counter of password objects**[162] **to subjects successful authenticated with the old secret of this password object**[163]**,**

151 [assignment: *the authorised identified roles*]

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

153 [assignment: other operations]

154 [assignment: *the authorised identified roles*]

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

156 [assignment: *other operations*]

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

158 [assignment: *list of security attributes*]

159 [assignment: *the authorised identified roles*]

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*]

(3) **change by means of commands CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)[164] [165] the security attribute *transportStatus* from Transport-PIN to regularPassword to subjects allowed to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,00)*[166]*,**

(4) **change by means of commands CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01)[167] [168] the security attribute *transportStatus* from Leer-PIN to regularPassword to subjects allowed to execute the command CHANGE REFERENCE DATA with (CLA,INS,P1)=(00,24,01)*[169]*,**

(5) **reset by means of commands DISABLE VERIFICATION REQUIREMENT with (CLA,INS,P1)=(00,26,00)[170] [171] the security attribute retry counter of password objects [172] to subjects successful authenticated with the old secret of this password object *[173]*,**

(6) **reset by means of commands ENABLE VERIFICATION REQUIREMENT with (CLA,INS,P1)=(00,28,00)[174] [175] the security attribute retry counter of password objects [176] to subjects successful authenticated with the old secret of this password object *[177]*,**

(7) **reset by means of command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,00) or (CLA,INS,P1)=(00,2C,01)[178] [179] the security attribute retry counter of password objects [180] to subjects successful authenticated with the PUC of this password object *[181]*,**

(8) **reset by means of command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or (CLA,INS,P1)=(00,2C,03)[182] [183]**

---

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

165 [assignment: *other operations*]

166 [assignment: *the authorised identified roles*]

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

168 [assignment: *other operations*]

169 [assignment: *the authorised identified roles*]

170 [assignment: *other operations*]

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

172 [assignment: *list of security attributes*]

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*]

the security attribute retry counter of password objects [184] **to to subjects allowed to execute the command RESET RETRY COUNTER with (CLA,INS,P1)=(00,2C,02) or (CLA,INS,P1)=(00,2C,03)**[185]**,**

(9) **query by means of command GET PIN STATUS**[186] [187] **the security attribute *flagEnabled, retry counter, transportStatus*** [188] **to World**[189]**,**

(10) **enable**[190] **the security attributes *flagEnabled* requiring authentication with the selected password**[191] **to subjects authenticated with passwaord and allowed to execute the command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00'28,00)**[192]**,**

(11) **enable**[193] **the security attributes *flagEnabled* requiring authentication with the selected password**[194] **to subjects allowed to execute the command ENABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,28,01)**[195],

(12) **disable**[196] **the security attributes *flagEnabled* requiring authentication with the selected password**[197] **to subjects authenticated with passwaord and allowed to execute the command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,00)**[198]**,**

(13) **disable**[199] **the security attributes *flagEnabled* requiring authentication with the selected password**[200] **to subjects allowed to execute the command DISABLE VERIFICATION REQUIREMENT (CLA,INS,P1)=(00,26,01)**[201]**.**

---

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

184 [assignment: *list of security attributes*]

185 [assignment: *the authorised identified roles*]

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

191 [assignment: *list of security attributes*]

192 [assignment: *the authorised identified roles*]

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

194 [assignment: *list of security attributes*]

195 [assignment: *the authorised identified roles*]

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

197 [assignment: *list of security attributes*]

198 [assignment: *the authorised identified roles*]

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

200 [assignment: *list of security attributes*]

201 [assignment: *the authorised identified roles*]

196 *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.

197 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 commands LOAD APPLICATION[202] the root public keys to roles autorized to execute this command[203], **(2) import by means of commands PSO VERIFY CERTIFICATE[204] the root public keys to roles autorized to execute this command[205],** **(3) import by means of commands PSO VERIFY CERTIFICATE[206] the certificates as device authentication reference data to roles autorized to execute this command[207],** (4) **select by means of command MANAGE SECURITY ENVIRONMENT[208] the device authentication reference data to [selection: *World, roles autorized to execute this command*][209].** **The subject *logical channel* is allowed to execute a command if the security attributes *interface, globalPasswordList, globalSecurityList,***

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

203 [assignment: *the authorised identified roles*]

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

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*]

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

198 *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.

199 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[210] to restrict the ability to query[211] [212] the security attributes access control rights set for the key[213] to meet the access rules of command GET SECURITY STATUS KEY of the object dependent on *lifeCycleStatus*, *seIdentifier* and *interfaceDependentAccessRules* [214].

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

FMT_MTD.1/NE	Management of TSF data – No export
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/NE	The TSF shall restrict the ability to (1) export TSF data according to FPT_ITE.2[215] the (a) public authentication reference data, (b) security attributes for objects of the object system to [assignment*: list of security attributes of subjects*][216], **(2) export TSF data according to FPT_ITE.2[217] the [assignment: *list of all TOE specific security attributes not***

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

[211] [assignment: *other operations*]

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

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

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

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

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

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

described in COS specification [21]]**[218] [219] to [assignment:** ***list of security attributes of subjects*****][220],**

(3) export[221] 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

(i) Private keys of the user

(j) Symmetric keys of the user

(k) [assignment: ***list of types of user data*****][222]**
to nobody[223].

6.1.7 Cryptographic Functions

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

(1) length 256 bit
  (a) brainpoolP256r1 defined in RFC5639 [41],
  (b) ansix9p256r1] defined in ANSI X.9.62 [42],
(2) length 384
  (a) brainpoolP384r1 defined in RFC5639 [41],
  (b) ansix9p384r1 defined in ANSI X.9.62 [42],
(3) length 512 bit
  (a) brainpoolP512r1] defined in RFC5639 [41].

202 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 modul length.

203 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.

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

[219] [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: *the authorised identified roles*]

Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: deterministic, hybrid deterministic, physical, hybrid physical][224] random number generator **[selection: *DRG.3, DRG.4, PTG.2, PTG.3*]** [7] 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***][225].

204 *Application note 35*: This SFR requires the TOE to generate random numbers used for key generation according to TR-03116 [19] section 3.5, requiring RNG classes identified in the selection in element FCS_RNG.1.1 and recommending RNG of class PTG.3. Note that the RNG of class DRG4 are hybrid deterministic and of class PTG3 are hybrid physical which are not addressed in BSI-CC-PP-0035. The implementation of the PACE protocol requires RNG of class PTG.3 (cf. [16]). The COS specification [21] requires to implement RNG for

- the command GET CHALLENGE,
- the command GET RANDOM if package Logical Channel is supported[226],
- the authentication protocols as required by FIA_UAU.4,
- the key agreement for secure messaging

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

205 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[227] in accordance with a specified cryptographic algorithm (1) SHA-1, (2) SHA-256, (3) SHA-384, (4) SHA-512[228] and cryptographic key sizes none[229] that meet the following TR-03116 [19], FIPS 180-4[37][230].

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

225 [assignment: *a defined quality metric*]

226 cf. chapter Package Logical Channel

227 [assignment: *list of cryptographic operations*]

228 [assignment: *cryptographic algorithm*]

229 [assignment: *cryptographic key sizes*]

206 The TOE shall meet the requirement "Cryptographic key generation – 3TDES_SM (FCS_CKM.1/3TDES_SM)" as specified below.

FCS_CKM.1/3TDES_SM	Cryptographic key generation – 3TDES_SM
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/ 3TDES_SM	The TSF shall generate **session** cryptographic keys in accordance with a specified cryptographic key generation algorithm Key Derivation Function specified in sec. 5.6.3 in ANSI X9.63[231] and specified cryptographic key sizes 192 bit (168 bit effectively)[232] that meet the following: ANSI X9.63 [40][233].

207 The TOE shall meet the requirement "Cryptographic operation - COS for 3TDES (FCS_COP.1/COS.3TDES)" as specified below.

FCS_COP.1/COS.3TDES	Cryptographic operation - COS for 3TDES
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.3TDES	The TSF shall perform decryption and encryption for secure messaging[234] in accordance with a specified cryptographic algorithm 3TDES in CBC mode[235] and cryptographic key sizes 192 bit (168 bit effectively)[236] that meet the following TR-03116 [19], NIST SP 800-67 [38][237].

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

FCS_COP.1/COS.RMAC	Cryptographic operation COS for RMAC
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.RMAC	The TSF shall perform (1) computation and verification of cryptographic checksum

230 [assignment: *list of standards*]

231 [assignment: *cryptographic key generation algorithm*]

232 [assignment: *cryptographic key sizes*]

233 [assignment: *list of standards*]

234 [assignment: *list of cryptographic operations*]

235 [assignment: *cryptographic algorithm*]

236 [assignment: *cryptographic key sizes*]

237 [assignment: *list of standards*]

for command
a. MUTUAL AUTHENTICATE,
b. EXTERNAL AUTHENTICATE,

(2) computation and verification of cryptographic checksum for secure messaging[238]

in accordance with a specified cryptographic algorithm Retail MAC[239] and cryptographic key sizes 192 bit (168 bit effectively)[240] that meet the following TR-03116 [19], COS specification [21][241].

209 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 commands a. MUTUAL AUTHENTICATE, b. EXTERNAL AUTHENTICATE, 2. encryption with card internal key for command INTERNAL AUTHENTICATE, 3. encryption and decryption with card internal key for command GENERAL AUTHENTICATE, 4. encryption and decryption for secure messaging[242] in accordance with a specified cryptographic algorithm AES in CBC mode[243] and cryptographic key sizes 128 bit, 192 bit, 256 bit[244] that meet the following: TR-03116 [19], COS specification [21], FIPS 197 [33][245].

210 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.

238 [assignment: *list of cryptographic operations*]

239 [assignment: *cryptographic algorithm*]

240 [assignment: *cryptographic key sizes*]

241 [assignment: *list of standards*]

242 [assignment: *list of cryptographic operations*]

243 [assignment: *cryptographic algorithm*]

244 [assignment: *cryptographic key sizes*]

245 [assignment: *list of standards*]

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. 4.4.3 in [17][246] and specified cryptographic key sizes 128 bit, 192 bit, 256 bit[247] that meet the following TR-03111 [17], COS specification [21], FIPS 197 [33][248].

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

212 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 a. MUTUAL AUTHENTICATE, b. EXTERNAL AUTHENTICATE, (2) computation of cryptographic checksum for command INTERNAL AUTHENTICATE, (3) computation and verification of cryptographic checksum for secure messaging[249] in accordance with a specified cryptographic algorithm CMAC[250] and cryptographic key sizes 128 bit, 192 bit, and 256 bit[251] that meet the following TR-03116 [19], COS specification [21], NIST SP 800-38B [36][252].

213 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

246 [assignment: *cryptographic key generation algorithm*]

247 [assignment: *cryptographic key sizes*]

248 [assignment: *list of standards*]

249 [assignment: *list of cryptographic operations*]

250 [assignment: *cryptographic algorithm*]

251 [assignment: *cryptographic key sizes*]

252 [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/RSA	The TSF shall generate cryptographic **RSA** keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*][253] and specified cryptographic key 2048 bit and 3072 bit modulo length[254] that meet the following TR-03116 [19][255].

214 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**[256] and specified cryptographic key 256 bit, 384 bit and 512 bit [257] that meet the following TR-03111 [17], COS specification [21][258].

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

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

The ST writer shall perform the missing operations in the element FCS_CKM.1/RSA and FCS_CKM.1/ELC according to the implemented key generation algorithms.

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

FCS_COP.1/COS.RSA.S	Cryptographic operation – RSA signature-creation
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or

253 [assignment: *cryptographic key generation algorithm*]

254 [assignment: *cryptographic key sizes*]

255 [assignment: *list of standards*]

256 [assignment: *cryptographic key generation algorithm*]

257 [assignment: *cryptographic key sizes*]

258 [assignment: *list of standards*]

	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[259] in accordance with a specified cryptographic algorithm (1) RSASSA-PSS-SIGN with SHA-256, (2) RSA SSA PKCS1-V1_5, (3) RSA ISO9796-2 DS1 with SHA-256 (for INTERNAL AUTHENTICATE only), (4) RSA ISO9796-2 DS2 with SHA-256 (for PSO Compute DIGITAL SIGNATURE only) [260], (1) and cryptographic key sizes 2048 bit modulo length, (2) 3072 bit modulo length[261] that meet the following: TR-03116 [19], COS specification [21], [31], [34][262].

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

FCS_COP.1/COS.RSA.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/ COS.RSA.V	The TSF shall perform digital signature verification for import of RSA keys using the commands (1) PSO VERIFY CERTIFICATE, (2) EXTERNAL AUTHENTICATE[263] in accordance with a specified cryptographic algorithm RSA ISO9796-2 DS1[264] and cryptographic key sizes 2048 bit modulo length[265] that meet the following: TR-03116 [19], COS specification [21], [31] ,[34][266].

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

259 [assignment: *list of cryptographic operations*]

260 [assignment: *cryptographic algorithm*]

261 [assignment: *cryptographic key sizes*]

262 [assignment: *list of standards*]

263 [assignment: *list of cryptographic operations*]

264 [assignment: *cryptographic algorithm*]

265 [assignment: *cryptographic key sizes*]

266 [assignment: *list of standards*]

219 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 the commands (1) PSO VERIFY CERTIFICATE, (2) PSO VERIFY DIGITAL SIGNATURE, (3) EXTERNAL AUTHENTICATE[267] in accordance with a specified cryptographic algorithm ECDSA with COS standard curves using (1) SHA-256, (2) SHA-384, (3) SHA-512[268] and cryptographic key sizes 256 bits, 384 bits, 512 bits[269] that meet the following TR-03111 [17], TR-03116 [19], COS specification [21], [40][270].

220 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 command (1) PSO COMPUTE DIGITAL SIGNATURE, (2) INTERNAL AUTHENTICATE[271] in accordance with a specified cryptographic algorithm ECDSA with COS standard curves using (1) SHA-256, (2) SHA-384, (3) SHA-512[272] and cryptographic key sizes 256 bits, 384 bits, 512 bits[273] that meet the following TR-03111 [17], TR-03116 [19], COS

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

[268] [assignment: *cryptographic algorithm*]

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

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

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

[272] [assignment: *cryptographic algorithm*]

specification [21], [40][274].

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

222 The TOE shall meet the requirement "Cryptographic operation – RSA encryption and (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) [275] in accordance with a specified cryptographic algorithm (6) for encryption: a. RSAES-PKCS1-v1_5_Encrypt ([34] section 7.2.1), b. RSA-OAEP-Encrypt ([34] section 7.1.1]), (7) for decryption: a. RSAES-PKCS1-v1_5_Decrypt ([34] section 7.2.2]), b. RSA-OAEP-Decrypt ([34] section 7.1.2]) [276] and cryptographic key sizes 2048 bit and 3072 bit modulo length for RSA private key operation, 2048 bit length for RSA public key operation, and 256 bit, 384 bit and 512 bit for the COS standard

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

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

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

[276] [assignment: *cryptographic algorithm*]

curves[277] that meet the following TR-03116 [19], COS specification [21], [34][278].

223 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) [279] in accordance with a specified cryptographic algorithm (1) for encryption ELC encryption, (2) for decryption ELC decryption[280] and cryptographic key sizes 2048 bit and 3072 bit modulo length for RSA private key operation, 2048 bit length for RSA public key operation, and 256 bits, 384 bits, 512 bits for ELC keys with COS standard curves[281] that meet the following TR-03111 [17], TR-03116 [19], and COS specification [21][282].

224 *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 writer is asked to add a SFR FCS_COP.1/CB_HASH specifying the supported hash algorithms.

225 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

277 [assignment: *cryptographic key sizes*]

278 [assignment: *list of standards*]

279 [assignment: *list of cryptographic operations*]

280 [assignment: *cryptographic algorithm*]

281 [assignment: *cryptographic key sizes*]

282 [assignment: *list of standards*]

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

226 *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 writer.

6.1.8 Protection of communication

227 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[283] to initiate communication via the trusted channel.
FTP_ITC.1.3/TC	The TSF shall initiate communication via the trusted channel for none[284].

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

6.2 Security Assurance Requirements for the TOE

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

Security Target evaluation (Class ASE)

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

Assurance Level 4 (EAL4)

231 and augmented by taking the following components:

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

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

ALC_DVS.2 (Development security)

ATE_DPT.2 (Test depth)

AVA_VAN.5 (Advanced methodical vulnerability analysis).

232 The 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: Assurance components

6.2.1 Refinements of the TOE Assurance Requirements

233 In the BSI-CC-PP-0035-2007 [11] refinements of the TOE assurance requirements were performed. This Protection Profile takes over the refinements for the SFR listed in section 6.1.3 "Security Functional Requirements for the TOE taken over from BSI-CC-PP-0035-2007". The refinements must be applied for the SFR listed in section 6.1.3 (see Table 20). The refinements and the section where the refinement in BSI-CC-PP-0035-2007 [11] is specified are listed in Table 22 . The ST writer is asked to refer the corresponding sections of the BSI-CC-PP-0035-2007 [11] (see Table 22).

234 For all other Security Functional Requirements the TOE assurance requirements from Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [3] should be used. Note that it is possible to use the TOE assurance requirements as defined in BSI-CC-PP-0035-2007 [11] (see Table 22) for all SFR in this Protection Profile. According to Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [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)"
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 "Refinement regarding Vulnerability Analysis (AVA_VAN)"

Table 22: Refined TOE assurance requirements

235 The following sections define refinements and application notes to the chosen SAR.

6.2.2 Refinements to ADV_ARC.1 Security architecture description

236 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.

237 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

238 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.

239 *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], chapter 2.5.2, for details). This interface is also analysed as attack surface in the vulnerability analysis e.g. in respect to perturbation and emanation side channel analysis.

6.2.4 Refinement to ADV_IMP.1

240 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**.

241 *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 platform IC including all IC Embedded Software and especially the Card Operating System, (COS).

6.2.5 Refinements to AGD_OPE.1 Operational user guidance

242 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.

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

6.2.6 Refinements to ATE_FUN.1 Functional tests

244 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], SMC-K [25] or SMC-KT [26].

245 *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

246 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], SMC-K [25] and SMC-KT [26].

247 *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

248 This chapter comprises three parts:

- The SFR rationale provided by a table showing the coverage of security objective of the TOE by security functional requirements, already provided in the current version of this PP, and rationale explanatory text which will be provided in future versions of this PP
- The SFR dependency rationale missing in the current version and to be provided in future versions of this PP
- The SAR rationale provided in section 6.3.3.

6.3.1 Security Functional Requirements Rationale

249 Table 2 in section 6.3.1 “Security Functional Requirements Rational” in BSI-CC-PP-0035-2007 [11] gives an overview, how the security functional requirements taken over are combined to meet the security objectives. Please refer that table and the text following after that table justifying this in detail for the further details.

250 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		
FDP_ITT.1/SICP		X				X		
FMT_LIM.1/SICP							X	
FMT_LIM.2/SICP							X	
FPT_FLS.1/SICP				X				
FPT_ITT.1/SICP		X				X		
FPT_PHP.3/SICP			X		X			
FRU_FLT.2/SICP				X				

Table 23: Coverage of Security Objectives for the TOE IC part by SFR

251 As stated in section 2.4, this PP claims conformance to BSI-CC-PP-0035-2007 [11]. The objectives and SFRs as used in Table 23 are defined and handled in [11]. Hence, the rationale for these items and their correlation from Table 23 is given in [11] and not repeated here.

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

	O.Integrity	O.Confidentiality	O.Resp-COS	O.TSFDataExport	O.Authentication	O.AccessControl	O.KeyManagement	O.Crypto	O.SecureMessaging
FMT_SMF.1						X			
FMT_MSA.1/Life					X	X	X		
FMT_MSA.1/SEF						X			
FMT_MTD.1/PIN					X	X			
FMT_MSA.1/PIN					X	X			
FMT_MTD.1/Auth					X	X			
FMT_MSA.1/Auth					X	X			
FMT_MTD.1/NE		X				X			
FCS_RNG.1							X	X	
FCS_COP.1/SHA								X	
FCS_COP.1/COS.3TDES								X	X
FCS_COP.1/COS.AES								X	X
FCS_COP.1/COS.RMAC								X	X
FCS_CKM.1/3TDES_SM							X	X	X
FCS_CKM.1/AES.SM							X	X	
FCS_CKM.1/RSA							X	X	
FCS_CKM.1/ELC							X	X	
FCS_COP.1/COS.CMAC								X	
FCS_COP.1/COS.RSA.S								X	
FCS_COP.1/COS.RSA.V								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 SFR

252 A detailed justification required for *suitability* of the security functional requirements to achieve the security objectives is given below.

253 The security objective **O.Integrity** "Integrity of internal data" requires the protection of the integrity of user data, TSF data and security services. This 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.

254 The security objective **O.Confidentiality** "Confidentiality of internal data" requires the protection of the confidentiality of sensitive user data and TSF data. This 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.

255 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.

256 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 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.

257 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 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_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.

258 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 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 folders 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 folders 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 authorized 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 SFRs require 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 recorde. For that purpose the SFRs require 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.

259 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 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.1/3TDES_SM, FCS_CKM.1/AES.SM, FCS_CKM.1/RSA, FCS_CKM.1/ELC, require that the TSF generates cryptographic keys with specific key generation algorithms as stated in the SFRs. The mentioned SFRs are needed to fulfil different requirements of the intended usage of the cryptographic keys.

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

260 The security objective **O.Crypto** "Cryptographic functions" requires the ability of the TSF to implement secure cryptographic algorithms. This 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.3TDES requires that the TSF provides decryption and encryption using 3TDES for secure messaging.
- FCS_COP.1/COS.AES requires that the TSF provides decryption and encryption using AES with different key sizes.
- FCS_COP.1/COS.RMAC requires that the TSF provides computation and verification of cryptographic checksums using the Retail MAC algorithm.
- 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.RSA.V requires that the TSF provides the verification 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.1/3TDES_SM, FCS_CKM.1/AES.SM, FCS_CKM.1/RSA, 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.

261 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 objective is addressed by the following SFRs:

- FCS_COP.1/COS.3TDES requires that the TSF provides decryption and encryption using 3TDES for secure messaging.
- 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.RMAC requires that the TSF provides computation and verification of cryptographic checksums using the Retail MAC algorithm. One use case of that required functionality is secure messaging.
- FCS_CKM.1/3TDES_SM requires that the TSF generates cryptographic keys with specific key generation algorithms as stated in the SFR.
- 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's Dependencies

262 Table 3 in section 6.3.1 "Dependencies of security functional requirements" in BSI-CC-PP-0035-2007 [11] lists the security functional requirements defined in BSI-CC-PP-0035-2007, their dependencies and whether they are satisfied by other security requirements defined in this Protection Profile. Please refer that table and the text following after that table justifying this in detail for the further details on the remaining cases.

263 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.

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

265 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
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.

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

SFR	dependent on	fulfilled by
	control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY, FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/PIN	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/PIN	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY, FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Auth	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Auth	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY, FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/NE	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FMT_SMR.1, FMT_SMF.1
FCS_RNG.1	No dependencies.	n. a.
FCS_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.3TDES	[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.1/3TDES_SM, FCS_CKM.4
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/AES.SM, FCS_CKM.4

SFR	dependent on	fulfilled by
	FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	
FCS_COP.1/COS.RMAC	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction.	FCS_COP.1/COS.3TDES, FCS_CKM.4
FCS_CKM.1/3TDES_SM	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction.	FCS_COP.1/COS.3TDES, 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/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.V, FCS_COP.1/COS.RSA, 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, FCS_CKM.4

SFR	dependent on	fulfilled by
FCS_COP.1/COS.RSA.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, 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 as of TSF data used by FCS_COP.1/COS.ECDSA.V (instead of import of user data FDP_ITC.1 or FDP_ITC.2) FCS_CKM.4
FCS_COP.1/COS.RSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/RSA, FCS_CKM.4
FCS_COP.1/COS.ELC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/ELC, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1/3TDES_SM, FCS_CKM.1/AES.SM, FCS_CKM.1/RSA, FCS_CKM.1/ELC, FCS_CKM.1/DH.PACE
FTP_ITC.1/TC	No dependencies.	n. a.

Table 25: Dependencies of the SFR

6.3.3 Security Assurance Requirements Rationale

266 The current 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.

267 Please refer section 6.3.3 “Rationale for the Assurance Requirements” in BSI-CC-PP-0035-2007 [11] for the details regarding the chosen assurance level EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

268 The selection of the component ATE_DPT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR-enforcing modules. The functional testing of SFR-enforcing modules is due to the TOE building a smartcard platform with very broad and powerful security functionality but without object system. An augmentation with ATE_DPT.2 only for the SFR specified in BSI-CC-PP-0035-2007 [11] would have been sufficient to fulfil the conformance, but this would contradict the intention of BSI-CC-PP-0035-2007. Therefore the augmentation with ATE_DPT.2 is required for the complete Protection Profile.

269 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.

270 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.

271 The set of assurance requirements being part of EAL4 fulfils all dependencies a priori.

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

– ATE_DPT.2,

– ALC_DVS.2, and

– AVA_VAN.5.

273 For these additional assurance component, 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

Component	Dependencies required by CC Part 3	Dependency fulfilled by
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

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

7.1 TOE Overview

275 Additional to the TOE definition given in section 1.2.1 TOE definition and operational usage the TOE is equipped with additional cryptographic functionality.

7.2 Security Problem Definition

7.2.1 Assets and External Entities

Assets

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

Subjects and external entities

277 There are no additional external entities and subjects than those defined in section 3.1.

7.2.2 Threats

278 There are no additional threats than the threats defined in section 3.2.

7.2.3 Organisational Security Policies

279 There are no additional Organisational Security Policies than the Organisational Security Policies defined in section 3.3.

7.2.4 Assumptions

280 There are no additional Assumptions than the Assumptions defined in section 3.4.

7.3 Security Objectives

281 The Security Objectives for the TOE (section 4.1) and the Security Objectives for Operational Environment (section 4.2) is supplemented for the package Crypto Box. Therefore the Security Objective Rationale (section 4.3) is supplemented as well.

282 The TOE shall provide a "**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 successful authenticated device and receiving responses from this device on demand of the external application.

283 The operational environment shall provide a "**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 trough a trusted channel supports device authentication with key derivation, secure messaging for received commands and sending responses.

284 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

285 Additional to the Authentication reference data of the devices and security attributes listed in Table 15 the following table defines the authentication reference data of subjects for the TOE with package Crypto Box.

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

Table 27: Authentication reference data of the devices and security attributes

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

User type resp. Subject type	Authentication verification 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

287 Additional to the Security Functional Requirements for the TOE defined in section 6.1 the TOE shall meet the following SFR.

288 The TOE shall meet the requirement "Re-authenticating (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**[285] under the conditions (1) each message received after establishing the trusted channel by successful authentication by execution of the 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 [286].

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

FIA_API.1/CB	Authentication Proof of Identity – Trusted channel
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1/CB	The TSF shall provide ~~a~~

[285] Refinement identifying the concrete user

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

(1) PSO ENCIPHER and PSO COMPUTE CRYPTOGRAPHIC CHECKSUM with SK4TC used for trusted channel commands[287]

to prove the identity of the TSF itself[288] to an external entity.

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

FIA_USB.1/CB	User-subject binding
Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition – Trusted channel
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[289].
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[290].
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 commands PSO VERIFY CRYPTOGRAPHIC CHECKSUM fails the verification or the message received in command PSO DECIPHER fail 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*][291].

291 The TOE shall meet the requirement "Cryptographic operation – CB 3TDES (FCS_COP.1/CB.3TDES)" as specified below.

FCS_COP.1/CB.3TDES	Cryptographic operation – CB 3TDES
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.3TDES	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 with card internal key for commands a. MUTUAL AUTHENTICATE,

[287] [assignment: *authentication mechanism*]

[288] [assignment: *object, authorized user or rule*].

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

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

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

b. EXTERNAL AUTHENTICATE,

(4) encryption with card internal key for command INTERNAL AUTHENTICATE, and

(5) encryption and decryption for trusted channel PSO ENCIPHER and PSO DECIPHER[292]

in accordance with a specified cryptographic algorithm 3TDES in CBC mode[293] and cryptographic key sizes 192 bit (168 bit effectively)[294] that meet the following TR-03116 [19], NIST SP 800-67 [38][295].

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

FCS_COP.1/CB.RMAC	Cryptographic operation – CB RMAC
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.RMAC	The TSF shall perform (1) computation of cryptographic checksum for a. INTERNAL AUTHENTICATE, (2) computation and verification of cryptographic checksum for command b. PSO COMPUTE CRYPTOGRAPHIC CHECKSUM, c. PSO VERIFY CRYPTOGRAPHIC CHECKSUM (3) computation and verification of cryptographic checksum for trusted channel[296] in accordance with a specified cryptographic algorithm Retail MAC 32[297] and cryptographic key sizes 192 bit (168 bit effectively)[298] that meet the following TR-03116 [19], COS specification [21][299].

293 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

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

[293] [assignment: *cryptographic algorithm*]

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

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

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

[297] [assignment: *cryptographic algorithm*]

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

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

	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[300] in accordance with a specified cryptographic algorithm AES in CBC mode[301] and cryptographic key sizes 128 bit, 192 bit, 256 bit[302] that meet the following: TR-03116 [19], COS specification [21], FIPS 197 [33][303].

294 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 a. INTERNAL AUTHENTICATE, (2) computation and verification of cryptographic checksum for trusted channel a. PSO COMPUTE CRYPTOGRAPHIC CHECKSUM, b. PSO VERIFY CRYPTOGRAPHIC CHECKSUM[304] in accordance with a specified cryptographic algorithm CMAC[305] and cryptographic key sizes 128 bit, 192 bit, and 256 bit[306] that meet the following TR-03116 [19], COS specification [21], [36][307].

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

300 [assignment: *list of cryptographic operations*]

301 [assignment: *cryptographic algorithm*]

302 [assignment: *cryptographic key sizes*]

303 [assignment: *list of standards*]

304 [assignment: *list of cryptographic operations*]

305 [assignment: *cryptographic algorithm*]

306 [assignment: *cryptographic key sizes*]

307 [assignment: *list of standards*]

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[308] 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]) [309] and cryptographic key sizes 2048 bit and 3072 bit modulo length for RSA private key operation and 2048 bit length for RSA public key operation[310] that meet the following PKCS #1 [34][311].

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

FCS_COP.1/CB.ELC	Cryptographic operation – CB ECC
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/CB.ELC	The TSF shall perform encryption with stored key for command PSO ENCIPHER[312] in accordance with a specified cryptographic algorithm ELC encryption with COS standard curves[313] and cryptographic key sizes 256 bits, 384 bits, 512 bits[314] that meet the following TR-03111 [17], chapter 4.3.1, 4.3.3 and 5.3.1.2[315].

297 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 cryptobox package.

308 [assignment: *list of cryptographic operations*]

309 [assignment: *cryptographic algorithm*]

310 [assignment: *cryptographic key sizes*]

311 [assignment: *list of standards*]

312 [assignment: *list of cryptographic operations*]

313 [assignment: *cryptographic algorithm*]

314 [assignment: *cryptographic key sizes*]

315 [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
FIA_API.1/CB										X
FIA_UAU.6/CB										X
FIA_USB.1/CB										X
FCS_COP.1/CB.3TDES								X		X
FCS_COP.1/CB.RMAC								X		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 SFR for Package Cryptobox

298 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.

299 The security objective **O.TrustedChannel** "Trusted channel" requires cryptographic functionality for trusted channel support as described by SFR FIA_API.1/CB, FIA_UAU.6/CB, FIA_USB.1/CB, FCS_COP.1/CB.3TDES, FCS_COP.1/CB.RMAC, 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.3TDES requires that the TSF provides decryption and encryption using 3TDES to be used in dedicated commands.
- FCS_COP.1/CB.RMAC requires that the TSF provides computation and verification of cryptographic checksums using the Retail MAC algorithm to be used in dedicated commands.
- 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.

300 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.3TDES requires that the TSF provides decryption and encryption using 3TDES to be used in dedicated commands.
- FCS_COP.1/CB.RMAC requires that the TSF provides computation and verification of cryptographic checksums using the Retail MAC algorithm to be used in dedicated commands.
- 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.

301 The following table lists the required dependencies of the SFRs of this PP package and gives the concrete SFRs from this document which fulfils the required dependencies.

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.3TDES	[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.1/3TDES_SM, FCS_CKM.4
FCS_COP.1/CB.RMAC	[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.1/3TDES_SM, FCS_CKM.4
FCS_COP.1/CB.AES	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/AES.SM, FCS_CKM.4
FCS_COP.1/CB.CMAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or	FCS_CKM.1/AES.SM, FCS_CKM.4

SFR	dependent on	fulfilled by
	FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	
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, FCS_CKM.4

Table 30: Dependencies of the SFRs for Package Cryptobox

8 Package Contactless

302 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 chapter defines Package Contactless to be used by the ST writer if the TOE provides this security functionality.

303 The TSF for the Proximity Coupling Devices (PCD) is described in the Package PACE for Proximity Coupling Device in the chapter 9. Both packages are describing TSF for different roles in the PACE protocol. E.g. the human user input the CAN into the smartcard terminal (as PCD) and the smartcard 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 smartcard (as PICC), which is a sample of the TOE but with Package Contactless and is running the PACE protocol in PICC role.

8.1 TOE Overview

304 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 depended access rules in that case.

8.2 Security Problem Definition

8.2.1 Assets and External Entities

Assets

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

Security Attributes of Users and Subjects

306 The PACE protocol provides mutual authentication between a smartcard running the Proximity Integrated Circuit Chip (PICC) role and a terminal running 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 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.

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

User type	Definition
device with contactless communication	An external Device communicating with the TOE trough the contactless interface. The subject bind to this device has the security attribute “kontaktlos” (contactless communication).
device authenticated using PACE protocol in PCD role	An external Device communicating with the TOE trough the contactless interface and successful authenticated by PACE protocol in PCD role.

8.2.2 Threats

308 There are no additional threats than the threats defined in section 3.2.

8.2.3 Organisational Security Policies

309 There are no additional Organisational Security Policies than the Organisational Security Policies defined in section 3.3.

8.2.4 Assumptions

310 There are no additional Assumptions than the Assumptions defined in section 3.4.

8.3 Security Objectives

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

312 The TOE shall provide a “Protection of contactless communication with PACE (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.

313 The operational environment shall provide a “PACE support by terminals (OE.PACE_Terminal)” as specified below.

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

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

314 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

315 Additional 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 user in PCD role and the authentication verification data used by the TSF itself (cf. FIA_API.1) in PICC role.

User type resp. Subject type	Authentication reference data and security attributes	Operations
Device as PCD	**Symmetric Card Connection Object** (SCCO) Authentication reference data SCCO stored in TOE and corresponding to the CAN, MAC session key SK4SM Security attributes *keyIdentifier* of the SCCO in the *globalSecurityList* if SCCO was in 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 TOE running PACE protocol role as PICC to authenticate the external device running PACE protocol role as PCD.
TOE as PICC	SK4SM referenced in *macKey* and *SSCmac*	SK4SM is used to generate MAC for command responses.

Table 30: Authentication Data of the COS for Package Contactless

316 Additional to the Security Functional Requirements for the TOE defined in section 6.1 the TOE shall meet the following SFR.

317 The security functionality for access control in case of contactless communication is covered already by the SFR 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 30 even the package Contactless is not included.

318 The TOE shall meet the requirement "Random number generation – RNG for 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*][316] random number generator **RNG class [selection: *DRG.4, PTG.3*] for PACE protocol** that implements: [assignment: *list of security capabilities* ***of the selected RNG***

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

	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***].

319 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[317] in accordance with a specified cryptographic algorithm AES in CBC mode[318] and cryptographic key sizes **[selection: *128, 192, 256*] bit**[319] that meet the following TR-03110 [16], COS specification [21][320].

320 *Application note 49*: 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.

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

FCS_COP.1/ PACE.PICC.MAC	Cryptographic operation – PACE secure messaging MAC
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ PACE.PICC.MAC	The TSF shall perform MAC calculation for secure messaging[321] in accordance with a specified cryptographic algorithm CMAC[322] and cryptographic key sizes **[selection: *128, 192, 256*] bit**[323] that meet the following TR-03110 [16], COS specification [21][324].

317 [assignment: *list of cryptographic operations*]

318 [assignment: *cryptographic algorithm*]

319 [assignment: *cryptographic key sizes*]

320 [assignment: *list of standards*]

321 [assignment: *list of cryptographic operations*]

322 [assignment: *cryptographic algorithm*]

323 [assignment: *cryptographic key sizes*]

322 *Application note 50*: 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.

323 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***]**** [325] and specified cryptographic key sizes **[selection:** ***256, 384, 512***]** [326] that meet the following TR-03110 [16], TR-03111 [17] [327].

324 *Application note 51*: 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].

325 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*

324 [assignment: *list of standards*]

325 [assignment: *cryptographic key generation algorithm*]

326 [assignment: *cryptographic key sizes*]

327 [assignment: *list of standards*]

standards].

326 *Application note 52*: 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.

327 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*][328] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/ PACE	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

328 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*][329] 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.

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

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

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

FIA_UAU.4/ PACE.PICC	Single-use authentication mechanisms
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 [19], COS specification [21][330].

330 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 protocol
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] [20] using commands GENERAL AUTHENTICATE, (2) secure messaging in MAC-ENC mode using PACE session keys according to [20], chapter 13, and [16], part 3, in PICC role[331] 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 PACE protocol in PCD role and secure messaging in MAC-ENC mode using PACE session keys is used to authenticate its commands[332].

331 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 protocol
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[333].

332 *Application note 53*: . 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

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

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

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

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

secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal (see FIA_UAU.5/PACE.PICC).

333 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 protocol
Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1/ PACE.PICC	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: The authentication state for the device using PACE protocol in PCD role with (1) *keyIdentifier* of the used SCCO in the *globalSecurityList* if SCCO was in MF or in *dfSpecificSecurityList* if the SCCO was in the *respective folder*, (2) *SK4SM referenced* in *macKey and SSCmac*[334].
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[335].
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 authenticated 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) [336].

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

FDP_RIP.1/	Subset residual information protection – PACE/PICC protocol

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

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

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

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*][337] the following objects: (1) session keys (immediately after closing related communication session), (2) any ephemeral secret having been generated during DH key exchange (3) [assignment: *list of additional objects*][338].

335 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 protocol
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[339] to transmit and receive[340] user data in a manner protected from unauthorised disclosure.

336 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 protocol
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[341] to transmit and receive[342] user data in a manner protected from modification, deletion, insertion, and replay[343] errors.

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

338 [assignment: *list of objects*]

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

340 [selection: *transmit, receive*]

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

342 [selection: *transmit, receive*]

FDP_UIT.1.2/ PACE	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, and replay[344] has occurred.

337 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[345] 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[346].

338 *Application note 54*: 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.

339 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 protocol
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*][347].
FMT_SMR.1.2/ PACE.PICC	The TSF shall be able to associate users with roles.

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

---

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

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

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

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

347 [assignment: *the authorised identified roles*]

FMT_MTD.1/ PACE.PICC	Management of TSF data – PACE/PICC protocol
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[348] [349] the (1) SCCO used for PACE protocol in PICC role, (2) session keys of secure messaging channel established using PACE protocol in PICC role [350] to none[351].

341 *Application note 55*: 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.

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

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

FIA_ATD.1/ PACE	User attribute definition – PACE protocol
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:

348 [assignment: *other operations*]

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

350 [assignment: *list of TSF data*]

351 [assignment: *the authorised identified roles*]

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

353 [assignment: *conditions for export*]

(1) for users defined in FIA_ATD.1

(2) additionally for device: authentication state gained with SCCO[354].

344 The TOE shall meet the requirement "TOE emanation - PACE (FPT_EMS.1/PACE.PICC)" as specified below (CC part 2 extended).

FPT_EMS.1/ PACE.PICC	TOE emanation – PACE/PICC protocol
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*][355] and [assignment: *list of types of user data*].
FPT_EMS.1.2/ PACE.PICC	The TSF shall ensure any users[356] are unable to use the following interface the contactless interface and circuit contacts[357] 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*] [358] and [assignment: *list of types of user data*].

8.5 Security Requirements rationale

345 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".

354 [assignment: *list of security attributes*]

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

356 [assignment*: type of users*]

357 [assignment: *type of connection*]

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

	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 31: Mapping between security objectives for the TOE and SFR for package Contactless

346 Table 31 above should be taken as extension of Table 24 in order to cover the whole set of security objectives. Hence, the mappings between security objectives and SFRs in the table above are used as *additional* mappings to address the corresponding security objectives.

347 All SFR of the Package Contactless are implementing security functionality for the security objective **O.PACE_Chip**.

348 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 protect the confidential authentication data against compromise.

349 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.

350 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 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.

351 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 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.

352 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 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.

353 The security objective **O.Crypto** "Cryptographic functions" requires the ability of the TSF to implement secure cryptographic algorithms. This security objectives 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.

354 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 SFR, 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 Contacless.

355 The following table lists the required dependencies of the SFRs of this PP package and gives the concrete SFRs from this document which fulfils the required dependencies.

SFR	dependent on	fulfilled by
FCS_CKM.1/ DH.PACE.PICC	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction.	FCS_COP.1/PACE.PICC.ENC, FCS_COP.1/PACE.PICC.MAC, FCS_CKM.4/PACE.PICC
FCS_CKM.4/ PACE.PICC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	FCS_CKM.1/DH.PACE.PICC
FCS_COP.1/ PACE.PICC.ENC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/DH.PACE.PICC, FCS_CKM.4/PACE.PICC
FCS_COP.1/ PACE.PICC.MAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/DH.PACE.PICC, FCS_CKM.4/PACE.PICC
FCS_RNG.1/PACE	No dependencies.	n. a.
FDP_RIP.1/ PACE.PICC	No dependencies.	n. a.
FDP_RIP.1/PACE	No dependencies.	n. a.
FDP_UCT.1/PACE	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FTP_ITC.1/PACE, FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF, FDP_ACC.1/SEF, FDP_ACC.1/KEY,
FDP_UIT.1/PACE	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted	FTP_ITC.1/PACE, FDP_ACC.1/MF_DF, FDP_ACC.1/EF, FDP_ACC.1/TEF,

SFR	dependent on	fulfilled by
	path]	FDP_ACC.1/SEF, FDP_ACC.1/KEY,
FIA_ATD.1/PACE	No dependencies.	n. a.
FIA_UAU.1/PACE	FIA_UID.1 Timing of identification.	FIA_UID.1/PACE
FIA_UAU.4/ PACE.PICC	No dependencies.	n. a.
FIA_UAU.5/ PACE.PICC	No dependencies.	n. a.
FIA_UAU.6/ PACE.PICC	No dependencies.	n. a.
FIA_UID.1/PACE	FIA_UAU.1 Timing of authentication.	FIA_UAU.1/PACE
FIA_USB.1/ PACE.PICC	FIA_ATD.1 User attribute definition	FIA_ATD.1/PACE
FMT_MTD.1/PACE	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1/PACE, FMT_SMF.1
FMT_SMR.1/ PACE.PICC	FIA_UID.1 Timing of identification	FIA_UID.1/PACE
FMT_SMR.1/PACE	FIA_UID.1 Timing of identification	FIA_UID.1/PACE
FPT_EMS.1/ PACE.PICC	No dependencies.	n. a.
FPT_ITE.2/PACE	No dependencies.	n. a.
FTP_ITC.1/ PACE.PICC	No dependencies.	n. a.
FTP_ITC.1/PACE	No dependencies.	n. a.

Table 32: Dependencies of the SFRs for Package Contactless

9 Package PACE for Proximity Coupling Device

356 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 chapter defines Package PACE for Proximity Coupling Device to be used by the ST writer if the TOE provides this security functionality.

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

9.1 TOE Overview

358 This package describes additional TSF supporting the contactless communication of a terminal in PCD role with the smartcard (PICC) using PACE. The TOE is part of the terminal and provides the cryptographic functions for the terminal through its contactbased interface. The terminal implements the contactless interface to PICC.

9.2 Security Problem Definition

9.2.1 Assets and External Entities

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

Security Attributes of Users and Subjects

360 The PACE protocol provides mutual authentication between a smartcard running the Proximity Integrated Circuit Chip (PICC) role and a terminal running Proximity Coupling Devices (PCD) role of the protocol as described in [16] part 2. When the TOE running the PCD role of the PACE protocol the subject gains security attributes defining the authentication status of the external user communicating through the trusted channel established after successful authentication. This authentication status is identified in the response code of the trusted channel commands PSO DECIPHER and PSO VERIFY CRYPTOGRAPHIC CHECKSUM.

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

User type	Definition
device with contactless communication	An external Device communicating with the TOE trough the contactless interface. The subject bind to this device has the security attribute “kontaktlos” (contactless communication).
device authenticated using PACE protocol in PICC role	An external Device communicating with the TOE trough the contactless interface and successful authenticated by PACE protocol in PICC role.

9.2.2 Threats

362 There are no additional threats than the threats defined in section 3.2.

9.2.3 Organisational Security Policies

363 There are no additional Organisational Security Policies than the Organisational Security Policies defined in section 3.3.

9.2.4 Assumptions

364 There are no additional Assumptions than the Assumptions defined in section 3.4.

9.3 Security Objectives

365 The TOE shall provide a “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.

366 The operational environment shall provide a “PACE support by chip (OE.PACE_Chip)” as specified below.

OE.PACE_Chip	**PACE/PICC support by contactless chip** The external device communicating trough its contactless interface using PACE shall support the chip part of the PACE protocol.

367 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

368 Additional to the authentication reference data of the devices listed in Table 15 the following table defines the authentication reference data for the TOE with package PACE for user PICC including the authentication verification data used by the TSF itself as Proximity Coupling Device (cf. FIA_API.1).

User type resp. Subject type	Authentication reference 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 TOE running PACE protocol role as PCD to authenticate the external device running PACE protocol role as PICC. Note, the commands PSO VERIFY CRYPTOGRAPHIC CHECKSUM and PSO DECIPHER supported by TOE with package Cryptobox 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 33: Authentication Data of the COS with Package PACE for Proximity Coupling Device

369 Additional to the Security Functional Requirements for the TOE defined in section 6.1 the TOE shall meet the following SFR.

370 The TOE shall meet the requirement "Cryptographic operation – PACE trusted channel 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[359] in accordance with a specified cryptographic algorithm AES in CBC mode[360] and cryptographic key sizes

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

[360] [assignment: *cryptographic algorithm*]

[selection: *128, 192, 256*] bit[361] that meet the following TR-03110 [16], COS specification [21][362].

371 *Application note 49*: 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.

372 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[363] in accordance with a specified cryptographic algorithm CMAC[364] and cryptographic key sizes **[selection: *128, 192, 256*] bit**[365] that meet the following TR-03110 [16], COS specification [21][366].

373 *Application note 50*: 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.

374 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.PCD	Cryptographic key generation – DH by PACE/PCD
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-***

361 [assignment: *cryptographic key sizes*]

362 [assignment: *list of standards*]

363 [assignment: *list of cryptographic operations*]

364 [assignment: *cryptographic algorithm*]

365 [assignment: *cryptographic key sizes*]

366 [assignment: *list of standards*]

ECDH-GM-AES-CBC-CMAC-256_PCD_with_brainpoolP512r1][367]
and specified cryptographic key sizes **[selection: *256, 384, 512*]**[368]
that meet the following TR-03110 [16], TR-03111 [17][369].

375 *Application note 51*: 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].

376 The TOE shall meet the requirement "Cryptographic key destruction - PACE (FCS_CKM.4/PACE.PCD.PICC)" 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*].

377 *Application note 52*: 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.

378 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 protocol
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] [20] using commands GENERAL AUTHENTICATE, (2) trusted channel using PACE session keys according to [20], chapter 13, and [16], part 3, in PCD role[370]

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

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

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

	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[371].

379 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 protocol
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[372].

380 *Application note 53*: 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).

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

FIA_USB.1/ PACE.PCD	User-subject binding – PACE/PCD protocol
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*[373].
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[374].

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

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

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

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

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

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 commands PSO VERIFY CRYPTOGRAPHIC CHECKSUM fails the verification or the message received in command PSO DECIPHER fail 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)[375].

382 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 protocol
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*] [376] the following objects: (1) trusted channel keys (immediately after closing related communication session), (2) any ephemeral secret having been generated during DH key exchange, (3) [assignment: *list of additional objects*][377].

383 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 protocol
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,

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

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

377 [assignment: *list of objects*]

(4) any object listed in FPT_EMS.1

(5) [assignment: *list of additional types of TSF data*][378]

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

FPT_EMS.1.2/ PACE.PCD: The TSF shall ensure any users[379] are unable to use the following interface the contactless interface and circuit contacts[380] 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*] [381]

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

384 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.
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[382] 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[383].

385 *Application note 54*: 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.

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

---

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

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

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

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

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

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

FMT_SMR.1/ PACE.PCD	Security roles – PACE/PCD protocol
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*][384].
FMT_SMR.1.2/ PACE/PCD	The TSF shall be able to associate users with roles.

387 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 protocol
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/ PACE.PCD	The TSF shall restrict the ability to (1) read[385] [386] the keys of trusted channel established using PACE protocol in PCD role [387] to none[388], (2) define[389] [390] the CAN used for PACE protocol in PCD role to everybody[391].

388 *Application note 55*: 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

389 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".

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

[385] [assignment: *other operations*]

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

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

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

[389] [assignment: *other operations*]

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

[391] [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
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
FMT_SMR.1/PACE.PCD					X	X			X
FTP_ITC.1/PACE.PCD					X	X			X

Table 34: Mapping between security objectives for the TOE and SFR for Package PACE for Proximity Coupling Device

390 Table 34 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.

391 All SFR identified in this PACE for Proximity Coupling Device" are implementing security functionality for the security objective **O.PACE_Terminal**.

392 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 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.

393 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 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.

394 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 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.

395 The security objective **O.Crypto** "Cryptographic functions" requires the ability of the TSF to implement secure cryptographic algorithms. This security objectives 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.

396 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 SFR, 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.

397 The following table lists the required dependencies of the SFRs of this PP package and gives the concrete SFRs from this document which fulfils the required 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_CKM.4 Cryptographic key destruction.	FCS_COP.1/PACE.PCD.ENC, FCS_COP.1/PACE.PCD.MAC, FCS_CKM.4/PACE.PCD
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 35: Dependencies of the SFRs

10 Package Logical Channel

10.1 TOE Overview

398 Additional to the TOE definition given in section 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 optional package Logical Channel in [21].

10.2 Security Problem Definition

10.2.1 Assets and External Entities

Assets

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

Subjects and external entities

400 There are no additional external entities and subjects than those defined in section 3.1.

10.2.2 Threats

401 There are no additional threats than the threats defined in section 3.2.

10.2.3 Organisational Security Policies

402 There are is an additional Organisational Security Policy additional to those defined in section 3.3.

OSP.LogicalChannel	**Logical channel** The TOE supports and the operational environment uses logical channels bound to independent subjects.

403 *Application note 56:* The COS specification [21] describes the concept of logical channels in chapter 12.

10.2.4 Assumptions

404 There are no additional Assumptions than the Assumptions defined in section 3.4.

10.3 Security Objectives

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

406 The TOE shall provide a "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.

407 The operational environment shall provide a "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.

408 The security objectives O.LogicalChannel and OE.LogicalChannel implement the OSP.LogicalChannel.

10.4 Security Requirements for Package Logical Channel

409 Additional to the Security Functional Requirements for the TOE defined in section 6.1 the TOE shall meet the following SFR.

410 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[392] random number generator **[selection: *PTG.2, PTG.3*] [6] for GET RANDOM** that implements: [assignment: *list of security capabilities* ***of the selected RNG class***].
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***].

411 *Application note 48*: If the TOE will provide random numbers by means of 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 SMC-KT) the provided random numbers shall meet TR-03116 [19] section 3.5. If the command GET RANDOM will be used to seed another deterministic

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

RNG the external device the TOE shall implement RNG of class PTG.2 or PTG.3 for this purpose.

412 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[393].
FIA_USB.1.2/LCs	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[394].
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 reseted, 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*][395].

413 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[396] on (1) the subjects FDP_ACF.1/EF and FDP_ACF.1/MF_**DF,** (2) the objects

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

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

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

396 [assignment: *access control SFP*]

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[397].

414 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 Logical Channel SFP[398] 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"[399].
FDP_ACF.1.2/LC	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) The command MANAGE CHANNEL is [selection: *ALWAYS allowed*, *[assignment*: *supported access control rules]*]. (2) An 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) An subject is allowed to select an object as current object in more than one logical channel if it the security attribute "shareable" is set to "*True*"[400].
FDP_ACF.1.3/LC	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[401].
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[402].

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*]

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

415 *Application note57:* The COS specification [21] claims that the security attribute "shareable" is always "True".

416 The TOE shall meet the requirement "Static attribute initialisation (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[403] to provide restrictive[404] default values for security attributes that are used to enforce the SFP. **After a logical channel is opened the security attributes of the subject associated with this logical channel are set as follows** **(1)** ***currentFolder*** **is root,** **(2)** ***keyReferenceList, globalSecurityList, globalPasswordList, dfSpecificSecurityList, dfSpecificPasswordList bitSecurityList*** **are empty,** **(3)** ***SessionkeyContext.flagSessionEnabled*** **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[405] to specify alternative initial values to override the default values when an object or information is created.

10.5 Security Requirements rationale

417 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 Logical Channel package.

	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

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

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

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

405 [assignment: *the authorised identified roles*]

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

Table 36: Mapping between security objectives for the TOE and SFR for the package Logical Channels

418 Table 36 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.

419 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. This security objective is addressed by the following SFRs:

- FCS_RNG.1/GR providing secure random numbers for external entities, these are the same as using more than one logical channel,
- FIA_USB.1/LC requires that the TSF associates the user authentication state with subjects acting on behalf of that user. Also, the TSF shall enforce rules governing changes of these security attributes by the implementation of commands that perform these changes.
- FDP_ACC.1/LC requires that the TSF enforces an 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 an 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 sharable".
- FMT_MSA.3/LC requires that the TSF assign restrictive security attributes to the subjects of new opened logical channel.

420 The following table lists the required dependencies of the SFRs of this PP package and gives the concrete SFRs from this document which fulfils the required 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

SFR	dependent on	fulfilled by
FMT_MSA.3/LC	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles	FMT_MSA.1/Life, FMT_MSA.1/PIN, FMT_MSA.1/Auth, FMT_SMR.1

Table 37: Dependencies of the SFRs

11 Annex: Composite Evaluation of Smart Cards as Signature Products based on COS Smart Card Platforms (Informative)

421 The TOE of the protection profile in hand may be used as smart card platform for smart cards used as secure signature-creation devices (SSCD) and as parts of signature-creation applications (SCA). The SSCD shall and SCA should be evaluated for approval as signature product according to the German Signature Ordinance [46]. This evaluation may be performed as composite evaluation [8] with a TOE certified conforming to the protection profile in hand as Certified Platform and the object system of the smart card as Application.

422 This informative annex discuss how security targets for such composite evaluation may be written on the examples of the electronic Health Card (eHC), electronic health professional card (eHPC) as SSCD and the secure module cards of KT (gSMC-KT) and K (gSMC-K) as part of SCA. It uses the CEN standards [12], [14] and [15] as protection profiles describing security requirements for SSCD.

423 Note however, that the German Digital Signature Ordinance does not require conformance to any protection profile in order to evaluate a product for qualified digital signatures. Therefore an ST author may also consider relevant contents from one of these PPs without claiming formal conformance.

11.1 Smart Cards as Secure Signature-creation Devices based COS (Informative)

424 The preparation of a smart card as SSCD includes the following steps.

(1) The personalisation as SSCD comprises the definition of the signatory as authorized user of the signature-creation data (SCD) in the SSCD i.e. a private signature key.

(2) The initialization of the SSCD comprises the loading into or generation by the SSCD of the signature key pair. The SSCD shall implement the SCD and should implement the signature verification data (SVD), i.e. the public key e.g. for verification of the digital signature generated with the private key as self-test.

(3) The generation of the qualified certificate by Certification Service Provider for qualified certificates (CSP-QC) containing the SVD which correspond to the SCD under the control of the signatory, the name of the signatory or a pseudonym, which is to be identified as such, 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 SSCD should load certificate info or the certificate into the SSCD for signatory convenience.

425 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 eHC and [23] for eHPC.[406]

[406] Note the smart card platform, the MF and the DF.QES define the security features of the eHC and 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 being stable and independent on updates of the object system specifications.

426 The ST for the eHC and eHPC as SSCD may claim conformance to the protection profile in hand and appropriate SSCD protection profile depending on the method of the initialization and the method of use as SSCD.

11.1.1 eHC as SSCD

427 The eHC are issued by the German health insurance companies to patients insured by them for use health care services. If the patient as cardholder wishes the eHC shall be prepared by a CSP-QC as SSCD where the patient is the signatory.

428 The object system specification of the eHC [22] already specifies in 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 optional Pr.CH.QES.R3072 and Pr.CH.QES.E384,

(3) the EF.C.CH.QES.R2048 and optional additional files for other certificates.

429 The role Signatory is different from role cardholder defined by regular password PIN.CH in MF and the roles defined by multi-reference password referencing to the secret of the PIN.CH.

430 The eHC may be initialized 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 profiles for secure signature creation device — Part 2: Device with key generation, BSI-CC-PP-0059 [12].

(2) The CSP-QC may generate the signature key pair and load the private key as signature-creation data into the SSCD. In this case the ST author should claim conformance to the Protection profiles for secure signature creation device — Part 3: Device with key import, BSI-CC-PP-0075 [13]. The CSP-QC will send the public key to the certificate-generation application in its trusted environment.

(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 trusted channel after delivery of the smart card to the cardholder. In this case the ST author should claim conformance to the Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, BSI-CC-PP-0071 [14].

431 Note the object specification of the eHC [22] does not specifies the access control rule for Pr.CH.QES.x and command GENERATE ASYMMETRIC KEY PAIR and therefore allows for product and CSP-QC specific solutions.

432 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 personalization as SSCD by changing the *transportStatus* to *regularPassword*. The security attribute "*SCD operational*" defined in the SSCD PP [13] and [12] and referenced by conformance claim [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*".

433 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 command PSO COMPUTE DIGITAL SIGNATURE defined in [22] meet the SFR FDP_ACF.1/Signature_Creation as defined in the SSCD PP [12], [13] and [14].

11.1.2 eHPC as SSCD

434 The eHPC is mandatory issued as SSCD. 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 send 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 signature after authentication as signatory.

435 The object system specification of the eHPC [23] already specifies in DF.QES

(1) the user Signatory by means of PIN object PIN.QES,

(2) the signature-creation data as Pr.CH.QES.R2048 (mandatory) and optional Pr.CH.QES.R3072 and Pr.CH.QES.E384,

(3) the EF.C.CH.QES.R2048 and optional files for other certificates.

436 The role Signatory is different from role cardholder defined by regular password PIN.CH in MF and the roles defined by multi-reference password referencing to the secret of the PIN.CH.

437 The eHPC may be initialized 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 profiles for secure signature creation device — Part 2: Device with key generation, BSI-CC-PP-0059 [12].

(2) The CSP-QC may generate the signature key pair and load the private key as signature-creation data into the SSCD. In this case the ST author should claim conformance to the Protection profiles for secure signature creation device — Part 3: Device with key import, BSI-CC-PP-0075 [13]. The CSP-QC will send the public key to the certificate-generation application in its trusted environment.

(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 trusted channel after delivery of the smart card to the cardholder. In this case the ST author should claim conformance to the Protection profiles for secure signature creation device — Part 4:

Extension for device with key generation and trusted communication with certificate generation application, BSI-CC-PP-0071 [14].

438 Note the object specification of the eHPC [23] does not specifies the access control rule for Pr.CH.QES.x and command GENERATE ASYMMETRIC KEY PAIR but leave the access control rule up to the CSP-QS. Because of mandatory initialization of eHPC as SSCD the case (3) is unlikely of practical use for the first SCD but may be considered for update of DF.QES with meaw SCD and corresponding certificates.

439 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 personalization as SSCD by changing the *transportStatus* to *regularPassword*. The security attribute "*SCD operational*" defined in the SSCD PP [13] and [12] and referenced by conformance claim [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*".

440 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 mutual authentication between gSMC-KT as PIN sender and eHPC as PIN receiver and establishing a secure messaging channel between them. Note because the eHPC supports both local PIN entry and remote PIN entry and cannot distinguish between them the eHPC does not enforce secure messaging as PIN receiver for the PIN.QES.

441 The access control rules for the single signature creation function with signature-creation data Pr.CH.QES.R2048, Pr.CH.QES.R3072 and Pr.CH.QES.E384 and command PSO COMPUTE DIGITAL SIGNATURE defined in [23] requires successful authentication with PIN.QES only and meet the SFR FDP_ACF.1/Signature_Creation as defined in the SSCD PP [12], [13] and [14].

442 The access control rules for the batch signature creation function with signature-creation data Pr.CH.QES.R2048, Pr.CH.QES.R3072 and Pr.CH.QES.E384 and command PSO COMPUTE DIGITAL SIGNATURE defined in [23] enforces

(1) successful authentication of the signatory with PIN.QES, and

(2) successful device authentication with CHA 'D2760000400033', i.e. gSMC-K as representative of the SCA of the Konnektor as sender of the data to be signed (DTBS) (cf. chapter 10.2.2 gSMC-K as part of the SCA of the Konnektor for details) and secure messaging with protection of integrity and confidentiality.

443 The security requirements for protected communication between SSCD (with key generation) and SCA are described in the prEN 14169-5:2012: Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, BSI-CC-PP-0072 [15]. The ST writer for TOE as SSCD with key import (cf. [13]) may use the SFR in analogous way.

444 Note the BSI-CC-PP-0072 [15] requires the SSCD or human interface device (i.e. the smart card terminal) to initiate the trusted channel for protection of the signature verification data as required by the method of authentication used (i.e. of confidentiality and integrity in case of PIN), cf. SFR FTP_ITC.1/VAD. Furthermore this PP requires the SSCD to detect manipulation and insertion of

DTBS received, cf. FDP_UIT.1/DTBS, and establishment of trusted channel between SCA and SSCD for signature-creation cf. FTP_ITC.1/DTBS. Therefore the ST writer **cannot** claim conformance to BSI-CC-PP-0072 [15] for the ST describing the eHCP as SSCD.

445 The ST writer shall instead describe more precise security objectives for the operational environment to address optional usage of trusted channel for remote PIN entry like this.

OE.TC_PIN	**Trusted channel for remote PIN entry** The PIN entry device shall authenticate themselves as PIN sender and the TOE as PIN receiver, and send the PIN of the signatory in trusted channel to the TOE.

446 The ST writer may describe more precise security objectives for the TOE and the operational environment and similar but not identical SFR in order

(1) to allow for single signature-creation without trusted channel for DTBS and

(2) to enforce the authentication and the transmission of DTBS in the established trusted channel for as access control condition for batch signature-creation

like these.

447 The TOE shall fulfil the security objective “Batch signature support (O.BatchSignature)” as specified below.

O.BatchSignature	**Batch signature support** The TOE enforces the authentication of SCA and the transmission of DTBS in the established trusted channel for as access control condition for batch signature-creation.

448 The operational environment shall fulfil the security objective “Batch signature control (OE.BatchSignature)” as specified below.

OE.BatchSignature	**Batch signature control** The SCA authenticates themselves to the TOE and transmits the DTBS for batch signature-creation in the established trusted channel to the TOE.

449 The TOE shall meet the requirements “Subset Access Control (FDP_ACC.1)” and “Security attribute based access control (FDP_ACF.1)”as specified below.

450 **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[407] on
1. subjects:
   (a) signatory,
   (b) signature-creation application,
2. objects:
   (a) Signature-creation data PrK.HP.QES,
   (b) DTBS-representation,
3. operations:
   (a) command PSO: COMPUTE DIGITAL SIGNATURE[408].

451 **FDP_ACF.1/BatchSign Security attribute based access control– 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[409] to objects based on the following:
1. subjects:
   (a) human user with authentication status,
   (b) signature-creation application with authentication status,
2. objects:
   (a) Signature-creation data PrK.HC.QES with security attribute *lifeCycleStatus* set to *"Operation state(activated)"*,
   (b) DTBS-representation[410].

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 signatures using PrK.HP.QES with *lifeCycleStatus* set to *"Operation state(activated)"* by means of the command PSO: COMPUTE DIGITAL SIGNATURE in security environment #1
2. the human user successful 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 *"Operation state(activated)"* by means of the command PSO: COMPUTE DIGITAL SIGNATURE in security environment #2[411].

---

407 [assignment: *access control SFP*]

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

409 [assignment: *access control SFP*]

410 [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*]

411 [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[412].
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 "*Operation state(activated)*", 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'[413].

452 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[414] to initiate communication via the trusted channel.
FTP_ITC.1.3/SM_BatchSig	The TSF shall ~~**initiate**~~ **enforce**[415] communication via the trusted channel **with SK4SM** for receiving of commands from the SCA and sending responses to the SCA[416].

453 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 generating the secure messaging keys SK4SM of the TSF (cf [21], chapter 15.4.1).

454 The refinement in the element FPT_ITC.1.3/SM_BatchSig describes that the eHPC uses secure messaging with SK4SM. Note the COS specification distinguishes (simplified) between
(1) secure messaging for smart cards
  (a) verifying the MAC of received commands and decrypting received data and
  (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.

The CC terminology summarizes the communication under the term "trusted channel".

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

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

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

415 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 enforce the trusted channel.

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

11.2 Smart Cards as Part of Signature-creation Application based on COS Smart Card Platforms (Informative)

11.2.1 gSMC-KT as part of Electronic Health Card Terminal

455 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 eHKT is part of the SCA. The eHKT may use 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 DF.KT used for establishing the TLS channel between the eHKT and the Konnektor as describe in the Technical guidance for batch signature creation [18].

The security functionality of trusted channel used by the gSMC-KT is already described in chapter 7 Package Crypto Box.

456 The private key for authentication as PIN sender to the SSCD eHPC is PrK.SMC.AUTD_RPS_CVC.R2048 and PrK.SMC.AUTD_RPS_CVC.E256 for the SMC-KT stored in MF. The authentication reference data are certificates C.SMC.AUTD_RPS_CVC.R2048 and C.SMC.AUTD_RPS_CVC.E256 for the SMC-KT stored also in MF. The establishment of the trusted channel between these smart cards is controlled by the Konnektor. The ST writer may describe the SFR for this trusted channel by means of the component FTP_ITC.1 like this.

457 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 [417] to initiate communication via the trusted channel.
FTP_ITC.1.3/TC_PIN	The TSF shall ~~**initiate**~~ **enforce**[418] communication via the trusted channel **with SK4TC** for sending of PIN commands to the SSCD and receiving responses from the SSCD[419].

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

[418] 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 enforce the trusted channel.

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

458 The private keys PrK.SMKT.AUTD_RPS_CVC.R2048 and PrK.SMKT.AUTD_RPS_CVC.E256 are used for the command PSO DECIPHER by the eHKT. The certificates C.SMKT.AUTD_RPS_CVC.R2048 and C.SMKT.AUTD_RPS_CVC.E256 are used by the external device as authentication reference data for the eHKT.

11.2.2 gSMC-K as part of the SCA of the Konnektor

459 The Konnektor implements a SCA and includes 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. chapter 10.1.2 eHPC as SSCD),

- protected storage of asymmetric key material and other security critical data in DF.KT used for establishing the TLS channel between the eHKT and the Konnektor as describe in the Technical guidance for batch signature creation [18].

The security functionality of trusted channel used by the gSMC-KT is already described in chapter 7 Package Crypto Box.

460 .The private key for authentication gSMC-K as SCA is PrK.SAK.AUTD_CVC.E256 (alternative PrK.SAK.AUTD_CVC.E384) stored in DF.SAK. The authentication reference data are certificates C.SAK.AUTD_CVC.E256 (optional C.SAK.AUTD_CVC.E384) stored also in DF.SAK. The establishment of the trusted channel between these smart cards is controlled by the SCA. The ST writer may describe the SFR for this trusted channel provided by the gSMC-K like this.

461 The trusted channel 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 [420] to initiate communication via the trusted channel.
FTP_ITC.1.3/TC_BatchSig	The TSF shall ~~**initiate**~~ **enforce**[421] communication via the trusted channel **with SK4TC** for sending of commands to the SSCD and receiving responses from the SSCD[422].

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

[421] 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 enforce the trusted channel.

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

12 Acronyms

462 The terminology and abbreviations of Common Criteria version 3.1 [1], [2], [3], Revision 4 and the specification [21] apply.

Acronyms	Term
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	Folder, i.e. Application, Dedicated file and Application Dedicated file
eHC	Electronic health care card (elektronische Gesundheitskarte)
eHCT	Electronic Health Card Terminal
eHPC	Electronic professional card (elektronischer Heilberufsausweis)
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 applications
SCD	Signature creation data
SEF	Structured elementary file
SFP	Security Function Policy
SFR	Security Functional Requirement
SICP	Secure integrated chip platform
SMC-B	Secure modul card type B
SMC-K	Secure modul card type K
SMC-KT	Secure modul card type KT
SPD	Security Problem Definition
SSCD	Secure signature-creation device
SVD	Signature verification data

Acronyms	Term
ST	Security Target
TEF	transparent elementary file
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

13 Bibliography

Common Criteria

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

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

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

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

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

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

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

[8] CC Supporting Document, Composite product evaluation for Smart Cards and similar devices, April 2012, Version 1.2, CCDB-2012-04-001

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

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

Protection Profiles

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

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

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

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

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

Technical Guidelines and Specifications

[16] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents Part1 – eMRTDs with BAC/PACEv2 and EACv1, Part 2, Part 2 – Extended

Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI), Part 3 – Common Specifications, TR-03110, version 2.10, 24.03.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

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

[19] Technische Richtlinie TR-03116, eCard-Projekte der Bundesregierung, Version 3.18 vom 30.01.2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[20] Technische Richtlinie TR-03143 „eHealth G2-COS Konsistenz-Prüftool“ (in Vorbereitung) [423]

[21] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.7.0 vom 26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH einschließlich der Errata zu Release 1.4.0 Online-Rollout (Stufe 1) Erprobung und Produktivbetrieb führt zu Release 1.4.1 vom 02.10.2014 und 2. Errata zu Release 1.4.0 Online-Rollout (Stufe 1) Erprobung und Produktivbetrieb führt zu Release 1.4.2 vom 06.10.2014

[22] Einführung der Gesundheitskarte Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem, Version 3.8.0 vom 26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[23] Einführung der Gesundheitskarte Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem, Version 3.7.0 vom 26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[24] Einführung der Gesundheitskarte Spezifikation der Secure Module Card SMC-B Objektsystem, Version 3.7.0 vom 26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[25] Einführung der Gesundheitskarte Spezifikation der gSMC-K Objektsystem, Version 3.7.0 vom 26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[26] Einführung der Gesundheitskarte Spezifikation gSMC-KT Objektsystem, Version 3.7.0 vom 26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[27] Einführung der Gesundheitskarte Spezifikation Wrapper, actual version[424], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

Cryptography

[28] ISO/IEC 7816-3: 2006 (2nd edition), Identification cards - Integrated circuit cards with contacts Part 3: Electrical interface and transmission protocols

[29] ISO/IEC 7816-4: 2013 (2nd edition) Identification cards - Integrated circuit cards - Part 4: Organisation, security and commands for interchange

[30] ISO/IEC 7816-8: 2004 (2nd edition) Identification cards - Integrated circuit cards- Part 8: Commands for security operations

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

[423] Please note that this Technical Guideline may annually be updated, see www.bsi.bund.de (e.g. Publikationen -> Technische Richtlinien -> Technische Richtlinie fuer die eCard-Projekte der Bundesregierung (BSI TR-03116)).

[424] The version 1.6.0 was actual on 12th of November 2014.

[32] ISO/IEC 9797-1 Information technology - Security techniques - Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher

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

[34] PKCS #1: RSA Cryptography Standard, RSA Laboratories, Version 2.2, October 27, 2012 (http://www.rsa.com/rsalabs/node.asp?id=2125)

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

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

[37] Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2011 February, 11

[38] NIST SP 800-67, Recommandation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, National Institute of Standards and Technology

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

[40] American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, November 16, 2005

[41] Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, March 2010, http://tools.ietf.org/html/rfc5639

[42] ANSI X9.62 Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005

Other Sources

[43] ISO 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards, 2000

[44] ISO 7498-2 (1989): Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture

[45] Law Governing Framework Conditions for Electronic Signatures of 16 May 2001 (Federal Law Gazette I page 876), last amended by Article 4 of the Act of 17 July 2009 (Federal Law Gazette I page 2091)

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

Additional references

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

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