Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Protection Profile
Security Module Card Type A (PP-SMC-A)

Common Criteria

BSI-CC-PP-0019-V2

Approved by the
Federal Ministry of Health

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189, 53175 Bonn ▪ Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 ▪ Fax: +49 (0) 1888 9582-400 ▪ Internet: www.bsi.bund.de

—— this page was intentionally left blank ——

Foreword

This 'Protection Profile — Security Module Card Type A (PP-SMC Type A)' 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 2.3 [1], [2], [3] with final interpretations of the CCIMB.

Correspondence and comments to this Protection Profile — Security Module Card (PP-SMC) should be referred to:

CONTACT ADDRESS

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
D-53175 Bonn, Germany

Tel +49 228 99 9582-0
Fax +49 228 9582-400

Email bsi@bsi.bund.de

NUR FÜR DIE ERARBEITUNGPHASE GÜLTIG

Change history

Version	Date	Reason	Remarks
1.910	1st February 2008	Updated according to HPC specification version 2.1.1	
1.95	29th August 2008	Updated according to HPC specification version 2.3.0	
1.99	13th November 2008		
2.1	9th March 2009	Updated according to the remarks of the evaluator	
2.2	21st April 2009	Updated according to the remarks of the evaluator and BSI	

Last Version: 2.2 (21st April 2009)

Variables

Name	Value	Display
File name and sizes	Set automatically	Protection_Profile_SMC-A_v2.2.doc
Last Version	2.2	2.2
Date	21st April 2009	21st April 2009
Classification	unclassified	unclassified
Authors	Wolfgang Killmann, Dr. Alla Gnedina, Jens Kroder	Wolfgang Killmann, Dr. Alla Gnedina, Jens Kroder

Table of Content

1 PP Introduction

1.1 PP reference

1	Title:	Protection Profile — Security Module Card Type A (PP-SMC-A))
	Sponsor:	Bundesamt für Sicherheit in der Informationstechnik
	Editors:	Wolfgang Killmann, T-Systems GEI GmbH
	CC Version:	2.3
	Assurance Level:	The minimum assurance level for this PP is EAL4 augmented.
	General Status:	final version
	Version Number:	2.2
	Registration:	BSI-CC-PP-0019-V2
	Keywords:	electronic health card, security module card

1.2 PP Overview

2 The protection profile defines the security objectives and requirements for the electronic **Security Module Card Type A** (SMC-A, German: "Sicherheitsmodul-Karte Typ A") based on the regulations for the German health care system. It address the security services provided by this card, mainly:

- Card-to-Card Authentication between the Security Module Card (SMC) and a Health Professional Card (HPC) or an electronic Health Card (eHC) or another Security Module Card with and without establishment of a trusted channel.

1.3 Conformance Claim

3 This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.3, August 2005, CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.3, August 2005, CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.3, August 2005, CCMB-2005-08-003

as follows

- Part 2 extended,
- Part 3 conformant,

- Package conformant to EAL4 augmented with ADV_IMP.2, AVA_MSU.3 and AVA_VLA.4.

2 TOE Description

2.1 TOE definition

4 The Target of Evaluation (TOE) is the Security Module Card Type A. The SMC-A is a contact based smart cards, which is conformant to the specification documents [17], [19]. The physical characteristics shall comply with ISO/IEC 7816-1 and related standards.

5 The **TOE** comprises of

TOE_IC, consisting of :
- the circuitry of the SMC's chip (the integrated circuit, IC) and
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software

TOE_ES
- the IC Embedded Software (operating system)

TOE_APP
- the SMC Type A applications (data structures and their content)

and

TOE_GD
- the guidance documentation delivered together with the TOE.

TOE usage and security features for operational use

6 The **TOE** is used by an institution which is under control of an individual acting as accredited health profession in a health care environment

(1) to support medical assistants, pharmaceutical staff and other persons under control of a health professional using HPC to get access to data eHC,

(2) to support trusted channel in interaction with other smart cards,

7 The **TOE** provides the following main security services:

(1) Access control for the functions (2) to (5) listed below,

(2) Asymmetric card-to-card authentication between the SMC Type A and an eHC, a HPC or a SMC without establishment of a trusted channel,

(3) Asymmetric card-to-card authentication between the SMC Type A and a HPC or SMC with establishment of a trusted channel, possibly with storage of introduction keys,

(4) Support of secure messaging by means encryption of data, decryption of data, generation of MAC and verification of MAC,

(5) Terminal Support Service including random number generation, storage of and cryptographic operation with a private key for TLS protocol ad storage of configuration data and network data.

2.2 TOE usage and security features for operational use

8 The following list provides an overview of the security services provided by the SMC during the usage phase. These security services together with the functions for the initialization and the personalization build the TSF scope of control. In order to refer to these services later on, short identifiers are defined:

9 **Service_Asym_Mut_Auth_w/o_SK**[1]: Authentication of technical user using asymmetric techniques between the SMC, eHC or HPC without agreement of a symmetric key (cf. [17], chapter 15).

This service of the SMC-A includes two independent parts (a) the verification of an authentication attempt of an external entity by means of the commands GET CHALLENGE and EXTERNAL AUTHENTICATE and (b) the command INTERNAL AUTHENTICATE to authenticate themselves to an external entity (cf. to [17], 15.1.2, 15.2 for details). The algorithmic identifier '*rsaRoleCheck*' is used for the command EXTERNAL AUTHENTICATE and '*rsaRoleAuthentication*' is used for the command INTERNAL AUTHENTICATE (cf. for details to [17], section 15).

10 **Service_Asym_Mut_Auth_with_SM**: Mutual Authentication using asymmetric techniques between the SMC-A and a HPC with agreement of symmetric secure messaging keys and establishment of a secure messaging channel after successful authentication as receiver of secured commands and sending of secured responses. The keys of a secure messaging channel are stored temporarily. This service runs a protocol in two linked together parts (a) the command INTERNAL AUTHENTICATE to authenticate themselves to an external entity and (b) the verification of an authentication attempt of an external entity by means of the commands GET CHALLENGE and EXTERNAL AUTHENTICATE (cf. for details to [17], 15.4.4). This service uses the commands INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE with algorithmic identifier '*rsaSessionkey4SM*'.

11 **Service_Asym_Mut_Auth_with_TC**: Mutual Authentication using asymmetric techniques between the SMC-A and a HPC, SMC or eHC[2], with establishment of a trusted channel keys after

[1] The Abbreviation SK here stands for symmetric key used for establishing Secure Messaging, which is the card security protocol realising a trusted channel.

[2] Note the agreement of introduction keys is intended for smart cards often working together as SMC-A and HBA but not eHC. Nevertheless this combination is possible. The SMC specification [19], sec. 6.3.11, states "PrK.SMC.AUTR_CVC is the global private key for C2C-authentication between SMC/eGK" and in table 78 the algid "rsaRoleAuthentication, rsaSessionkey4SM" are defined. Typically only rsaRoleAuthentication

successful authentication. The TOE supports secure messaging by means encryption of data, decryption of data, generation of MAC and verification of MAC.

This service of the SMC-A runs a protocol in two linked together parts (a) the command INTERNAL AUTHENTICATE to authenticate themselves to an external entity and (b) the verification of an authentication attempt of an external entity by means of the commands GET CHALLENGE and EXTERNAL AUTHENTICATE (cf. for details to [17], 15.4.4). This service uses the commands INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE with algorithmic identifier '*rsaSessionkey4TC*' (cf. for details to [17], section 15) to establish symmetric keys of type *desSessionkey4TC* for PSO: ENCIPHER, PSO: DECIPHER, PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM and PSO: VERIFY CRYPTOGRAPHIC CHECKSUM.

12 **Service_Asym_Mut_Auth_with_Intro**: Mutual Authentication using asymmetric techniques between the HPC and a SMC-A with storage of introduction keys after successful authentication (cf. for details to [18], sec 6.1.4).

This service is meant for situations, where the SMC-A frequently interacts with a manageable number of HPCs, SMC-Bs and SMC-Ks. In the context of the so called "Round of introduction" a mutual authentication with negotiation of session keys is executed; these sessions keys will be stored in a persistent way as „Introduction Keys" after successful authentication. The agreed introduction keys belong individually to the corresponding authentication keys. The CHR of the involved certificate is stored as key reference after adjusting the index (first byte of CHR) to the computed key material. This service runs a protocol similar to the Service_Asym_Mut_Auth_with_SM, but the algorithmic identifier is '*rsaSessionkey4Intro*' for both authentication commands (cf. for details to [18], section 7.1.3) in order to request storage of the resulting keys. The authentication related data contain data elements for key computation. The symmetric introduction keys, which are stored this way, will be used as the asymmetric keys for agreement of symmetric trusted channel keys that were involved in the authentication procedure. Thus, an introduction object inherits certain information of the public key certificate as well as security-related properties of the private key.

13 **Service_Sym_Mut_Auth_with_TC**: Mutual Authentication using symmetric techniques between the SMC-A[3] and an external entity with establishment of symmetric keys for secure massaging, where the TOE is the sender of the secured commands and the receiver of the secured responses.

If the TOE and a certain SMC have been introduced to each other before, i.e. had performed Service_Asym_Mut_Auth_with_Intro, then both cards can perform a symmetric authentication by using the shared introduction keys. During a successful symmetric authentication the security

---

will be used. "rsaSessionkey4SM" makes no sense because the eHC cannot send secure messaging commands. It should be "rsaSessionkey4TC" in order to generate secured command for the eHC as reciever.

[3] Note the SMC specification [19], sec. 6.3.11, states "PrK.SMC.AUTR_CVC is the global private key for C2C-authentication between SMC/eGK" and in table 78 the algid "rsaRoleAuthentication, rsaSessionkey4SM" are defined. But "rsaSessionkey4SM" makes no sense because the eHC cannot send secure messaging commands. It should be "rsaSessionkey4TC" in order to generate secured command for the eHC.

status “Successful verification of the SMC role identifier” is set, since the verified role identifier, the used key identifier and the access rule of the private key have been assigned to the introduction keys during the successful asymmetric authentication.

According to the protocol of this service, there are two versions of command sequences: (i) for SMC/eHC communication (cf. [17], sec. 15.4.1) (ii) SMC/HPC communication (cf. [17], sec. 15.4.2). For SMC/eHC communication the command MUTUAL AUTHENTICATE with algorithmic identifier ‘*desSessionkey4TC*‘ is received by the eHC to authenticate the SMC, to authenticate itself to the eHC and simultaneously to agree the session keys. For SMC/HPC communication firstly the command INTERNAL AUTHENTICATE with algorithmic identifier set to ‘*desSessionkey4TC*‘ (by MSE) is received by the SMC to authenticate itself to an external entity and simultaneously determine a random number, which is included in the response data. Secondly the verification of an authentication attempt of an external entity is done by means of the command EXTERNAL AUTHENTICATE with algorithmic identifier ‘*desSessionkey4TC*’.

A successful verification sets in the HPC and the SMC the security status “CHA with role ID 'xx' successfully presented”. A trusted channel has been established, i.e. data can be transferred to the HPC and the SMC in secure messaging mode.

14 **Service_SM_Support**: The SMC-A service intermediates between an application communication in plain text and a remote smart card (e.g. HPC) communicating by means of secure messaging or encryption or using MAC. The TOE provides (i) the encryption of plaintext with the secure messaging encryption key by means of command PSO.ENCIPHER, (ii) the decryption of cipher text with the secure messaging encryption key by means of command PSO.DECIPHER, (iii) the MAC generation, i. e. the production of secured commands with cryptographic checksum data objects and with cryptogram data objects using the secure messaging encryption key by means of command PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM, and (iv) the MAC verification i. e. processing of secured responses where these keys are established by card-to-card authentication with the secure messaging MAC key by means of command PSO: VERIFY CRYPTOGRAPHIC CHECKSUM.[4]

15 **Service_Sym_Mut_Auth_with_SM**: Mutual Authentication using symmetric techniques between the SMC-A and an external entity with establishment of symmetric keys for secure massaging, where the TOE is the receiver of the secured commands and sending secured responses.

If the SMC-A and a certain other SMC have been introduced to each other before, i.e. had performed Service_Asym_Mut_Auth_with_Intro, then both cards can perform a symmetric authentication by using the shared introduction keys. During a successful symmetric authentication the security status “Successful verification of the SMC role identifier” is set, since the verified role identifier, the used key identifier and the access rule of the private key have been assigned to the introduction keys during the successful asymmetric authentication.

According to the protocol of this service, firstly the command INTERNAL AUTHENTICATE with algorithmic identifier set to ‘*desSessionkey4SM*‘ (by MSE) is received by the SMC to

[4] Note the use of ENVELOP command is optional (cf. [19], sec. 5.9.6 and 5.9.7, and therefore not addressed in this protection profile.

authenticate itself to an external entity and simultaneously determine a random number, which is included in the response data. Secondly the verification of an authentication attempt of an external entity is done by means of the command EXTERNAL AUTHENTICATE with algorithmic identifier '*desSessionkey4SM*'.

A successful verification sets in the SMC the security status "CHA with role ID 'xx' successfully presented". A trusted channel has been established, i.e. data can be transferred to the SMC in secure messaging mode.

16 **Terminal Support Service**: The SMC-A provides random number generation for the operational environment.

17 In detail the functionality of the SMC-A is defined in the specifications:

Specification German Health Professional Card and Security Module Card - Part 1: Commands, Algorithms and Functions of the COS Platform, Version 2.3.0, 04.07.2008, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychotherapeuten-kammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft

Specification German Health Professional Card and Security Module Card - Part 3: SMC Applications and Functions, Version 2.3.0, 04.07.2008, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychotherapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft

18 **Application note 1:** The TOE may provide an additional service for symmetric authentication e.g. as described in [18] for communication between SMC and server which is mentioned as option for the communication between the SMC and the Card Application Management System. The SMC specification [17] and [19] does not specify a Card Application Management System for the SMC administration in the Phase 7 "Smartcard End-usage". Therefore such functionality is not addressed in this PP but the card initialisation and personalisation by a Card Management System. It is up to the security target writer to include additional functions in the security target if necessary for the Phase 7 "Smartcard End-usage".

2.3 TOE life cycle

19 The following description is a short summary of the SMC life cycle model based on a common model normally used for smart cards. The TOE life cycle is described in terms of the seven life cycle phases as usually defined for smart cards, see for example the SSVG-PP [**Fehler! Textmarke nicht definiert.**]. They are summarized in the following table.

Phase		Description
1	**Smartcard Embedded Software Development**	The **Smartcard Embedded Software Developer** is in charge of • the development of the Smartcard Embedded Software of the TOE, • the development of the TOE related Applications

		• the specification of the IC initialisation and pre-personalisation requirements (though the actual data for the IC initialisation and pre-personalisation come from Phase 4, 5 resp. 6). The purpose of the Smartcard Embedded Software and Applications designed during phase 1 is to control and protect the TOE and its different configurations during phases 4 to 7 (product usage).The global security requirements of the TOE are such that it is mandatory during the development phase to anticipate the security threats of the other phases.
2	**IC Development**	The **IC Designer** • designs the IC, • develops the IC Dedicated Software, • provides information, software or tools to the Smartcard Embedded Software Developer, and • receives the Smartcard Embedded Software from the developer through trusted delivery and verification procedures. From the IC design, IC Dedicated Software and Smartcard Embedded Software, the **IC Designer** • constructs the smartcard IC database, necessary for the IC photomask fabrication.
3	**IC Manufacturing and Testing**	The **IC Manufacturer** is responsible for • producing the IC through three main steps: - IC manufacturing, - IC testing, and - IC pre-personalisation. The **IC Mask Manufacturer** • generates the masks for the IC manufacturing based upon an output from the smartcard IC database.
4	**IC Packaging and Testing**	The **IC Packaging Manufacturer** is responsible for • the IC packaging (production of modules) and • testing.
5	**Smartcard Product Finishing Process**	The **Smartcard Product Manufacturer** is responsible for • the initialisation of the TOE (in form of the initialisation of the modules of phase 4) and • its testing. The smartcard product finishing process comprises the embedding of the initialised modules for the TOE and the card production what may be done alternatively by the Smartcard Product Manufacturer or by his customer

		(e. g. Personaliser or Card Issuer)**.**
6	**Smartcard Personalisation**	The **Personaliser** is responsible for • the smartcard personalisation and • final tests. The personalization of the smart card includes the printing of the (cardholder specific) visual readable data onto the physical smart card, and the writing of (cardholder specific) TOE User Data and TSF Data into the smartcard.
7	**Smartcard End-usage**	The **Smartcard Issuer** is responsible for • the smartcard product delivery to the smartcard end-user (the cardholder), and the end of life process. • The authorized personalization agent (Card Management System) are allowed to add data, modify or delete an SMC application. • The TOE is used as SMC by the smartcardholder in the Operational use phase

Table 1: Smart Card Life Cycle Overview

20 The following paragraphs describe, how the application of the CC assurance classes is related to these phases.

21 The CC do not prescribe any specific life cycle model. However, in order to define the application of the assurance classes, the CC assume the following implicit life cycle model consisting of three phases:

- TOE development (including the development as well as the production of the TOE),
- TOE delivery,
- TOE operational use.

22 For the evaluation of the SMC the phases 1 up to 4 as defined in Table 1 are part of the TOE development in the sense of the CC. The phases 6 and 7 are part of the operational use in the sense of the CC. The phase 5 may be part of one of these CC phases or may be split between them depending on the specific model used by the TOE developer. The writer of the ST shall define the exact boundary. However, this Protection Profile requires that the following conditions have to be met:

23 All executable software in the TOE has to be covered by the evaluation. This is one of the reasons to include the assurance component ADV_IMP.2.

24 The data structures and the access rights to the health application data as defined in the SMC specification [17] are covered by the evaluation.

25 If the Card Management System or the card issuer load data onto the smartcard in the phase 7 Smartcard End-usage these data shall be non-executable only.

26 **Application note 2**: The following examples and remarks may help ST writers to define the boundary of TOE development.

a. The following variations for the boundary of the TOE development are acceptable:

- Phase 5 completely belongs to the TOE development, i.e. the TOE is delivered as an IC already embedded in the plastic card and containing all software and at least the data structures as defined in the specification [19].

- The TOE is delivered as an initialised module, i.e. it contains all software and at least the data structures as defined in the specification [19], but isn't embedded in a plastic card yet.

- The TOE is delivered in (at least) two parts: The hardware as a module or already embedded in a plastic card on the one hand and a file containing parts of the initialisation data on the other hand. Both parts together again contain all software and at least the data structures as defined in the specification [19] (which in particular means that all of this is evaluated during ADV activities). In this case the evaluation must also show as a result that the functions used by the customer (Card Management System / card issuer) for loading the initialisation data into the hardware provide sufficient protection against modification and (where applicable) disclosure of these data.

b. The following remarks may show how some CC assurance activities apply to parts of the life cycle[5]:

- The ALC and ACM classes, which deal with security measures in the development environment of the TOE apply to all development and production environments of Phases 1 up to 4 and those parts of Phase 5 belonging to TOE development as defined in the ST for a TOE. In particular the sites, where the software of the TOE is developed as well as the hardware development and production sites are subject to these CC classes (for example with regard to site visits). In the context of a composite evaluation some of the phases may already be covered by a IC hardware evaluation.

- The measures for delivery of the TOE to the Card Management System / card issuer are subject to ADO_DEL.

- If the third model described in a. above is used (delivery of hardware and initialisation file), the loading of the initialisation data can be interpreted as part of installation, generation and start-up and is therefore covered by ADO_IGS.

[5] These activities already follow from the CC definitions. Therefore it is not necessary to define them as refinements to the CC assurance components. However these explicit notes may serve as a help for ST writers and TOE developers to understand the connection between the life cycle model and some CC requirements.

- The guidance documentation delivered by the TOE developer as part of the TOE delivery procedures are covered by AGD and ADO_IGS. Since the Card Management System / card issuer is the first "user" of the TOE after delivery, the guidance documentation is mainly directed to him. He may be defined as the administrator of the TOE or as a special user role. Since the guidance documentation in particular needs to describe all measures necessary for secure use of the TOE, it needs to contain information on the following issues:
  - Secure handling of the personalisation of the TOE
  - Secure handling of delivery of the personalised TOE from the Card Management System / card issuer to the cardholder.
  - Security measures for end-usage, which the Card Management System / card issuer needs to communicate to the cardholder. A simple example for this may be the requirement for the cardholder, to handle his PIN(s) securely. Since the documents accompanying the card during transport from card issuer to cardholder will probably not be available at the time of evaluation, the guidance documents for the Card Management System / card issuer need to contain this information connected with the requirement that the card issuer covers all such issues in his delivery documents.

3 Security Problem Definition

27 The Security Problem Definition (SPD) is the part of a PP, which describes

- **assets**, which the TOE shall protect,
- **subjects**, who are users (human or system) of the TOE or who might be threat agents (i. e. attack the security of the assets)
- **Operational security policies**, which describe overall security requirements defined by the organisation in charge of the overall system including the TOE. In particular this may include legal regulations, standards and technical specifications.
- **threats** against the assets, which shall be averted by the TOE together with its environment
- **assumptions** on security relevant properties and behaviour of the TOE's environment

3.1 Introduction

Assets

28 The assets to be protected by the TOE and its environment are as follows

29 Table 2: Assets of the SMC-A

Name of asset	Description	Operation by commands[6]
Certificate Service Provider self-signed Certificate (C.CA_SMC.CS)	The certificate of the Certificate Service Provider for card verifiable certificates in the health care environment C.CA_SMC.CS containing the public key PuK.CA_SMC.CS for verification of the card verifiable certificates like C.SMC.AUTR_CVC. It is part of the user data provided for the convenience of the IT environment.	SELECT, READ BINARY
Card Authentication Private Keys for role authentication (PrK.SMC.AUTR_CVC)	The Card Authentication Private Key PrK.SMC.AUTR_CVC is an asymmetric cryptographic key used for the card-to-card authentication of a SMC-A to a eHC on behalf of the cardholder. It is part of the TSF data.	INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE
Card Verifiable Authentication Certificates for role authentication (C.SMC.AUTR_CVC)	Card verifiable certificate C.SMC.AUTR_CVC for the Card Authentication Public Keys PuK.SMC.AUTR_CVC as authentication reference data corresponding to the Authentication Private Key PrK.SMC.AUTR_CVC and used for the card-to-card authentication of the SMC-A to the eHC with or without establishing a trusted channel by means of secure messaging. It contains encoded access rights (Role ID for SMC profile 2 to 6[7]) and is signed by the SMC-A card issuer. It is part of the user data provided for use by external entities as authentication reference data of the SMC. It is stored in the file EF.C.SMC.AUTR_CVC, which integrity shall be protected.	SELECT, READ BINARY
Card Authentication	The Card Authentication Private Key	INTERNAL

[6] All other access methods are forbidden (access right is set to NEVER).

[7] Note the profiles are assign informative only, cf. [22].

Name of asset	Description	Operation by commands[6]
Private Keys as remote PIN sender (PrK.SMC.AUTD_RPS_CVC)	PrK.SMC.AUTD_RPS_CVC is an asymmetric cryptographic key used for the card-to-card authentication of a SMC to a HPC or another SMC or RFID as remote PIN sender. It is part of the TSF data.	AUTHENTICATE, EXTERNAL AUTHENTICATE
Card Verifiable Authentication Certificates as remote PIN sender (C.SMC.AUTD_RPS_CVC)	Card verifiable certificate C.SMC.AUTD_RPS_CVC for the Card Authentication Public Keys PuK.SMC.AUTD_RPS_CVC as authentication reference data corresponding to the Authentication Private Key PrK.SMC.AUTD_RPS_CVC and used for the card-to-card authentication of the SMC to a HPC or another SMC or RFID as remote PIN sender with establishing a trusted channel by means of secure messaging.. It contains encoded access rights (Role ID for SMC as PIN sender: profile 54) and is signed by the SMC card issuer. It is part of the user data provided for use by external entities as authentication reference data of the HPC. It is stored in the file EF.C.SMC.AUTD_RPS_CVC, which integrity shall be protected.	SELECT, READ BINARY
EF.ATR	The transparent file EF.ATR contains a constructed data object for indication of I/O buffer sizes and the DO 'Pre-issuing data' relevant for CAMS services.	SELECT, READ BINARY
EF.DIR	EF.DIR contains the application templates for MF, DF.SMA, and DF.KT according to ISO/IEC 7816-4.	SELECT, READ RECORD, SEARCH RECORD, APPEND RECORD, UPDATE RECORD
EF.GDO	EF.GDO contains the DO ICC Serial Number.	SELECT, READ BINARY
EF.VERSION	The EF.Version with linear fixed record structure contains the version	SELECT, READ RECORD, SEARCH RECORD,

Name of asset	Description	Operation by commands[6]
	numbers of the specification, which the card is compliant to.	UPDATE RECORD
EF.SMD	EF.SMD contains SMC-A related data, e.g. special configuration data.	SELECT, READ BINARY, UPDATE BINARY, ERASE BINARY
C.SMKT.CA	C.SMKT.CA is the X.509 certificate of the Certification Authority (CA) which is the issuer of the X.509-certificate C.SMKT.AUT.	SELECT, READ BINARY
C.SMKT.AUT	C.SMKT.AUT contains the X.509 certificate for authentication of the card terminal to a specific con¬nec¬tor	SELECT, READ BINARY
PrK.SMKT.AUT	PrK.SMKT.AUT is the private authentication key for connecting the card terminal to a specific con¬nec¬tor.	PSO: DECIPHER, INTERNAL AUTHENTICATE
Random number	Random number generation	GET RANDOM

30 Table 3: TSF data of the SMC-A

TSF data	Description	Operation in terms of commands
Root Public Key of the Certificate Service Provider (PuK.RCA.CS)	The public key PuK.RCA.CS of the Health Care Root CA for verification of the card verifiable certificate of the certificate service provider for card verifiable certificates in the health care environment (cf. to [19], sec. 5.3.11, for details). It is part of the TSF data which integrity shall be protected.	PSO: VERIFY CERTIFICATE
PuK.CAMS_SMC.-AUT_CVC	PuK.CAMS_SMC.AUT_CVC (optional) is the public key for performing an asymmetric SMC/CAMS authentication procedure (with TC establishment).	EXTERNAL AUTHENTICATE

TSF data	Description	Operation in terms of commands
TOE initialization data	Data stored in the TOE during the initialization process. It is part of the TSF data.	
TOE personalization data	Data stored in the TOE during personalization process. It contains user data and TSF data.	

31 **Application note 3:** The Public Key for CV Certification Verification (PuK.CA_SMC.CS) is used as authentication reference by TSF for card authentication. The Card Authentication Private Keys (PrK.SMC.AUT) is used as a cryptographic key by the TOE security services provided to the user. Therefore they are assessed as user data.

Subjects

32 This protection profile considers the following subjects:

Name of subject	Description
Card Management System	Person(s) responsible for the manufacturing and personalization of the TOE for the Cardholder a.
Cardholder	Person for whom the SMC is personalized and which controls the use of the SMC.
Smart card in the role HPC, SMC or eHC	A Health Professional Card (HPC), Security Module Card (SMC) or electronic Health Card (eHC) is authenticating themselves to the TOE by means of card-2-card authentication with a card verifiable certificate with corresponding cardholder authorisation (CHA) of HPC/SMC/eHC of a specific area defining its access rights.
Terminal	External entity communicating with the TOE without successful authentication by sending commands to the TOE and receiving responses from the TOE according to ISO/IEC 7816 .
Unauthorized subject	All subjects who is trying to interact with the TOE as Card Management System or HPC without being authenticated for this role.

Table 4: Subjects

33 **Application note 4:** The smart cards in the health care environment possess card verifiable certificate (CVC) with cardholder authorizations (CHA) identifying them as HPC or SMC of a

specific environment as defined in [17], Chapter 7. The CHA of SMC is defined in [18], Annex A.3.

3.2 Organisational Security Policies

34 OSPs will be defined in the following form:

OSP.name Short Title

Description.

35 The TOE and its environment shall comply to the following organization security policies (which are security rules, procedures, practices, or guidelines imposed by an organization upon its operations, see CC part 1, sec. 3.2).

36 **OSP.SMC_Spec Compliance to SMC specifications**

The SMC shall be implemented according to the specifications:

Specification German Health Professional Card and Security Module Card - Part 1: Commands, Algorithms and Functions of the COS Platform, Version 2.3.0, 04.07.2008, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychotherapeuten-kammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft

Specification German Health Professional Card and Security Module Card - Part 3: SMC Applications and Functions, Version 2.3.0, 04.07.2008, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychotherapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft

37 **OSP.Manufact Manufacturing of the Smart Card**

The IC Manufacture and Card Manufacture ensure the quality and integrity of the manufacturing process and control the smart card material in the Phase 3, 4 and 5.

3.3 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 TOE method of use in the operational environment and the assets stored in the TOE.

39 Threats will be defined in the following form:

T.name Short Title

Description.

3.3.1 Threats mainly addressing TOE_ES and TOE_APP

40 The TOE shall avert the threats, which are application and operating system oriented, as specified below.

41 **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 independent on or listening the communication between a terminal with the TOE.

This threat comprises several attack scenarios e.g. reconstruction the private decipher key using the response code for chosen cipher texts (like Bleichenbacher attack for the SSL protocol implementation).

42 **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.

43 **T.Misuse Misuse of TOE functions**

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

The attacker may try alter the TSF data e.g. to extend the user rights after successful card-to-card authentication.

44 **T.Intercept Interception of Communication**

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

This threat comprises several attack scenarios. The Health Professional using the TOE reads from and writes onto eHC data like medication or medical data which an attacker may read or forge during transmission.

3.3.2 Threats mainly addressing TOE_IC and TOE_ES

45 **T.Abuse_Func Abuse of Functionality**

An attacker with high attack potential may use functions of the TOE which shall not be used in TOE operational phase in order (i) to disclose or manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or manipulate TSF Data.

This threat address attacks using the IC as production material for the smart card and using function for personalization in the operational state after delivery of the smart card.

46 **T.Information_Leakage Information Leakage from smartcard**

An attacker with high attack potential may exploit information which is leaked from the TOE during its usage in order to disclose confidential data (User Data or TSF data). The information leakage may be inherent in the normal operation or caused by the attacker.

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. No direct contact with the IC internals is required here. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

47 **T.Malfunction Malfunction due to Environmental Stress**

An attacker with high attack potential may cause a malfunction of TSF or of the IC Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify security functions of the IC Embedded Software.

This may be achieved e.g. by operating the IC outside the normal operating conditions, exploiting errors in the IC Embedded Software or misuse of administration function. To exploit this an attacker needs information about the functional operation.

48 **T.Phys_Tamper Physical Tampering**

An attacker with high attack potential may perform physical probing of the IC in order (i) to disclose User Data, (ii) to disclose/reconstruct the IC Embedded Software or (iii) to disclose TSF data. An attacker may physically modify the IC in order to (i) modify security features or functions of the IC, (ii) modify security functions of the IC Embedded Software, (iii) to modify User Data or (iv) to modify TSF data.

The physical tampering may be focused directly on the discloser or manipulation of TOE User Data (e.g. the document decipherment key) or TSF Data (e.g. authentication key of the smart card) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the IC internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

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 will be defined in the following form:

A.name Short Title

Description.

51 **A.Pers_Agent Personalization and management of the smartcard**

The Card Management System performs the personalisation and additional management steps correctly during the end-usage phase according to the specifications [17], [19] and ensures the correctness, the quality and - if necessary - the confidentiality of all data structures and data on the card.

52 **A.Users Adequate usage of TOE and IT-Systems**

The cardholder of the TOE uses the TOE adequately. In particular he doesn't hand the card to unauthorised persons. The Card Management System and the health professionals use their data systems according to the overall system security requirements.

4 Security Objectives

53 This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

4.1.1 Security Objectives for the TOE

54 This section describes the security objectives for the TOE address the aspects of identified threats to be countered by the TOE and organisational security policies to be met by the TOE.

55 Objectives for the TOE will be defined in the following form

OT.name short title

Description of the objective.

56 The security objectives describe the protection of the primary assets as User Data and the secondary assets as TOE security functions data (TSF data) against threats identified in TOE environment. The security objectives as mutual supporting set ensure protection against attacks with high attack (even though not mentioned separately for each security objective).

57 **OT.AC_Pers Access control for personalization and management**

The TOE must ensure that the User data and the TSF data can be created, written and updated by authorized Card Management system only.

58 **OT.Data_Confident Confidentiality of internal data**

The TOE must ensure the confidentiality of the Card Authentication Private Keys, the Client-Server Authentication Private Key, and other confidential user data and TSF data under the TSF scope of control.

59 **OT.Data_Integrity Integrity of internal data**

The TOE must ensure the integrity of the Health Professional Data, User Authentication Reference Data, the Card Authentication Private Keys, the Client-Server Authentication Private Key, the Public Key for CV Certification Verification, the Card Verifiable Authentication Certificates, the Certificate Service Provider self-signed Certificate, and other user data and TSF data under the TSF scope of control.

60 **OT.TSS Terminal support service**

The TOE provides service random number generation for the operational environment by means of command GET RANDOM and storage of and cryptographic operation with private keys for TLS protocol for card terminals to all users.

61 **OT.Trusted_Channel Trusted Channel**

The TOE establishes a trusted channel for protection of the confidentiality and integrity of the transmitted data between the TOE and the successful authenticated smart card on demand of the external application. The TOE supports other smart cards and applications to use the secure messaging by providing the security service the Service_SM_Support.

62 **OT.AC_Serv Access Control for TOE Security Services**

The TOE provides the TOE security services Service_Asym_Mut_Auth_w/o_SK, Service_Asym_Mut_Auth_with_SM, Service_Asym_Mut_Auth_with_TC, Service_Asym_Mut_Auth_with_Intro, Service_Sym_Mut_Auth_with_TC, Service_SM_Support, Service_Sym_Mut_Auth_with_SM and the Terminal Support Service.

63 **OT.Prot_Abuse_Func Protection against abuse of functionality**

The TOE prevent that functions intended for the testing, the initialization and the personalization of the TOE and which must not be accessible after TOE delivery can be abused in order (i) to disclose critical User Data, (ii) to manipulate critical User Data of the Smart Card Embedded Software, (iii) to manipulate Soft-coded Smart Card Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

64 **OT.Prot_Inf_Leak Protection against information leakage**

The TOE must provide protection against disclosure of confidential data (User Data or TSF data) stored and/or processed in the TOE. This includes protection against attacks by means of

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines (side channels) and
- by forcing a malfunction of the TOE (e.g. fault injection) and/or
- by a physical manipulation of the TOE.

65 **Application note 5:** This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

66 **OT.Prot_Malfunction Protection against Malfunctions**

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. The TOE will preserve a secure state to prevent errors and deactivation of security features of functions. The environmental conditions include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, and temperature.

67 **Application note 6:** A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Phys-Manipulation) provided that detailed knowledge about the TOE´s internals.

68 **OT.Prot_Phys_Tamper Protection against physical tampering**

The TOE must provide protection the confidentiality and integrity of the User Data, the TSF Data, and the IC Embedded Software. This includes protection against attacks with high attack potential by means of

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

- reverse-engineering to understand the design and its properties and functions.

69 **Application note 7:** In order to meet the security objectives OT.Prot_Phys_Tamper the TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack. This is addressed by the security objective OD.Assurance.

4.1.2 Security Objectives for the Development and Manufacturing Environment

70 This chapter describes the security objectives for the development and manufacturing environment. These security objectives result in assurance requirements for the TOE (see section 6.2 Security Assurance Requirements for the TOE)

71 Security objectives for the Development and Manufacturing Environment will be defined in the following form

OD.name short title

Description of the objective.

72 **OD.Assurance Assurance Security Measures in Development and Manufacturing Environment**

The developer and manufacture ensure that the TOE is designed and fabricated so that it requires a combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through attack. The developer provides necessary evaluation evidence that the TOE fulfils its security objectives and is resistant against attack with high attack potential.

73 **OD.Material Control over Smart Card Material**

The IC Manufacture, the Card Manufacture and the Card Management System must control all materials, equipment and information to produce, to initialise, to pre-personalize genuine smart card materials and to personalize authentic smart cards in order to prevent counterfeit of the TOE.

4.1.3 Security Objectives for the Operational Environment

74 Security objectives for the operational environment will be defined in the following form

OE.name short title

Description of the objective.

75 The following objectives for the operational environment correspond directly to the assumptions in section 3.4 Assumptions.

76 **OE.Perso** **Secure personalization and management**

All data structures and data on the card produced during personalisation or additional administration steps during the end-usage phase must be performed correctly according to the specifications [17] [19] and are handled correctly regarding integrity and confidentiality of these data. The Card management system ensure (i) the generation of the card-to-card authentication keys stored on smart card and the distribution of the corresponding public key in form of CV certificates, (ii) writing the public key for verification of CV certificates for card-to-card authentication. This includes in particular sufficient cryptographic quality of cryptographic keys (in accordance with the cryptographic algorithms specified for the SMC) and their confidential handling.

77 **OE.Users** **Adequate usage of TOE and IT-Systems**

The cardholder of the TOE needs to use the TOE adequately. In particular he must not hand the card to unauthorised persons. The Card Management System and the health professionals must use their data systems according to the overall system security requirements.

5 Extended Components Definition

78 This protection profile uses components defined as extensions to CC part 2. Some of these components are defined in [**Fehler! Textmarke nicht definiert.**], other components are defined in this protection profile.

5.1 Definition of the Family FCS_RNG

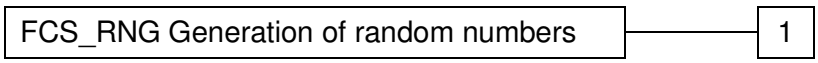
79 To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This extended family FCS_RNG describes SFR for random number generation used for cryptographic purposes.

80 The family “Generation of random numbers (FCS_RNG)” is specified as follows.

FCS_RNG Generation of random numbers

Family behaviour This family defines quality requirements for the generation of random numbers, which are intended to be use for cryptographic purposes.

81 Component levelling:



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

82 Management: FCS_RNG.1

There are no management activities foreseen.

83 Audit: FCS_RNG.1

There are no actions defined to be auditable.

84 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, physical hybrid, deterministic hybrid*] random number generator, which implements: [assignment: *list of security capabilities*].

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

5.2 Definition of the Family FIA_API

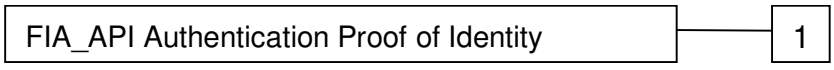
85 To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external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

86 The family "Authentication Proof of Identity (FIA_API)" is specified as follows.

FIA_API Authentication Proof of Identity

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

87 Component levelling:



FIA_API.1 Authentication Proof of Identity.

88 Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

89 Audit: FIA_API.1

There are no actions defined to be auditable.

90 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: *authorized user or rule*].

5.3 Definition of the Family FMT_LIM

91 To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

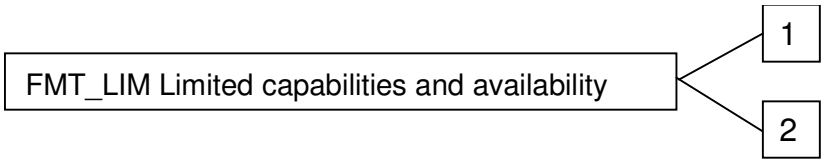
92 The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



FMT_LIM.1 Limited capabilities require that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

93 Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

94 Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

95 The TOE Functional Requirement "Limited capabilities (FMT_LIM.1)" is specified as follows.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

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

Dependencies: FMT_LIM.2 Limited availability.

96 The TOE Functional Requirement "Limited availability (FMT_LIM.2)" is specified as follows.

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

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

Dependencies: FMT_LIM.1 Limited capabilities.

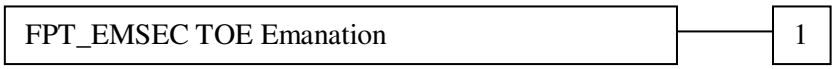
5.4 Definition of the Family FPT_EMSEC

97 The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.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_EMSEC.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

Dependencies: No dependencies.

6 Security Requirements

98 The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of part 2 of the CC. Each of these operations is used in this PP.

99 The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is (i) denoted by the word “refinement” in bold text and the added/changed words are in bold text, or (ii) included in text as underlined text and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

100 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. 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 *italicized*.

101 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. 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 *italicized*.

102 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.

6.1 Security Functional Requirements for the TOE

103 This section on security functional requirements (SFR) for the TOE is divided into sub-section following the main security functionality. They are usually ordered like CC part 2 [2].

104 **Application note 8:** The following table provides an overview how the security services (listed in section 2.2 TOE usage and security features for operational use) match to the SFRs.

Security Service	SFR	Comment
Card-to-card authentication	FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_RNG.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FMT_MTD.1/RAD_WR, FMT_MTD.1/RAD_MOD, FIA_ATD.1, FIA_API.1	Card-to-card authentication according to [17], Annex E, - verification of digital signatures of certificates according to ISO 9796-2 (without random numbers) - RSA with private key for INTERNAL AUTHEN-TICATE and RSA with public key for EXTERNAL AUTHEN-TICATE with DSI according [17], Chapter 15
Authorization of SMC-A for access to data on eHC	FDP_ACC.1, FDP_ACF.1, FIA_UAU.4	Access control for the certificate with special encoded access rights to open the eHC
Secure messaging	FCS_CKM.1, FCS_CKM.4, FCS_RNG.1, FCS_COP.1/3TDES, FCS_COP.1/RMAC,	Secure messaging key generation is described in [17], Chapter 15 and secure messaging encryption and MAC is described in [17],

Security Service	SFR	Comment
	FDP_UCT.1, FDP_UIT.1	Chapter 13.

Table 5: Overview of SFRs used to describe the TOE security services

6.1.1 Cryptographic support (FCS)

105 The cryptographic algorithms implemented in the TOE shall meet the TR-03116 [6] and [29]. The ST writer shall iterate the relevant SFR components if the TOE supports the optional cryptographic algorithms described in [17].

6.1.1.1 Basic Algorithms

106 The TOE shall meet the requirement "Quality metric for random numbers (FCS_RNG.1)" as specified below (Common Criteria Part 2 extended).

107 **FCS_RNG.1 Quality metric for random numbers**

Hierarchical to: No other components.

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, physical hybrid, deterministic hybrid*][8] random number generator, which implements: [assignment: list of security capabilities]9.

FCS_RNG.1.2 The TSF shall provide random numbers that meet
1. each output 128 bit random number has at least an entropy of 100 bit.
2. [assignment: *other defined quality metrics*][10].

Dependencies: No dependencies.

108 **Application note 9:** This SFR requires the TOE to generate random numbers used for (i) the key agreement FCS_CKM.1 / Asym_Auth and FCS_CKM.1 / Sym_Auth for secure messaging and (ii) the terminal support service using the command GET RANDOM. The quality metric shall be chosen to resist attacks with high attack potential. With respect to the applied scheme it may also be necessary to evaluate the RNG in accordance to the 'AIS 20' [27] or 'AIS 31', [28].

---

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

9 [assignment: *list of security capabilities*]

10 [assignment: *a defined quality metric*]

109 The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

110 **FCS_COP.1/SHA Cryptographic operation – Hash Algorithm**

Hierarchical to: No other components.

FCS_COP.1.1/ SHA	The TSF shall perform hashing [11] in accordance with a specified cryptographic algorithm SHA-256 [12] and cryptographic key sizes none [13] that meet the following: FIPS 180-2 [14].

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
FMT_MSA.2 Secure security attributes

111 **Application note 10:** This SFR requires the TOE to implement the hash functions SHA-256 (256 bit hash value) as the cryptographic primitive of the authentication mechanism according to [17].

112 **FCS_COP.1/CCA_SIGN Cryptographic operation – Digital Signature-Creation for Card-to-Card Authentication**

Hierarchical to: No other components.

FCS_COP.1.1/ CCA_SIGN	The TSF shall perform digital signature-creation [15] in accordance with a specified cryptographic algorithm [selection RSA_ISO9796_2_DS1_SIGN, RSASSA_PSS_SIGN] [16] and cryptographic key sizes 2048 bit module length [17] that meet the following: [17] [18].

[11] [assignment: *list of cryptographic operations*]
[12] [assignment: *cryptographic algorithm*]
[13] [assignment: *cryptographic key sizes*]
[14] [assignment: *list of standards*]
[15] [assignment: *list of cryptographic operations*]
[16] [assignment: *cryptographic algorithm*]
[17] [assignment: *cryptographic key sizes*]
[18] [assignment: *list of standards*]

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

113 **Application note 11:** This SFR requires the TOE to implement the RSA for the cryptographic primitive of the digital signature-creation for the card-to-card authentication mechanism (i.e. INTERNAL AUTHENTICATE) according to [17].

114 **FCS_COP.1/CCA_VERIF Cryptographic operation – Digital Signature-Verification for Card-to-Card Authentication**

Hierarchical to: No other components.

FCS_COP.1.1/ CCA_VERIF: The TSF shall perform digital signature-verification [19] in accordance with a specified cryptographic algorithm RSA_ISO9796_2_DS1_VERIFY [20] and cryptographic key sizes 2048 bit module length[21] that meet the following: [17] [22].

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
FMT_MSA.2 Secure security attributes

115 **Application note 12:** This SFR requires the TOE to implement the RSA for the cryptographic primitive of the digital signature-verification for the card-to-card authentication mechanism (i.e. INTERNAL AUTHENTICATE) according to [17].

116 **FCS_COP.1/3TDES Cryptographic operation – 3TDES Encryption / Decryption**

Hierarchical to: No other components.

FCS_COP.1.1/ TDES: The TSF shall perform encryption and decryption [23] in accordance with a specified cryptographic algorithm 3TDES in CBC mode [24] and cryptographic key sizes 168 bit [25] that meet the following: FIPS 46-3 [8] and [17] [26].

---

19 [assignment: *list of cryptographic operations*]

20 [assignment: *cryptographic algorithm*]

21 [assignment: *cryptographic key sizes*]

22 [assignment: *list of standards*]

23 [assignment: *list of cryptographic operations*]

24 [assignment: *cryptographic algorithm*]

25 [assignment: *cryptographic key sizes*]

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 FMT_MSA.2 Secure security attributes s

117 **Application note 13:** This SFR requires the TOE to implement the cryptographic primitive for encrypting data to be transmitted using secure messaging and for the Service_SM_Support. The key is agreed between the TSF according to the FIA_UAU.4.

118 **FCS_COP.1/RMAC Cryptographic operation – Retail MAC**

Hierarchical to: No other components.

FCS_COP.1.1/ MAC	The TSF shall perform generation and verification of message authentication code [27] in accordance with a specified cryptographic algorithm Retail MAC [28] and cryptographic key sizes 168 bit [29] that meet the following: ANSI X9.19 with DES and [17], Section 6.6 [30].

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 FMT_MSA.2 Secure security attributes

119 **Application note 14:** This SFR requires the TOE to implement the cryptographic primitive for calculating message authentication code over data to be transmitted using secure messaging and for the Service_SM_Support. The key is agreed or defined as the key for secure messaging encryption.

6.1.1.2 Cryptographic key generation (FCS_CKM.1)

120 The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2).

---

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

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

[28] [assignment: *cryptographic algorithm*]

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

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

121 **FCS_CKM.1/Asym_Auth Cryptographic key generation - Asymmetric card-to-card authentication with key agreement**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.1.1/ Asym_Auth: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm mutual asymmetric card-to-card authentication with key agreement using RSA and SHA-256 with algorithmic identification rsaSessionkey4Intro and rsaSessionkey4SM [31] and specified cryptographic key sizes 168 bit[32] that meet the following: [6], [17] [33].

122 **Application note 15:** The **asymmetric** card-to-card authentication with key agreement [17], chap. 15, is used for **Service_Asym_Mut_Auth_with_Intro** with algorithmic identification rsaSessionkey4Intro and **Service_Asym_Mut_Auth_with_SM**. with algorithmic identification rsaSessionkey4SM. The TOE is equipped with its Card Authentication Private Key and has received and verified the Card Authentication Public Key of the communication partner. The key agreement method is the same for both algorithmic identification rsaSessionkey4Intro and rsaSessionkey4SM but result in symmetric keys for different usage: (i) introduction keys are permanently stored in the TOE and used for symmetric authentication (with or without symmetric key agreement), and (ii) temporarily stored symmetric secure messaging keys, where SMK.ENC and SMK.MAC are different. The introduction keys may be used further on for **Service_Sym_Mut_Auth_with_SM** according to FCS_CKM.1/Sym_Auth and symmetric internal or external authentication. The **symmetric** card-to-card authentication with key agreement is used for **Service_Sym_Mut_Auth_with_SM**. The algorithms use the random numbers generated by TSF as required by FCS_RNG.1.

123 **FCS_CKM.1/Sym_Auth Cryptographic key generation - Symmetric authentication key**

Hierarchical to: No other components.

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

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

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

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.1.1/ Sym_Auth: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm symmetric mutual card-to-card authentication with key agreement 3TDES and SHA-256 [34] and specified cryptographic key sizes 168 bit[35] that meet the following: [6], [17] [36].

124 **Application note 16:** The TOE may be equipped with symmetric secret introduction keys being agreed upon before (cf. [19], sec. 5.9.3) and agrees on secure messaging keys which are used for encryption and message authentication. The algorithms use the random number generated by TSF as required by FCS_RNG.1.

125 The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2).

126 **FCS_CKM.4 Cryptographic key destruction**

Hierarchical to: No other components.

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

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]
FMT_MSA.2 Secure security attributes

127 **Application note 17:** The TOE shall destroy the Triple-DES encryption key (SMK.ENC) and the Retail-MAC message authentication keys (SMK.MAC) for secure messaging after reset or termination of secure messaging session or reaching fail secure state according to FPT_FLS.1.

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

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

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

6.1.2 Identification and Authentication

6.1.2.1 User attribute definition (FIA_ATD.1)

128 The TOE shall meet the requirement "User attribute definition (FIA_ATD.1)" as specified below (Common Criteria Part 2).

129 **FIA_ATD.1 User attribute definition**

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:
(1) identity and role of entities authenticated with introduction keys[37].

Dependencies: No dependencies.

130 **Application note 18:** The component FIA_ATD.1 applies to the card-to-card authentication where the identity (i.e. the ICCSN.ICC) and the role (i.e. Role ID) are encoded in the CHA of the CV certificate (cf. [17] Chapter 7 for details).

6.1.2.2 Timing of identification (FIA_UID.1)

131 The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (Common Criteria Part 2).

132 **FIA_UID.1 Timing of identification**

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow
(1) reading the ATR
(2) reading EF.ATR, EF.DIR, EF.GDO, EF.SMD, EF.VERSION and EF containing certificates EF.C.*.*,
(3) reading security status information using command GET SECURITY STATUS KEY,
(4) execution of the command GET RANDOM,
(5) [assignment: *list of TSF-mediate actions*] [38]
on behalf of the user to be performed before the user is identified.

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

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

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.

Dependencies: No dependencies.

133 **Application note 19:** The ST writer shall perform the missing operation in FIA_UID.1.1. According to the specification [19] the list of data objects with read access condition includes but is not limited to the Card Verifiable Authentication Certificates and the X.509 Certificates. The card management system may create DF and EF in MF and DF, and define their access conditions.

6.1.2.3 Timing of authentication (FIA_UAU.1)

134 The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria Part 2).

135 **FIA_UAU.1 Timing of authentication**

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow

(1) reading the ATR

(2) reading EF.ATR, EF.DIR, EF.GDO, EF.SMD, EF.VERSION and EF containing certificates EF.C.*.*,

(3) reading security status information using command GET SECURITY STATUS KEY,

(4) execution of the command GET RANDOM,

(5) identification by providing the users certificate,

(6) [assignment: *list of TSF mediated actions*][39]

on behalf of the user to be performed before the user is authenticated.

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

Dependencies: FIA_UID.1 Timing of identification.

136 **Application note 20:** The ST writer shall perform the missing operation in FIA_UAU.1.1. According to the specification [19] the list of data objects with read access condition includes but is not limited to the Health Professional Data, the Card Verifiable Authentication Certificates and the X.509 Certificates. The card management system may create DF and EF in MF and DF and define their access conditions.

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

6.1.2.4 Single-use authentication mechanisms (FIA_UAU.4)

137 The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

138 **FIA_UAU.4 Single-use authentication mechanisms**

Hierarchical to: No other components.

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) secure messaging channel[40].

Dependencies: No dependencies.

139 **Application note 21:** The command EXTERNAL AUTHENTICATE may be used as part of the mutual card-to-card authentication mechanisms Service_Asym_Mut_Auth_w/o_SK, and Service_Asym_Mut_Auth_with_SM or independent on mutual authentication. It uses the fresh generated by the TOE random data RND.ICC (see also FCS_RNG.1) as challenge to prevent reuse of a response generated in a successful authentication attempt.

140 The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2).

141 **FIA_UAU.5 Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

(1) execution of the command EXTERNAL AUTHENTICATE as part of the Service_Asym_Mut_Auth_w/o_SK,

(2) execution of the command EXTERNAL AUTHENTICATE as part of the Service_Asym_Mut_Auth_with_SM,

(3) execution of the command EXTERNAL AUTHENTICATE as part of

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

the Service_Sym_Mut_Auth_with_SM,

(4) secure messaging channel[41]

to support user authentication.

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

(1) The TSF shall authenticate the Security Module Card with Root Public Key of the Certificate Service Provider and Card verifiable certificate with a corresponding cardholder authorization of SMC [42].

142 The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2).

143 **FIA_UAU.6 Re-authenticating**

Hierarchical to: No other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions successful established secure messaging as receiver of commands [43].

Dependencies: No dependencies.

144 **Application note 22:** The specification [17] states in section 13.1.1.2 item (N341): "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 (i.) flagSessionEnabled MUST be set to the value noSK, (ii.) the security status of the key that was involved in the negotiation of the ses-sion keys MUST be deleted by means of clearSecurityStatus(...)."

145 **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 with PrK.SMC.AUTR_CVC[44] to prove the identity of the role SMC[45]
(2) **INTERNAL AUTHENTICATE with PrK.SMC.AUTD_RPS_-CVC to prove the identity of the PIN sender.**

---

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

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

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

Application note 23: The refinement adds a list of authentication mechanisms and roles as defined in clause 1 for FIA_API.1.1 (instead of iteration of the component).

6.1.3 Access Control

6.1.3.1 Subset Access Control (FDP_ACC.1)

146 The following Security Function Policy (SFP) **SMC Access Control SFP** is defined by the requirements "Subset Access Control (FDP_ACC.1)", "Security attribute based access control (FDP_ACF.1)", "Import of user data without security attributes (FDP_ITC.1)", "Basic data exchange confidentiality (FDP_UCT.1)" "Data exchange integrity (FDP_UIT.1)" and "Static attribute initialisation (FMT_MSA.3)**"**..

"The TOE provides the security services with private keys for the Cardholder only. The TOE protects the communication with the outside world in confidentiality and integrity on demand of the IT environment."

147 The TOE shall meet the requirement "Complete Access Control (FDP_ACC.1)" as specified below (Common Criteria Part 2).

148 **FDP_ACC.1 Subset Access Control**

Hierarchical to: No other components.

[44] [assignment: *authentication mechanism*]

[45] [assignment: *authorized user or rule*]

FDP_ACC.1.1 The TSF shall enforce the SMC Access Control SFP [46] on

1. the subjects
   (a) the Card Management System,
   (b) the HPC/SMC,
   (c) the eHC,
   (d) (unauthorised) Terminal and
2. the objects
   (a) MF, DF.KT and DF.SMA
   (b) Global Data Object (EF.GDO),
   (c) EF.ATR,
   (d) EF.DIR
   (e) EF.VERSION
   (f) EF.C.SMKT.CA and EF.C.SMKT.AUT
   (g) SMC related Data (EF.SMD),
   (h) Card Authentication Private Keys (PrK.SMC.AUTR_CVC, and PrK.SMC.AUTD_RPS_CVC),
   (i) Card Terminal to Connector Authentication Private Key for connecting (PrK.SMKT.AUT)
   (j) Card Verifiable Certificates (EF.C.SMC.AUTR_CVC, EF.C.SMC.AUTD_RPS_CVC, and EF.C.CA_SMC.CS),
   (k) PuK.CAMS_SMC.AUT_CVC
   (l) PuK.RCA.CS
3. operations by commands defined in table 2[47].

Dependencies: FDP_ACF.1 Security attribute based access control

149 **Application note 24:** The subjects and objects are described in section 3.1 Introduction. The public key for CV certificate verification (PuK.RCA.CS) is TSF data.

6.1.3.2 Security attribute based access control (FDP_ACF.1)

150 The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2).

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

[47] [assignment: *list of subjects and objects*]

151 **FDP_ACF.1 Security attribute based access control**

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the SMC Access Control SFP[48] to objects based on the following: authentication status of user [49].

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

1. the (unauthorised) Terminal is allowed
   (a) to select the MF, DF.KT, and DF.SMA by the means of the command SELECT
   (b) to read by means of commands SELECT and READ BINARY the EF.ATR, EF.GDO, EF.SMD, EF.C.SMKT.CA, and EF.C.SMKT.AUT,
   (c) to read by means of commands SELECT, READ RECORD and SEARCH RECORD the EF.DIR and EF.VERSION,
   (d) to read by means of commands SELECT and READ BINARY the Card Verifiable Authentication Certificates (EF.C.CA_SMC.CS, EF.C.SMC.AUTR_CVC, and EF.C.SMC.AUTD_RPS_CVC),
   (e) to execute the command EXTERNAL AUTHENTICATE with PrK.SMC.AUTR_CVC, PrK.SMC.AUTD_RPS_CVC, and PuK.CAMS_SMC.AUT_CVC,
   (f) to execute the command INTERNAL AUTHENTICATE with PrK.SMKT.AUT,
   (g) to execute the command PSO: VERIFY CERTIFICATE with PuK.RCA.CS,
   (h) to execute the command PSO: DECIPHER with PrK.SMKT.AUT,
   (i) to execute the command GET RANDOM
2. a successful authenticated HPC is allowed
   (a) to execute the command INTERNAL AUTHENTICATE using with PrK.SMC.AUTR_CVC,
   (b) to execute the commands UPDATE BINARY and ERASE BINARY with EF.SMD
   (c) to perform all actions a terminal is allowed to perform.

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

[49] [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*]

3. a successful authenticated CAMS is allowed
   (a) to execute the command LOAD APPLICATION with MF and DF.SMA,
   (b) to execute the command UPDATE RECORD with EF.DIR and EF.VERSION,
   (c) to execute the command APPEND RECORD with EF.DIR,
   (d) to perform all actions a terminal is allowed to perform.
4. a successful authenticated HPC/SMC is allowed
   (a) to execute the command INTERNAL AUTHENTICATE with PrK.SMC.AUTD_RPS_CVC,
   (b) to perform all actions a terminal is allowed to perform.[50].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[51].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rule:no other access than defined in FDP_ACF.1.2 to the objects listed in FDP_ACC.1.1 is allowed to any subject[52]

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

152 The TOE shall meet the requirement "Import of user data without security attributes (FDP_ITC.1)" as specified below (Common Criteria Part 2).

153 **FDP_ITC.1 Import of user data without security attributes**

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the SMC Access Control SFP [53] when importing user data, controlled under the SFP, from outside of the TSC.

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

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

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

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

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *additional importation control rules*].

154 The TOE shall meet the requirement "Residual Information Protection (FDP_RIP.1)" as specified below (Common Criteria Part 2).

155 **FDP_RIP.1 Residual Information Protection**

Hierarchical to: No other components.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *[assignment: allocation of the resource to, deallocation of the resource from]* the following objects: *[assignment: list of objects at least including, secret and private cryptographic keys, data in all files, which are not freely accessible]*[54].

Dependencies: No dependencies.

156 **Application note 25**: 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 de-allocation and those which can be deleted upon allocation. Note that the SSCD-PP requires deletion of secret signature keys upon de-allocation and that this is advisable for all PINs and secret/private cryptographic keys in general. For secret user data deletion upon allocation should be sufficient (depending on the resistance of the concrete TOE against physical attacks).

157 The TOE shall meet the requirement "Stored Data Integrity (FDP_SDI.2)" as specified below (Common Criteria Part 2).

158 **FDP_SDI.2 Stored Data Integrity**

Hierarchical to: FDP_SDI.1.

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

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for integrity errors[55] on all objects, based on the following attributes: *[assignment: user data attributes – the attributes shall be chosen in a way that at least the following data are included:*

- *cryptographic keys,*
- *security relevant status variables of the card (e. g. authentication status for mutual authenticate)*
- *user data in files on the card,*
- *file management information (like access rules for files), and*
- *the card life cycle status]*[56].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall

1. Prohibit the use of the altered data,
2. inform the connected entity about integrity error[57].

Dependencies: No dependencies.

159 **Application note 26:** The writer of the Security Target may want to use iterations of FDP_SDI.2, for example in order to distinguish between different types of data (compare the SSCD-PP, where this is done for persistent data on the one hand and other data on the other hand).

6.1.3.3 Inter-TSF-Transfer

160 **Application note 30:** FDP_UCT.1, FDP_UIT.1 require the TOE to protect User Data transmitted between the TOE and a connected device by secure messaging with encryption and message authentication codes after successful authentication of the remote device. The authentication mechanisms as part of the Card-to-Card Authentication Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging. The rules for the data transfer are defined in the security policy SMC Access Control SFP defined in the preceding section.

161 The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

162 **FDP_UCT.1 Basic data exchange confidentiality**

Hierarchical to: No other components.

[55] [assignment: *integrity errors*]

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

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

FDP_UCT.1.1 The TSF shall enforce the SMC Access Control SFP [58] to be able to transmit and receive[59] objects in a manner protected from unauthorised disclosure.

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]

163 **Application note 27**: The SMC-A supports secure messaging with TDES encryption (cf. SFR FCS_COP.1/3TDES) after card-to-card authentication.

164 The TOE shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below (Common Criteria Part 2).

165 **FDP_UIT.1 Data exchange integrity**

Hierarchical to: No other components.

FDP_UIT.1.1 The TSF shall enforce the SMC Access Control SFP [60] to be able to transmit and receive [61] user data in a manner protected from modification, deletion, insertion and replay [62] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [63] has occurred.

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]

166 **Application note 28**: The SMC-A supports secure messaging with MAC (cf. FCS_COP.1/RMAC) after card-to-card authentication.

---

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

59 [selection: *transmit, receive*]

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

61 [selection: *transmit, receive*]

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

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

167 The TOE shall meet the requirement "Inter-TSF trusted channel (FTP_ITC.1)" as specified below (Common Criteria Part 2).

168 **FTP_ITC.1 Inter-TSF trusted channel**

Hierarchical to: No other components.

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote 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	The TSF shall permit the remote trusted IT product [64] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for commands and responses after successful card-to-card authentication with SM key agreement[65].

Dependencies: No dependencies.

169 **Application note 29:** The specification [17], Chapter 13 and 15, describes the use of secure messaging as trusted channel. The remote trusted IT product (may be a security module of SMC or a HPC) may initiate the trusted channel using Service_Asym_Mut_Auth_with_SM. The TOE enforces secure messaging after asymmetric card-to-card authentication with algorithm 'rsaSessionkey4SM' (i.e. Service_Asym_Mut_Auth_with_SM). If the external entity sent any command in plain the security status of the HPC/SMC reached after this authentication is lost and the secure messaging keys deleted.

6.1.4 Security Management

170 **Application note 30**: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

171 The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2).

172 **FMT_SMF.1 Specification of Management Functions**

Hierarchical to: No other components.

---

64 [selection: *the TSF, the remote trusted IT product*]

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

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

1. Initialization,
2. Personalization,
3. Card management,[66].

Dependencies: No Dependencies

173 The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below (Common Criteria Part 2).

174 **FMT_SMR.1 Security roles**

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles Manufacturer, Personalisation Agent, Card Management system, HPC/SMC [67].

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

Hierarchical to: FIA_UID.1 Timing of identification

175 **Application note 31**: The Certificate Holder authorization (CHA) Role ID are defined in [18], annex A.3.

176 **Application note 32**: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases. The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

(A) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced

or conversely

(B) the TSF is designed with high functionality but is removed or disabled in the product in its user environment.

The combination of both requirements shall enforce the policy.

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

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

177 The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

178 **FMT_LIM.1 Limited capabilities**

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks [68].

Dependencies: FMT_LIM.2 Limited availability.

179 The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

180 **FMT_LIM.2 Limited availability**

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks [69].

Dependencies: FMT_LIM.1 Limited capabilities.

181 The TOE shall meet the requirement "**Secure security attributes** (FMT_MSA.2)" as specified below (Common Criteria Part 2).

182 **FMT_MSA.2 Secure security attributes**

Hierarchical to: No other components.

Dependencies: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes

[68] [assignment: *Limited capability and availability policy*]

[69] [assignment: *Limited capability and availability policy*]

FMT_SMR.1 Security roles

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

183 The TOE shall meet the requirement "Static attributes initialisation (FMT_MSA.3)" as specified below (Common Criteria Part 2).

184 **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 SMC Access Control SFP [70] to provide restrictive[71] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the none[72] to specify alternative initial values to override the default values when an object or information is created.

185 The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

186 **FMT_MTD.1/INI Management of TSF data – Writing of Initialization Data and Pre-personalization Data**

Hierarchical to: No other components.

FMT_MTD.1.1/ INI The TSF shall restrict the ability to write [73] the Initialization Data and Pre-personalization Data [74] to the Manufacturer [75].

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

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

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

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

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

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

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

187 **FMT_MTD.1/RAD_WR Management of TSF data – Writing of Authentication Reference Data**

Hierarchical to: No other components.

FMT_MTD.1.1/ RAD_WR: The TSF shall restrict the ability to write [76] the
1. public keys of the root for CV certificate verification [77]
to the Personalisation Agent [78].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

188 **FMT_MTD.1/RAD_MOD Management of TSF data – Modification of Authentication Reference Data**

Hierarchical to: No other components.

FMT_MTD.1.1/ RAD_MOD: The TSF shall restrict the ability to modify [79] the public keys of the root for CV certificate verification [80] to nobody [81].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

6.1.5 SFR for TSF Protection

189 The TOE shall prevent inherent and forced illicit information flow for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect

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

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

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

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

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

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

to forced leakage they have to be considered in combination with the security functional requirements "Failure with preservation of secure state (FPT_FLS.1)" and "TSF testing (FPT_TST.1)" on the one hand and "Resistance to physical attack (FPT_PHP.3)" on the other. The SFR "Non-bypassability of the TSP (FPT_RVM.1)" and "TSF domain separation (FPT_SEP.1)" together with "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" and "Resistance to physical attack (FPT_PHP.3)" prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

190 The TOE shall meet the requirement "**TOE Emanation** (FPT_EMSEC.1)" as specified below (CC extended):

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.1.1 The TOE shall not emit [*assignment: types of emissions*] in excess of [assignment: *specified limits*] enabling access to

1. none[82]

and

2. Card Authentication Private Keys,
3. secure messaging keys [83].

FPT_EMSEC.1.2 The TSF shall ensure any authorized user [84] are unable to use the following interface smart card circuit contacts [85] to gain access to

1. none[86]

and

2. Card Authentication Private Key,
3. secure messaging keys [87].

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

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

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

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

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

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

Dependencies: No dependencies..

191 **Application note 33**: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The SMC-A has to provide a smart card interface with contacts according to ISO/IEC 7816-2 [26] but the integrated circuit may have additional contacts or a contactless interface as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

192 The following security functional requirements address the protection against forced illicit information leakage.

193 The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (Common Criteria Part 2).

194 **FPT_FLS.1 Failure with preservation of secure state**

Hierarchical to: No other components.

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 [88].

Dependencies: ADV_SPM.1 Informal TOE security policy model

195 The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2).

196 **FPT_PHP.3 Resistance to physical attack**

Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing [89] to the TSF [90] by responding automatically such that the TSP is not violated.

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

Dependencies: No dependencies.

197 **Application note 34**: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

198 The following security functional requirements support the separation and the protection of TSF.

199 The TOE shall meet the requirement "Non-bypassability of the TSP (FPT_RVM.1)" as specified below (Common Criteria Part 2).

200 **FPT_RVM.1 Non-bypassability of the TSP**

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

201 The TOE shall meet the requirement "TSF domain separation (FPT_SEP.1)" as specified below (Common Criteria Part 2).

202 **FPT_SEP.1 TSF domain separation**

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

203 **Application note 35**: Those parts of the TOE which support the security functional requirements "TSF testing (FPT_TST.1)" and "Failure with preservation of secure state (FPT_FLS.1)" shall be protected from interference of the other security enforcing parts of the SMC-A chip Embedded Software. The security enforcing functions and health application data shall be separated in way preventing any inference.

---

89 [assignment: *physical tampering scenarios*]

90 [assignment: *list of TSF devices/elements*]

204 The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria Part 2).

205 **FPT_TST.1 TSF testing**

Hierarchical to: No other components.

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

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Dependencies: FPT_AMT.1 Abstract machine testing.

206 **Application note 36**: If SMC chip uses state of the art smart card technology it will run the some self tests at the request of the authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the "authorised user" Card Management system in the Phase 2 Manufactoring. Other self tests may run automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 Operational Use, e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks. The security target writer shall perform the operation claimed by the concrete product under evaluation.

6.2 Security Assurance Requirements for the TOE

207 The security assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ADV_IMP.2, AVA_MSU.3 and AVA_VLA.4.

208 The minimum strength of function is SOF-high. This protection profile does not contain any security functional requirement for which an explicit strength of function claim is required.

6.3 Security Requirements for the IT environment

209 This protection profile do not describe security functional requirements for the IT environment.

7 Rationale

210 All security objectives for the environment of the TOE are of the non-IT (organisational) type and hence need not to be met by security requirements for the IT environment.

211 The explicitly stated security requirements are taken form the Security IC Platform Protection Profile, Version 1.0, 15.06.2007; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0035 [15]. This PP provides a justification why the SFRs FCS_RNG.1 and FMT_LIM.1 resp. FMT_LIM.2 defined in chapter 5 Extended Components Definition are necessary to address smart card specific security functional requirements. This justification is valid for the current PP as well. The extended family FCS_RNG describes SFR for random number generation used for cryptographic purposes. The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

212 The definition of the family FPT_EMSEC is taken from the *Protection Profile Secure Signature Creation Device* [16], chapter 6.6.1. This family describes the functional requirements for the limitation of intelligible emanations. The TOE shall prevent attacks against secret data 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, radio emanation etc. Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data. Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

213 The family FIA_API is defined to describe the functional requirements for the proof of the claimed identity for the authentication verification by an external entity. The other families of the class FIA address the verification of the identity of an external entity. This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment. Therefore the FIA_API.1 is defined to provide a INTERNAL AUTHENTICATE with different keys to prove the identity of the different authorized users or rules.

7.1 Security Objectives Rationale

	OT.AC_Pers	OT.AC_Serv	OT.Data_Confident	OT.Data_Integrity	OT.TSS	OT.Trusted_Channel	OT.Prot_Abuse_Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys_Tamper	OD.Assurance	OD.Material	OE.Perso	OE.Users
T.Compromise_Internal_Data			x											
T.Forge_Internal_Data				x										
T.Misuse	x	x	x	x										
T.Intercept						x								
T.Abuse_Func							x							
T.Information_Leakage								x						
T.Malfunction									x					
T.Phys_Tamper										x				
OSP.SMC_Spec	x	x	x	x	x	x						x	x	
OSP.Manufact											x	x		
A.Pers_Agent													x	
A.Users														x

Table 1: Security Objective Rationale

214 The treat **T.Compromise_Internal_Data** "Compromise of confidential User or TSF data" address the compromise of internal confidential data through the communication interface of the TOE independent on or listening the communication between a terminal with the TOE. This threat is directly achieved by security objectives **OT.Data_Confident** "Confidentiality of internal data" requiring the protection of the confidential user data and TSF data.

215 The protection against the treat **T.Forge_Internal_Data** "Forge of User or TSF data" is directly achieved by the security objective **OT.Data_Integrity** "Integrity of internal data" requiring the protection of the integrity of the user data and the TSF data.

216 The threat **T.Misuse** "Misuse of TOE functions" addresses the use of TOE functions without knowledge of user authentication data or any implicit authorization. The protection against this treat is mainly achieved by the security objective **OT.AC_Pers** "Access control for personalization and management" protecting the personalization functions of the TOE, **OT.AC_Serv** "Access Control for TOE Functions" for the security services used in the operational usage phase. The security objectives **OT.Data_Confident** "Confidentiality of internal data" and **OT.Data_Integrity** "Integrity of internal data" ensure the protection of the assets independent on the TOE functionality used by the attack.

217 The threat **T.Intercept** "Interception of Communication" is countered by the security objective **OT.Trusted_Channel** "Trusted Channel". Note that according to the **OSP.SMC_Spec**

"Compliance to HPC specifications" and the security objective for the TOE environment **OE.Users** "Adequate usage of TOE and IT-Systems" the external application decides whether the transmitted data are sensitive and require the protection in the confidentiality and integrity. If the application selects the security environment SE #2 (cf. the specification [19]) the TOE will protect transmitted data. If the application selects the security environment SE #1 the TOE is not required to protect the data transmitted after card-to-card authentication because they are not sensitive.

218 The threat **T.Abuse_Func** "Abuse of Functionality" is adverted directly by the security objective **OT.Prot_Abuse_Func** "Protection against abuse of functionality" preventing the use of TOE functions which are intended for the testing, the initialization and the personalization of the TOE and which must not be accessible after TOE delivery.

219 The threat **T.Information_Leakage** "Information Leakage from smart card chip" is adverted directly by the security objective **OT.Prot_Inf_Leak** "Protection against information leakage" addressing the protection against disclosure of confidential data (User Data or TSF data) stored and/or processed in the TOE by attacks including but not limited to use of side channels, fault injection or physical manipulation.

220 The threat **T.Malfunction** "Malfunction due to Environmental Stress" is adverted directly by the security objective **OT.Prot_Malfunction** "Protection against Malfunctions".

221 The threat **T.Phys_Tamper** "Physical Tampering" is adverted directly by the security objective **OT.Prot_Phys_Tamper** "Protection against physical tampering".

222 The organizational security policy **OSP.SMC_Spec** "Compliance to SMC specifications" is implemented by the TOE security objectives **OT.AC_Pers** "Access control for personalization and management", **OT.TSS** "Terminal support service**", OT.Trusted_Channel** "Trusted Channel**", OT.AC_Serv** "Access Control for TOE Functions", **OT.Data_Confident** "Confidentiality of internal data", **OT.Data_Integrity** "Integrity of internal data" and **OT.Trusted_Channel** "Trusted Channel" and the security objectives for the TOE environment **OD.Material** "Control over Smart Card Material" and **OE.Perso** "Secure personalization and management". The TOE security objectives OT.AC_Pers, OT.Dig_Sign, OT.Dec_Trans, OT.DS_CSA, OT.TSS and OT.Trusted_Channel implement the security services of the TOE and their related user data and TSF data as specified in [19] referenced in the OSP.SMC_Spec. OT.AC_Serv OT.Data_Confident and OT.Data_Integrity protect the services against misuse, the confidentiality and the integrity of the user data and the TSF data. The security objectives for the environment OD.Material and OE.Perso ensure that the Card Management System will provide genuine TOE initialized and personalized according to specification [19] to the cardholder.

223 The security objectives for the environment **OD.Assurance** "Assurance Security Measures in Development and Manufacturing Environment" and **OD.Material** "Control over Smart Card Material" implement the organisational security policy **OSP.Manufact** "Manufacturing of the Smart Card" in the development and manufacturing of the TOE.

224 The security objectives for the environment **OE.Perso** "Secure personalization and management" implements the assumption **A.Pers_Agent** "Personalization of the Smart Card" with respect of the concrete user and TSF data described in the specification [17] and [19] (cf. to OSP.SMC_Spec).

225 The security objectives for the environment **A.Users** "Adequate usage of TOE and IT-Systems" implements directly the assumption **OE.Users** "Adequate usage of TOE and IT-Systems".

7.2 Security Requirements Rationale

7.2.1 Security Requirements Coverage

226 The following table shows, which SFRs for the TOE support which security objectives of the TOE. The table shows, that every objective is supported by at least one SFR and that every SFR supports at least one objective.

	OT.AC_Pers	OT.AC_Serv	OT.Data_Confident	OT.Data_Integrity	OT.TSS	OT.Trusted_Channel	OT.Prot_Abuse_Func	OT.Prot_Inf_Leak	OT.Prot?Malfunction	OT.Prot_Phys_Tamper
FCS_RNG.1		x			x	x				
FCS_COP.1/SHA		x				x				
FCS_COP.1/CCA_SIGN		x				x				
FCS_COP.1/CCA_VERIF		x				x				
FCS_COP.1/3TDES		x				x				
FCS_COP.1/RMAC		x				x				
FCS_CKM.1/Asym_Auth		x				x				
FCS_CKM.1/Sym_Auth		x				x				
FCS_CKM.4		x				x				
FIA_ATD.1										
FIA_UID.1	x	x			x					
FIA_UAU.1	x	x			x					
FIA_UAU.4		x				x				
FIA_UAU.5		x				x				
FIA_UAU.6		x				x				
FIA_API.1						x				
FDP_ACC.1	x		x	x	x					
FDP_ACF.1	x		x	x	x					
FDP_ITC.1										
FDP_RIP.1			x							
FDP_SDI.2				x						
FDP_UCT.1						x				
FDP_UIT.1						x				
FTP_ITC.1						x				
FMT_SMF.1	x									
FMT_SMR.1	x									
FMT_LIM.1		x					x			

	OT.AC_Pers	OT.AC_Serv	OT.Data_Confident	OT.Data_Integrity	OT.TSS	OT.Trusted_Channel	OT.Prot_Abuse_Func	OT.Prot_Inf_Leak	OT.Prot?Malfunction	OT.Prot_Phys_Tamper
FMT_LIM.2		x					x			
FMT_MSA.2		x					x			
FMT_MSA.3		x								
FMT_MTD.1/INI	x									
FMT_MTD.1/RAD_WR	x									
FMT_MTD.1/RAD_MOD	x									
FPT_EMSEC.1			x					x		
FPT_FLS.1			x	x				x	x	
FPT_PHP.3			x	x				x	x	x
FPT_RVM.1	x		x	x			x	x	x	
FPT_SEP.1			x	x			x	x	x	
FPT_TST.1			x	x				x	x	

Table 6: Security functional requirements rationale

7.2.2 Security Requirements Sufficiency

227 The security objective **OT.AC_Pers** "Access control for personalization and management" mainly implemented by following SFRs:

(i) The SFR **FMT_SMR.1** defines the Card Management System as known role of the TOE and the **SFR FMT_SMF.1** defines personalization as security management function.

(ii) The SFRs **FIA_UID.1** and **FIA_UAU.1** require identification and authentication as necessary precondition for the personalization (i.e. this TSF mediated function is not allowed before the user is identified and successfully authenticated).

(iii) The SFRs **FDP_ACC.1** and **FDP_ACF.1** limit the management activities for user data to the Card Management System.

(iv) The SFRs **FMT_MTD.1/RAD_WR** and **FMT_MTD.1/RAD_MOD** limit the management of the authentication reference data of the Cardholder and the PKI root for the card-to-card authentication to the Card Management System.

(v) The SFR **FMT_MDT.1/INI** defines that the Card Management System role shall create the initial roles.

(vi) The SFR **FPT_RVM.1** ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

228 The security objective **OT.AC_Serv** "Access Control for TOE Security Services" addresses the implementation and the access control of the TOE security services. The security services are implemented by the following SFRs:

(i) The TOE security service Service_Asym_Mut_Auth_w/o_SK is implemented by the SFRs **FCS_COP.1/CCA_SIGN**, **FCS_COP.1/CCA_VERIF**, **FCS_RNG.1** and **FIA_UAU.5**.

(ii) The TOE security services Service_Asym_Mut_Auth_with_SM, Service_Asym_Mut_Auth_with_TC, Service_Asym_Mut_Auth_with_Intro Service_Sym_Mut_Auth_with_TC and Service_Sym_Mut_Auth_with_SM are implemented by the SFRs **FCS_COP.1/SHA, FCS_CKM.1/Asym_Auth, FCS_CKM.1/Sym_Auth, FCS_CKM.4**, **FCS_COP.1/CCA_SIGN**, **FCS_COP.1/CCA_VERIF**, **FCS_RNG.1**, **FCS_COP.1/3TDES**, **FCS_COP.1/RMAC FIA_UAU.4, FIA_UAU.5** and **FIA_UAU.6**.

The access control for these security services is implemented by following SFRs:

(i) The SFRs **FIA_UID.1** and **FIA_UAU.1** require identification and authentication as necessary precondition for the use of the security services except Service_Asym_Mut_Auth_with_SM (i.e. this TSF mediated function is not allowed before the user is identified and successfully authenticated), and **FIA_UAU.6** require to re-authenticate the remote communication entity for each data package received by secure messaging.

(ii) The SFRs **FMT_MSA.2** and **FMT_MSA.3** ensure secure security attributes of cryptographic keys and other objects.

(iii) The SFRs **FMT_LIM.1** and **FMT_LIM.2** prevent the misuse of TOE functions intended for the testing, the initialization and the personalization of the TOE in the operational phase of the TOE,

229 The security objective **OT.Data_Confident** "Confidentiality of internal data" is implemented by following SFRs:

(i) The SFR **FDP_ACC.1** and **FDP_ACF.1** protect the confidentiality of the private keys.

(ii) The SFR **FDP_RIP.1** protects the misuse of residual user data.

(iii) The SFRs **FPT_EMSEC.1**, **FPT_FLS.1**, **FPT_PHP.3**, **FPT_RVM.1, FPT_SEP.1** and **FPT_TST.1** protect the confidential user data and TSF data against general smart card attacks.

230 The security objective **OT.Data_Integrity** "Integrity of internal data" is implemented by following SFRs:

(i) The SFRs **FDP_ACC.1** and **FDP_ACF.1** protect the integrity of the data under the TSC.

(ii) The SFR **FDP_SDI.2** protects the internal stored user data against alteration.

(iii) The SFRs **FPT_FLS.1**, **FPT_PHP.3**, **FPT_RVM.1, FPT_SEP.1** and **FPT_TST.1** protect the confidential user data and TSF data against general smart card attacks.

231 The security objective **OT.TSS** "Terminal support service" requires the TOE to provide a service of random number generation for the operational environment by means of command GET RANDOM and cryprographic operation with private keys for TSL protocol for card terminal to all users. It is implemented by the SFRs:

(i) The SFR **FCS_RNG.1** provides the random number generation.

(ii) The SFRs **FIA_UID.1** and **FIA_UAU.1** allow usage of this service before the user is identified.

(iii) The SFRs **FDP_ACC.1** and **FDP_ACF.1** enforce access control for the services.

232 The security objective **OT.Trusted_Channel** "Trusted Channel" as part of the TOE security services Service_Asym_Mut_Auth_with_SM are implemented by following SFRs:

(i) The SFRs **FCS_CKM.1/Asym_Auth**, **FCS_CKM.1/Sym_Auth** and **FCS_RNG.1** establish and **FCS_CKM.4** destructs the secure messaging keys.

(ii) The SFRs **FCS_COP.1/3TDES** and **FCS_COP.1/RMAC** provide encryption, decryption, MAC calculation and MAC verification.

(iii) The SFRs **FCS_COP.1/SHA**, **FCS_COP.1/CCA_SIGN**, **FCS_COP.1/CCA_VERIF** provide the necessary cryptographic primitives for user authentication used to enforce **OT.Trusted_Channel.**

(iv) The SFRs **FDP_UCT.1, FDP_UIT.1** and **FTP_ITC.1** provide the protection of the confidentiality and integrity of the transmitted data

(v) The SFR **FIA_UAU.4** ensures the use of fresh cryptographic keys for the trusted channel.

(vi) The SFR **FIA_UAU.5** provides multiple authentication mechanisms to support user authentication.

(vii) The SFR **FIA_UAU.6** re-authenticates the communicating entity by checking the MAC of each commands received from this entity.

(viii) The SFR **FIA_API.1** implements authentication Proof of Identity of the role SMC, PIN sender.

233 The security objective **OT.Prot_Abuse_Func** "Protection against abuse of functionality" is implemented by the following SFRs:

(i) The SFR **FMT_LIM.1** and **FMT_LIM.2** prevent the misuse of TOE functions intended for the testing, the initialization and the personalization of the TOE in the operational phase of the TOE.

(ii) The SFR **FMT_MSA.2** ensures that only secure values are accepted for security attributes.

(iii) The SFR **FPT_RVM.1** and **FPT_SEP.1** ensure that the protection of TOE functions intended for the testing, the initialization and the personalization of the TOE can not by bypassed or corrupted.

234 The security objective **OT.Prot_Inf_Leak** "Protection against information leakage" is implemented by the following SFRs:

(i) The SFR **FPT_EMSEC.1** protects user data and TSF data against information leakage through side channels.

(ii) The SFR **FPT_TST.1** detects errors and the SFR **FPT_FLS.1** preserves a secure state in case of detected error which may cause information leakage e.g. trough differential fault analysis.

(iii) The SFR **FPT_PHP.3** resists physical manipulation of the TOE hardware to enforce information leakage e.g. by deactivation of countermeasures or changing the operational characteristics of the hardware.

(iv) The SFRs **FPT_RVM.1** and **FPT_SEP.1** ensure that the TSF dealing with sensitive information or the TSF preventing information leakage can not be bypassed or corrupted.

235 The security objective **OT.Prot_Malfunction** "Protection against Malfunctions" is implemented by the following SFRs:

(i) The SFR **FPT_TST.1** detects errors and the SFR **FPT_FLS.1** prevents information leakage by preserving a secure state in case of detected errors or insecure operational conditions where reliability and secure operation has not been proven or tested.

(ii) The SFRs **FPT_RVM.1** and **FPT_SEP.1** ensure that the TSF detecting errors or insecure operational can not by bypassed or corrupted.

(iii) The SFR **FPT_PHP.3** resists physical manipulation of the TOE hardware controlling the operational conditions e.g. sensors.

236 The security objective **OT.Prot_Phys_Tamper** "Protection against physical tampering" is implemented directly by the SFR **FPT_PHP.3**.

7.2.3 Dependency Rationale

SFR	Dependencies	Support of the Dependencies
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	The cryptographic algorithm SHA-256 does not use any

SFR	Dependencies	Support of the Dependencies
	of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes	cryptographic key. Therefore none of the listed SFR is needed to be defined for this specific instantiation of FCS_COP.1.
FCS_COP.1/CCA_SIGN	[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_MSA.2 Secure security attributes	justification 2 for non-satisfied dependencies
FCS_COP.1/CCA_VERIF	[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_MSA.2 Secure security attributes	justification 2 for non-satisfied dependencies
FCS_COP.1/3TDES	[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 FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 1 for non-satisfied dependencies
FCS_COP.1/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 FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 1 for non-satisfied dependencies
FCS_CKM.1/Asym_Auth	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction,	FCS_CKM.4, FCS_COP.1, justification 1 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
	FMT_MSA.2 Secure security attributes	
FCS_CKM.1/Sym_Auth	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, FCS_COP.1, justification 1 for non-satisfied dependencies
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes	FCS_CKM.1, justification 1 for non-satisfied dependencies
FIA_ATD.1	No dependencies	n.a.
FIA_API.1	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	fulfilled
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	fulfilled
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	fulfilled
FDP_ITC.1	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1, FMT_MSA.3
FDP_RIP.1	No dependencies	n.a.
FDP_SDI.2	No dependencies	n.a.
FDP_UCT.1	[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]	Fulfilled by FTP_ITC.1 and FDP_ACC.1
FDP_UIT.1	[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]	Fulfilled by FTP_ITC.1 and FDP_ACC.1
FTP_ITC.1	No dependencies	n.a.

SFR	Dependencies	Support of the Dependencies
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	fulfilled
FMT_LIM.1	FMT_LIM.2	fulfilled
FMT_LIM.2	FMT_LIM.1	fulfilled
FMT_MSA.2	ADV_SPM.1 Informal TOE security policy model [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	ADV_SPM.1 FDP_ACC.1, FMT_SMR.1, FMT_MSA.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_SMR.1 fulfilled; there is no need and commands for management of security attributes, see justification 3 for non-satisfied dependencies
FMT_MTD.1/INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/RAD_WR	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/RAD_MOD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	ADV_SPM.1	fulfilled by EAL4
FPT_PHP.3	No dependencies	n.a.
FPT_RVM.1	No dependencies	n.a.
FPT_SEP.1	No dependencies	n.a.
FPT_TST.1	FPT_AMT.1 Abstract machine testing	See justification 4 for non-satisfied dependencies

Table 2: Dependency rationale overview

237 Justification for non-satisfied dependencies:

No. 1: The TSF according to SFRs FCS_CKM.1 and FCS_CKM.4 generate and destroy automatically the secure messaging keys used for FCS_COP.1/3TDES and FCS_COP.1/RMAC. If the TOE does not support the optional management of logical channels it will be no need for security attributes of these keys. If the TOE supports the management of logical channels the security target will describe the management security attributes of these keys (cf. Application note 29).

No. 2: The SFRs FCS_COP.1/CCA_SIGN and FCS_COP.1/CCA_VERIF use keys which are loaded or generated during the personalisation and are not updated or deleted over the life time of the TOE. Therefore none of the listed SFRs is needed to define for this specific instantiations of FCS_COP.1.

No. 3: The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFRs FMT_MSA.1 and FMT_MSA.2) is necessary here.

No. 4: The TOE consists of the software and its underlying hardware on which it is running. Thus there is no abstract machine to be tested.

7.2.4 Rationale for the Assurance Requirements

238 The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices, which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

239 The selection of component ADV_IMP.2 provides a higher assurance for the implementation of the TOE especially for the absence of unintended functionality.

240 In the component AVA_MSU.3, an analysis of the guidance documentation by the developer is required to provide additional assurance that the objective has been met, and this analysis is validated and confirmed through testing for insecure states performed by the evaluator.

241 The TOE shall be shown to be resistant to penetration attacks with high attack potential as described in the threats (cf. 3.3 Threats and 4.1.1 Security Objectives for the TOE, especially OT.Data_Confident and OT.Prot_Phys-Tamper). Therefore the component AVA_VLA.4 was included to meet the security objectives.

242 The minimal strength of function “high” was selected to ensure resistance against direct attacks on functions based on probabilistic or permutational mechanisms.

243 The component ADV_IMP.2 has the following dependencies:

- ADV_LLD.1 Descriptive low-level design
- ADV_RCR.1 Informal correspondence demonstration

- ALC_TAT.1 Well-defined development tools

All of these are met or exceeded in the EAL4 assurance package.

244 The component AVA_MSU.3 has the following dependencies:

- ADO_IGS.1 Installation, generation, and start-up procedures
- ADV_FSP.1 Informal functional specification
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

All of these are met or exceeded in the EAL4 assurance package.

245 The component AVA_VLA.4 has the following dependencies:

- ADV_FSP.1 Informal functional specification
- ADV_HLD.2 Security enforcing high-level design
- ADV_IMP.1 Subset of the implementation of the TSF
- ADV_LLD.1 Descriptive low-level design
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

All of these are met or exceeded in the EAL4 assurance package.

7.2.5 Security Requirements – Mutual Support and Internal Consistency

246 The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security assurance requirements (SARs) and the security functional requirements (SFRs) together forms a mutually supportive and internally consistent whole.

247 The analysis of the TOE´s security requirements with regard to their mutual support and internal consistency demonstrates:

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the additional assurance components in section 7.2.4 Rationale for the Assurance Requirements shows that the assurance requirements are mutually supportive and internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

The dependency analysis in section 7.2.3 Dependency Rationale 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 analyzed, and non-satisfied dependencies are appropriately explained.

248 The following additional reasons support consistency and mutual supportiveness of the SFRs. The chosen SFRs of class FCS implement the cryptographic algorithms as required by the SMC specification. The chosen SFRs of classes FIA and FDP support the access control policy SMC

Access Control SFP as defined in the objective OT.AC_Pers and OT.AC_Serv. The chosen SFRs of class FMT support the secure management of TSF data in a way, which is consistent to the policy SMC Access Control SFP. The SFRs of all these classes (FCS, FIA, FDP, FMT) together provide the HPC/SMC services as defined in the TOE description (chapter 2 TOE Description). The remaining SFRs, chosen from class FPT define low level protection of the TOE against any attempt to bypass the security policy SMC Access Control SFP or the services defined in the specification.

In detail these connections between the SFRs can be seen from section 7.2.3 Dependency Rationale.

249 Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 7.2.3 Dependency Rationale and 7.2.4 Rationale for the Assurance Requirements. Furthermore, as also discussed in section 7.2.4 Rationale for the Assurance Requirements, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

8 PP Application Notes

8.1 Glossary and Acronyms

Term	Definition
Advanced electronic signature	an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. Advanced electronic signatures are based on certificate and uses digital signature.
Application note	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
Card-to-Card authentication	Authentication protocols between smart cards using the commands EXTERNAL AUTHENTICATE, INTERNAL AUTHENTICATE and MUTUAL AUTHENTICATE without key agreement, with agreement of symmetric keys as introduction keys (e.g. desSessionkey4Intro), trusted channel keys (e.g. desSessionkey4TC) or secure messaging keys (e.g. desSessionkey4SM).

Term	Definition
Digital signature	Asymmetric cryptographic mechanism to proof the integrity of data as being originated by the signer and to verify the integrity of data as being originated by the signer.
Health Professional Data	Personal data identifying the Health Professional holding the HPC as natural person
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
Initialisation Data	Any data defined by the TOE Card Management systemr and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification (IC identification data).
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The eHC's chip is a integrated circuit.
Personalization	The process by which personal data are brought into the TOE before it is handed to the cardholder
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Security Module Card	Smart card providing security services in the health care environment.
Trusted channel	Common Criteria [1], para. 89: a means by which a TSF and a remote trusted IT product can communicate with necessary confidence. HPC specification [17], Kap. 15: communication using secure messaging while the HPC is using a secure messaging key desSessionKey4SM to receive and to answer commands and the SMC is using a trusted channel key desSessionKey4TC to encrypt commands,, to calculate MAC for commands to decrypt command responses and to verify MAC of command responses.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [1]).
User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [1]).

Acronyms

Acronyms	Term
C.SMC.AUTR_CVC	Card Verifiable Authentication Certificate for role authentication
C.SMC.AUTD_RPS_CVC	Card Verifiable Authentication Certificate as remote PIN sender
CA	Certification authority
CC	Common Criteria
CSP	Certification service provider
eHC	Electronic health card
HPC	Health professional card
PrK.SMC.AUTD_RPS_CVC	Card Authentication Private Key as remote PIN sender
PrK.SMC.AUTR_CVC	Card Authentication Private Key for role authentication between TOE and external SMC
PuK.CA_SMC.CS	Public key of certification service provider used for verification of card verifiable certificates
PuK.SMC.AUTR_CVC	Card Authentication Public Key for role authentication between TOE and external SMC
SAR	Security assurance requirements
SFR	Security functional requirement
SMC	Security module card
ST	security target
TOE	Target of Evaluation
TSF	TOE security functions

8.2 Literature

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.3, August 2005, CCMB-2005-08-001

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.3, August 2005, CCMB-2005-08-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.3, August 2005, CCMB-2005-08-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004

Cryptography

[5] Federal Office for Information Security (BSI) Technical Guideline TR-03111 Elliptic Curve Cryptography Based on ISO 15946, Version 1.00, 14.02.2007

[6] BSI TR-03116 Technische Richtlinie für eCard-Projekte der Bundesregierung, Version 3.0, April 2009

[7] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, 17.November 2008, veröffentlicht im Bundesanzeiger Nr. 13, S. 346, am 27. Januar 2009)

[8] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[9] Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[10] Federal Information Processing Standards Publication 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[11] AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©, September 20, 1998

[12] RFC 2104 - HMAC: Keyed-Hashing for Message Authentication, February 1997

[13] ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004

[14] PKCS #1: RSA Cryptography Specifications, Version 2.1. RSA Laboratories, 14.6.2002

Protection Profiles

[15] Security IC Platform Protection Profile, Version 1.0, 15.06.2007, developed by Atmel, Infineon Technologies AG, NXP Semiconductors, Renesas Technology Europe Ltd., STMicroelectronics, BSI-CC-PP-0035

[16] Protection Profile Secure Signature Creation Device Type 2 resp Type 3, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0005-2002T resp. BSI-PP-0006-2002T, also short SSVG-PPs or CWA14169

Sonstige

[17] Specification German Health Professional Card and Security Module Card - Part 1: Commands, Algorithms and Functions of the COS Platform, Version 2.3.0, 04.07.2008, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychotherapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft

[18] Specification German Health Professional Card and Security Module Card - Part 2: HPC Applications and Functions, Version 2.3.0, 04.07.2008, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychotherapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft

[19] Specification German Health Professional Card and Security Module Card - Part 3: SMC Applications and Functions, Version 2.3.0, 04.07.2008, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychotherapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft

[20] Specification Related Questions Nr. 0001 bis 0003, 08.08.2008, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychotherapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft

[21] Einführung der Gesundheitskarte. Konnektorspezifikation, Version 2.8.0, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH 12.06.2008

[22] Einführung der Gesundheitskarte. Registrierung einer CVC-CA der zweiten Ebene Version 1.5.0, 18.03.2008

[23] Sozialgesetzbuch Fünftes Buch Gesetzliche Krankenversicherung, in der Fassung des Gesetzes zur Sicherung der nachhaltigen Finanzierungsgrundlagen der gesetzlichen Rentenversicherung (RV-Nachhaltigkeitsgesetz) vom 21. Juli 2004 (BGBl. I S. 1791)

[24] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV), "Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)"

[25] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) "Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)"

[26] ISO/IEC 7816-2: 1999 Identification cards - Integrated circuit cards with contacts - Part 2: Dimensions and location of contacts

[27] Anwendungshinweise und Interpretationen zum Schema, AIS 20, Version 1, 02.12.1999, Bundesamt für Sicherheit in der Informationstechnik

[28] Anwendungshinweise und Interpretationen zum Schema, AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[29] Einführung der Gesundheitskarte, Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, gematik mbH, Version 1.4.0, (freigegeben), 10.07.2008