Security Target Lite
STARCOS 3.4 Health SMC-A C1

Version 1.8/18.05.2011

Author: Giesecke & Devrient GmbH
Document Status: Final

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München

Contents

1 Introduction

1.1 TOE Reference

This document refers to the following TOE:

1) STARCOS 3.4 Health SMC-A C1

1.2 ST Reference and ST Identification

Title: Security Target Lite STARCOS 3.4 Health SMC-A C1

Version Number/Date: Version 1.8/18.05.2011

Origin: Giesecke & Devrient GmbH

TOE: STARCOS 3.4 Health SMC-A C1

TOE documentation:

- Guidance Documentation STARCOS 3.4 Health HBA/SMC C1 - Main Document
- Guidance Documentation for the Initialisation Phase STARCOS 3.4 Health HBA/SMC C1
- Guidance Documentation for the Personalisation Phase STARCOS 3.4 Health HBA/SMC C1
- Guidance Documentation for the Operational Usage Phase STARCOS 3.4 Health SMC-A and SMC-B C1
- STARCOS 3.4 SmartCard Operating System Reference Manual

HW-Part of TOE: NXP P5CC052V0A (Certificate: BSI-DSZ-CC-0466-2008 [22], Assurance Continuity Maintenance Report: BSI-DSZ-CC-0466-2008-MA-01 [23]).

1.3 TOE Overview

The aim of this document is to describe the Security Target for 'STARCOS 3.4 Health SMC-A C1'.

The related product is the STARCOS 3.4 Operating System (OS) on a Smart Card Integrated Circuit. The SMC is a contact based plug-in smart card in ID-000 format with applications for the German health care system according to “Gesetz zur Modernisierung der Gesetzlichen Krankenversicherung” (GKV-Modernisierungsgesetz – GMG), the “Sozialgesetzbuch” (SGB) and the privacy legislation (“Datenschutzgesetze des Bundes und der Länder”). The SMC is based on the Integrated Circuit (IC) from NXP (P5CC052V0A). The SMC is conformant to the specifications of the SMC [15] and [17].

The SMC will be used by the cardholder, who may be a health professional.

STARCOS 3.4 is a fully interoperable ISO 7816 compliant multiapplication Smart Card OS, including a cryptographic library.

In this Security Target the security services provided by the Security Module Card Type A (SMC-A, German: "Sicherheitsmodul-Karte Typ A") are addressed, 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.

The SMC exists in 3 different configurations: SMC-A, SMC-B, and SMC-K. SMC-A and SMC-B are described in [17], SMC-K is described in [18].

When the term "SMC" is used in the following, this refers to the SMC-A variant, if not otherwise specified.

This document describes

- the Target of Evaluation (TOE)
- the security environment of the TOE
- the security objectives of the TOE and its environment
- and the TOE security functional and assurance requirements.

The assurance level for the STARCOS 3.4 Health SMC-A C1 TOE is CC **EAL4** augmented with **AVA_VAN.5**

1.4 CC Conformance

This ST is in accordance with Common Criteria V3.1 (see [1], [2], [3]) as follows

- CC V3.1 Part 2 extended
- CC V3.1 Part 3 conformant
- Package conformant to EAL4 augmented with AVA_VAN.5

1.5 Sections Overview

Chapter 1 provides the introductory material for the Security Target.

Chapter 2 provides the TOE description.

Chapter 3 contains the conformance claims.

Chapter 4 contains the Security Problem Definition

Chapter 5 defines the security objectives for both the TOE and the TOE environment. In addition, a rationale is provided to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat.

Chapter 6 contains the Extended component definition.

Chapter 7 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [2] and Part 3 [3], that must be satisfied.

Chapter 7.3 provides an explanation how the set of security requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Afterwards Chapter 7.3 provides a set of arguments that address dependency analysis.

Chapter 8 contains the TOE Summary Specification.

Chapter 9 provides information on applied conventions, used terminology, definitions of frequently used acronyms.

Chapter 10 provides a list of references used throughout the document.

2 TOE Description

2.1 TOE definition

The Target of Evaluation (TOE) is the Secure Module Card Type A (SMC-A). The SMC-A, which is a contact-based smart card, is described in the specification documents [15], [17]. The physical characteristics shall comply with ISO/IEC 7816-1 and related standards.

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 applications (data structures and their content)

and

TOE_GD

- the guidance documentation delivered together with the TOE.

The TOE_ES is the operating system STARCOS 3.4 from Giesecke & Devrient and is implemented in the ROM area of the chip hardware *(NXP P5CC052V0A).* The TOE_APP is implemented as a file system containing the Applications according to [15] and [17] and is installed in the EEPROM of the IC and the underlying IC itself. Parts of the operating system may also reside in the EEPROM. The evaluation is a ‘composite evaluation’, where the TOE_IC from NXP has been evaluated / certified in a separate Common Criteria process according to EAL5+.

The STARCOS 3.4 Health SMC-A C1 provides the following main security services:

1. Access control for the function (2) to (5) listed below,
2. Asymmetric card-to-card authentication between the SMC and an eHC, a HPC or another SMC without establishment of a trusted channel,
3. Asymmetric card-to-card authentication between the SMC and a HPC or SMC with establishment of a trusted channel, and 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 and storage of configuration data and network data.

2.2 Limits of the TOE

2.2.1 TOE usage and security features for operational use

The STARCOS 3.4 Health SMC-A C1 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.

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:

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. [15], 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 [15], 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 [15], section 15).

Service_Asym_Mut_Auth_with_SM: Mutual Authentication using asymmetric techniques between the SMC and a HPC with agreement of symmetric secure messaging keys and establishment of secure messaging channel after successful authentication as receiver of secured commands and for 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 [15], 15.4.4). This service uses the commands INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE with algorithmic identifier '*rsaSessionkey4SM*'.

Service_Asym_Mut_Auth_with_TC: Mutual Authentication using asymmetric techniques between the SMC and a HPC, SMC or eHC[2], with establishment of a trusted channel keys after 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 [20], 15.4.4). This service uses the commands INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE with algorithmic identifier '*rsaSessionkey4TC*' (cf. for details to [20], section 15) to establish symmetric keys of type *desSessionkey4TC* for PSO: ENCIPHER, PSO: DECIPHER, PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM and PSO: VERIFY CRYPTOGRAPHIC CHECKSUM.

Service_Asym_Mut_Auth_with_Intro: Mutual Authentication using asymmetric techniques between the HPC and an SMC with storage of introduction keys after successful authentication (cf. for details to [16], 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.

---

[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 [17], 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 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.

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 [16], 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.

Service_Sym_Mut_Auth_with_TC: Mutual authentication using symmetric techniques between the SMC[3] and an external entity with establishment of symmetric keys for secure messaging, 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 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. [15], sec. 15.4.1) (ii) SMC/HPC communication (cf. [15], 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 SMC and simultaneously to agree the session keys. For SMC/HPC communication firstly the command INTERNAL AUTHENTICATE with algorithmic identifier *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 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 HPC and the SMC in secure messaging mode.

[3] Note the SMC specification [17], 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 aldid “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.

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]

Service_Sym_Mut_Auth_with_SM: Mutual Authentication using symmetric techniques between the SMC 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 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 ‘*desSessionkey4SM*’ (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 ‘*desSessionkey4SM*’.

A successful verification sets in the HPC 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 in secure messaging mode.

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

---

[4] Note the use of ENVELOPE command is optional (cf. [17], sec. 5.9.7 and 5.9.8) and therefore not addressed in this security target.

In detail the functionality of the SMC is defined in the specifications:

[15] 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, Bundesapothekenkammer, Deutsche Krankenhaus-Gesellschaft

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

2.2.2 TOE type

The Target of Evaluation (TOE) is the Security Module Card Type A (SMC-A). The SMC-A is a contact based smart card.

2.2.3 TOE Life Cycle

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 [12]. They are summarized in the following Table 1.

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 and • 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 (card holder specific) visual readable data onto the physical smart card, and the writing of (card holder specific) TOE User Data and

		TSF Data into the smart card.
7	**Smartcard End-usage**	The **Smartcard Issuer** is responsible for • The smartcard product delivery to the smartcard end-user (the card holder), and the end of life process. The authorized personalization agent (Card Management System) is allowed to add data, modify or delete an SMC application. The TOE is used as SMC by the smart card holder in the Operational use phase

Table 1 Smart Card Life Cycle Overview

The Life Cycle phases are summarized in the table above.

The Life Cycle basically consists of the development phase and the operational phase.

Development phase includes phase 1 to phase 4. The initialisation data and the hardware containing parts of the TOE will be delivered. The initialisation data will be delivered in a way that allows no modification by the party loading the initialisation data into the hardware.

The operational phase starts with phase 5 and ends with phase 7.

Note, that this fulfils the requirements from application note 2 part a of the SMC-PP [13].

The roles during development phase, which are define*d* in Table 1 are managed by the following parties:

Smartcard Embedded Software Developer -	Giesecke & Devrient
IC Designer -	NXP
IC Manufacturer -	NXP
IC Packaging Manufacturer -	NXP
IC Mask Manufacturer -	NXP
Smartcard Product Manufacturer -	Giesecke & Devrient

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

The CC does 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.

Note by the ST-author 1:

After phase 4 the TOE consists of 2 parts: the initialisation table and the hardware containing parts of the TOE. Both parts will be delivered to a third party. The process guarantees that the third party is not able to modify neither the initialisation data nor the hardware containing TOE parts.

This meets the following SMC-PP [13] requirements:

- 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.
- The data structures and the access rights to these data as defined in the SMC specifications [15] and [17] are covered by the evaluation.

3 Conformance Claims

3.1 CC Conformance Claim

This Security Target is Common Criteria version 3.1 Revision 3 [1] [2] [3] conformant.

This Security Target is Common Criteria Part 2 [2] extended and Common Criteria Part 3 [3] conformant.

3.2 PP Conformance Claim

This ST claims strict conformance to PP-SMC-A [13].

3.3 Package Conformance Claim

This ST conforms to assurance package EAL4 augmented with AVA_VAN.5 defined in CC part 3 [3].

3.4 Conformance Claim Rationale

This security target is conformant to the claimed PP [13].

The TOE type is a contact based smart card (see chapter 1.3), which is consistent with the TOE type in the PP [13], chapter 1.2.2.

The Security Problem Definition (chapter 4) is taken directly from the PP [13], chapter 3, with the following exception:

In order to be consistent with the hardware ST, a new threat has been introduced: *T.Lifecycle_Flaw*.

In order to cover this threat, a new security objective which covers this threat has been introduced: *The following Objective added by the ST author:*

OT.Lifecycle_Security. The remaining security objectives are identical with those from the PP [13].

The security requirements (chapter 7) have been taken directly from the PP [13] (chapter 6) and operations as appropriate have been performed.

4 Security Problem Definition

4.1 Introduction

In the introduction the assets (which the TOE shall protect) and the subjects (users or threat agents – attacker – of the TOE) will be described.

4.1.1 Assets

The assets to be protected by the TOE and its environment are as follows. Not all assets exist in both configuration, but if an object which is classified as an asset exists it will be handled as described in the SFRs of this security target.

Name of asset	**Description**	**Operation by commands**[5]
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 Key for role authentication (PrK.SMC.AUTR_CVC)	The Card Authentication Private Key PrK.SMC.AUTR_CVC is an asymmetric cryptographic key used for the authentication of a SMC to an eHC on behalf of the card holder. It is part of the user 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 Key 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 to the eHC with or without establishing a trusted channel by means of secure messaging. It contains encoded	SELECT, READ BINARY

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

Name of asset	Description	Operation by commands[5]
	access rights (Role ID for SMC profile 2 to 6[6]) 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 SMC. It is stored in the file EF.C.SMC.AUTR_CVC which integrity shall be protected.	
Card Authentication Private Key as remote PIN sender (PrK.SMC.AUTD_RPS_CVC)	The Card Authentication Private Key PrK.SMC.AUTD_RPS_CVC is an asymmetric cryptographic key used for the card-to-card authentication between of an SMC to a HPC or another SMC or RFID as remote PIN sender. It is part of the TSF data.	INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE
Card Verifiable Authentication Certificates as remote PIN sender (C.SMC.AUTD_RPS_CVC)	The card verifiable certificate C.SMC.AUTD_RPS_CVC for the Card Authentication Public Key PuK.SMC.AUTD_RPS_CVC as authentication reference data corresponding to the Authentication Private Key PrK.SMC.AUTD_RPS_CVC is used for card-to-card authentication of the SMC to the 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
EF.GDO	EF.GDO contains the DO ICC	SELECT, READ

[6] Note the profiles are assign informative only, cf. [20].

Name of asset	Description	Operation by commands[5]
	Serial Number.	BINARY
EF.VERSION	The EF.Version with linear fixed record structure contains the version numbers of the specification, which the card is compliant to.	SELECT, READ RECORD, SEARCH RECORD
EF.SMD	EF.SMD contains SMC 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 connector	SELECT, READ BINARY
PrK.SMKT.AUT	PrK.SMKT.AUT is the private authentication key for connecting the card terminal to a specific connector.	PSO: DECIPHER, INTERNAL AUTHENTICATE
Random number	Random number generation	GET RANDOM

Table 2 Assets of the SMC-A

TSF data	Description	Operation by 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 provide for card verifiable certificates in the health care environment (cf. to [17], sec. 6.3.14, 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
TOE initialization data	Data stored in the TOE during the initialization process. It is part of the TSF data.	

TSF data	Description	Operation by commands
TOE personalization data	Data stored in the TOE during personalization process. It contains user data and TSF data.	

Table 3: TSF data of the SMC

Application note 2:

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.

4.1.2 Subjects

This security target 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.
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) are 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 are trying to interact with the TOE as Card Management System or HPC without being authenticated for any role.

Table 4: Subjects

Application note 3: 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 [15], Chapter 7. The CHA of SMC is defined in [16], Annex A.3.

4.2 Organisational Security Policies

OSPs will be defined in the following form:

OSP.name Short Title

Description.

The TOE and its environment shall comply with 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).

OSP.SMC_Spec Compliance to SMC specifications

The SMC shall be implemented according to the specifications:

[15] 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, Bundesapothekenkammer, Deutsche Krankenhaus-Gesellschaft

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

4.3 Threats

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

Threats will be defined in the following form:

T.name Short Title

Description.

4.3.1 Threats mainly addressing TOE_ES and TOE_APP

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

T.Compromise_Internal_Data Compromise of confidential User or TSF data

An attacker with high attack potential tries to compromise confidential user data or TSF data through the communication interface of the TOE 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).

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.

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.

T.Intercept Interception of Communication

An attacker with high attack potential try 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 patients data like medication or medical data which an attacker may read or forge during transmission.

4.3.2 Threats mainly addressing TOE_IC and TOE_ES

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.

T.Information_Leakage Information Leakage from smart card

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).

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.

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.

The following threat added by the ST author:

T.Lifecycle_Flaw TOE flaw in a particular lifecycle state

An attacker with high attack potential may introduce a chip into the lifecycle which is no correct TOE, but will erroneously be produced and delivered as if it was a real TOE. This would be a threat to the assets "TOE initialization data" and "TOE prepersonalization data". This could, for example, include (i) wrong chips, (ii) correct chips with wrong configuration, (iii) correct chips with wrong TSF data.

4.4 Assumptions

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

The assumptions will be defined in the following form:

A.name Short Title

Description.

A.Pers_Agent Personalization of the smart card

The Card Management System performs the personalisation and additional management steps correctly during the end-usage phase according to specifications [15], [17] and ensures the correctness, the quality and - if necessary - the confidentiality of all data structures and data on the card.

A.Users Adequate usage of TOE and IT-Systems

The card holder 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.

5 Security Objectives

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.

5.1 Security Objectives for the TOE

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.

Objectives for the TOE will be defined in the following form

OT.name short title

Description of the objective.

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).

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.

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.

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.

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.

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 Service_SM_Support.

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.

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.

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.

Application note 4:

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.

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.

Application note 5:

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 provided that detailed knowledge about the TOE´s internals.

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.

Application note 6:

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.

The following Objective added by the ST author:

OT.Lifecycle_Security Lifecycle security

The TOE shall detect flaws during the initialisation, personalisation and operational usage.

5.2 Security Objectives for the Operational Environment

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

OE.name short title

Description of the objective.

The following objectives for the operational environment correspond directly to the assumptions in section 4.4 Assumptions:

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 [15], [17] 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.

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.

5.3 Security Objectives Rationale

5.3.1 Security Objectives Coverage

	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	*OT.Lifecycle_security*	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			
T.Lifecycle_Flaw											x		
OSP.SMC_Spec	x	x	x	x	x	x						x	
A.Pers_Agent												x	
A.Users													x

Table 5: Security Objective Rationale

The threat **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.

The protection against the threat **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.

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.

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 [17]) 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.

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.

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.

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

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

The threat ***T.Lifecycle_Flaw*** “TOE flaw in a particular lifecycle state” is adverted directly by the security objective *The following Objective added by the ST author:* ***OT.Lifecycle_Security*** “Lifecycle security”.

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 objective for the TOE environment **OE.Perso** “Secure personalization and management”. The TOE security objectives OT.AC_Pers, OT.TSS and OT.Trusted_Channel implement the security services of the TOE and their related user data and TSF data as specified in [17] 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 objective for the environment OE.Perso ensures that the Card Management System will provide genuine TOE initialized and personalized according to specification [17] to the cardholder.

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 [15] and [17] (cf. to OSP.SMC_Spec).

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”.

6 Extended Components Definition

This Security Target uses components defined as extensions to CC part 2 [2].

6.1 Definition of the Family FCS_RNG

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 family describes the functional requirements for random number generation used for cryptographic purposes.

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.

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

FCS_RNG.1	Quality metric for random numbers
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*].

6.2 Definition of the Family FIA_API

To describe the IT security functional requirements of the SMC-A 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.

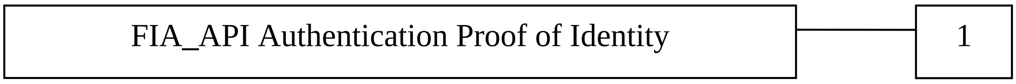
The family “Authentication Proof of Identity (FIA_API)” is specified as follows.

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.

Component levelling:



FIA_API.1	Authentication Proof of Identity
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.
Audit:	FIA_API.1
	There are no actions defined to be auditable.

FIA_API.1	Authentication Proof of Identity
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or rule*].

6.3 Definition of the Family FMT_LIM

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.

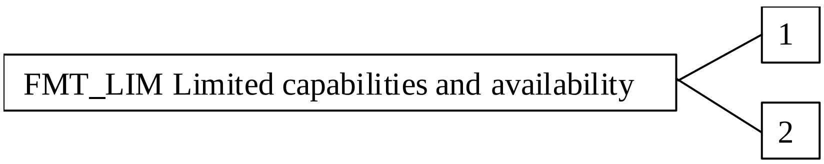
The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

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 requires 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.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

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.

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.

6.4 Definition of the Family FPT_EMSEC

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 to 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

7 Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE and the environment.

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in chapter C.4 of CC, part 1. Each of these operations is used in the SMC PP [13] and respectively also in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements made in the SMC PP [13] 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 <u>underlined text</u> and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

Additional refinements in the ST will be underlined and put in brackets "(…)" and marked by a footnote that states that this refinement is made by the ST-author.

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 of the SMC PP [13] are denoted as <u>underlined text</u> and the original text of the component is given by a footnote. Any uncompleted selections that have been completed by the ST author appear *italicized* and <u>underlined</u> and the original text of the SMC PP [13] is given by a footnote.

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 of the SMC PP [13] are denoted by showing as <u>underlined text</u> and the original text of the component is given by a footnote. Any uncompleted assignments that have been completed by the ST author appear *italicized* and <u>underlined</u> and the original text of the SMC PP [13] is given by a footnote.

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. Iterations in the ST, which do not appear in the PP apear *italicized* in the header and the full text.

7.1 TOE Security Functional Requirements

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].

Note by the ST-author 7:

In the SMC-A PP [13] a table informs about the mapping of security services to SFRs, not be copied in this ST.

7.1.1 Cryptographic support (FCS)

The cryptographic algorithms implemented in the TOE shall meet the TR-03116 [8] and [19].

7.1.1.1 Basic Algorithms

The TOE shall meet the requirement "Quality metric for random numbers (FCS_RNG.1)" as specified below (Common Criteria Part 2 extended). The iteration has been caused by different types of random number generators.

FCS_RNG.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1/DRNG	The TSF shall provide a *deterministic*[7] random number generator, which implements: *functionality class K4 with SOF-high of AIS20 [*6*]*[8].
FCS_RNG.1.1/PHYS	The TSF shall provide a *physical*[9] random number generator, which implements: *functionality class P2 with SOF-high of AIS31 [7]*[10].
FCS_RNG.1.2/DRNG	The TSF shall provide random numbers that meet 1. each output 128 bit random number has at least an entropy of 100 bit.[11,12]

---

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

8 [assignment: *list of security capabilities*]

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

10 [assignment: *list of security capabilities*]

11 [assignment: *a defined quality metric*]

12 This is an assignment already defined in the PP. The PP, however, demands for an additional assignment by the ST author ([assignment: *other defined quality metrics*]), in contradiction to the original definition of the FCS_RNG family. It is not reasonable to define an assignment of an additional quality metric here in the ST.

FCS_RNG.1.2/PHYS	The TSF shall provide random numbers that meet 1. each output 128 bit random number has at least an entropy of 100 bit.[13,14]

Note by the ST-author 8:

The *STARCOS 3.4 Health SMC-A C1* TOE *generates* 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 has been 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’ [6] or ‘AIS 31’, [7].

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.

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

Hierarchical to: No other components.

FCS_COP.1.1/ SHA	The TSF shall perform hashing[15] in accordance with a specified cryptographic algorithm SHA-256[16] and cryptographic key sizes none[17] that meet the following: FIPS 180-2 [10][18].

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

Note by the ST-author 9:

13 [assignment: *a defined quality metric*]

14 see footnote Number 12

15 [assignment: *list of cryptographic operations*]

16 [assignment: *cryptographic algorithm*]

17 [assignment: *cryptographic key sizes*]

18 [assignment: *list of standards*]

The *STARCOS 3.4 Health SMC-A C1* TOE *implements* the hash functions SHA-256 (256 bit hash value) as the cryptographic primitive of the authentication mechanism according to [15].

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[19] in accordance with a specified cryptographic algorithm *RSA ISO9796-2 DS1_SIGN and RSASSA_PSS_SIGN*[20] and cryptographic key sizes 2048 bit module length[21] that meet the following: [15]

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

Note by the ST-author 10:

The *STARCOS 3.4 Health SMC-A C1 implements* the RSA for the cryptographic primitive of the digital signature-creation for the card-to-card authentication mechanism (i.e. INTERNAL AUTHENTICATE) according to [15].

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[22] in accordance with a specified cryptographic algorithm RSA ISO9796-2 DS1_VERIFY[23] and cryptographic key sizes 2048 bit modulo length[24] that meet the following: [15]

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

[19] [assignment: *list of cryptographic operations*]
[20] [assignment: *cryptographic algorithm*]
[21] [assignment: *cryptographic key sizes*]
[22] [assignment: *list of cryptographic operations*]
[23] [assignment: *cryptographic algorithm*]
[24] [assignment: *cryptographic key sizes*]

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

Note by the ST-author 11:

The *STARCOS 3.4 Health SMC-A C1 implements* the RSA for the cryptographic primitive of the digital signature-verification for the card-to-card authentication mechanism (i.e. INTERNAL AUTHENTICATE according to [15].

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

Hierarchical to: No other components.

FCS_COP.1.1/ 3TDES	The TSF shall perform encryption and decryption[25] in accordance with a specified cryptographic algorithm 3TDES in CBC mode[26] and cryptographic key sizes 168 bit[27] that meet the following: FIPS 46-3 [9] and [15]

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

Note by the ST-author 12:

The *STARCOS 3.4 Health SMC-A C1 implements* the cryptographic primitive for secure messaging in with encryption of the transmitted data and for the Service_SM_Support. The key is agreed between the TSF according to the FIA_UAU.4.

FCS_COP.1/RMAC Cryptographic operation – Retail MAC

Hierarchical to: No other components.

FCS_COP.1.1/	The TSF shall perform generation and verification of message

[25] [assignment: *list of cryptographic operations*]
[26] [assignment: *cryptographic key generation algorithm*]
[27] [assignment: *cryptographic key sizes*]
[28] [assignment: *list of cryptographic operations*]

RMAC	authentication code[28] in accordance with a specified cryptographic algorithm Retail MAC[29] and cryptographic key sizes 168 bit[30] that meet the following: ANSI X9.19 with DES and [15], Section 6.6

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

Note by the ST-author 13:

The *STARCOS 3.4 Health SMC-A C1 implements* 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.

7.1.1.2 Cryptographic key generation (FCS_CKM.1)

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

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

Hierarchical to: No other components.

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 and specified cryptographic key sizes 168 bit[31] that meet the following: [8], [15]

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

Note by the ST-author 14:

---

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

The *STARCOS 3.4 Health SMC-A C1 implements* **asymmetric** card-to-card authentication with key agreement [15], 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 algorithms use the random numbers generated by TSF as required by FCS_RNG.1.

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

Hierarchical to: No other components.

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

FCS_CKM.1.1/ 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[32] and specified cryptographic key sizes 168 bit[33] that meet the following: [8], [15]

Note by the ST-author 15:

The *STARCOS 3.4 Health SMC-A C1 is* equipped with symmetric secret introduction keys being agreed upon before (cf. [17], sec. 5.9.3) secure message keys which are used for encryption and message authentication. The algorithms use the random number generated by TSF as required by FCS_RNG.1.

FCS_CKM.4 Cryptographic key destruction

31 [assignment: *cryptographic key sizes*]
32 [assignment: *cryptographic key generation algorithm*]
33 [assignment: *cryptographic key sizes*]

Hierarchical to: No other components.

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physical deletion of key value*[34] that meets the following: *none*[35].

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]

Note by the ST-author 16:

The TOE destroys 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.

7.1.2 Identification and Authentication

7.1.2.1 User attribute definition (FIA_ATD.1)

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

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: identity and role of entities authenticated with introduction keys[36]

Dependencies: No dependencies.

Application note 17:

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. [15] Chapter 7 for details).

---

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

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

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

7.1.2.2 Timing of identification (FIA_UID.1)

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

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1	The TSF shall allow (1) *generating a hash Self test according to FPT_TST.1* (2) *reading data with access condition ALWAYS*[37] (3) reading the ATR (4) reading EF.ATR, EF.DIR, EF.GDO, EF.SMD, EF.VERSION and EF containing certificates EF.C.*.*, (5) reading security status information using command GET SECURITY STATUS KEY, (6) execution of the command GET RANDOM[38] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

7.1.2.3 Timing of authentication (FIA_UAU.1)

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

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

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

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

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 EFs 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) Self test according to FPT_TST.1,* *(7) Identification of the user by means of TSF required by FIA_UID.1,* *(8) reading data with access condition ALWAYS* [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.

7.1.2.4 Single-use authentication mechanisms (FIA_UAU.4)

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

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].

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

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

Dependencies: No dependencies.

Application note 18:

The command EXTERNAL AUTHENTICATE may be used as part of the mutual card-to-card authentication mechanisms

Service_Asym_Mut_Auth_w/o_SK, 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_RND.1) as challenge to prevent reuse of a response generated in a successful authentication attempt.

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

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 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 Secure Module Card with Root Public Key of the Certificate Service Provider and Card verifiable certificate with a corresponding cardholder authorization of SMC[42].

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

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

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

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.

Application note 19:

The specification [15] 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 session keys MUST be deleted by means of clearSecurityStatus(...)."

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

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1	The TSF shall provide (1) INTERNAL AUTHENTICATE 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[46]

Application note 20:

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).

Note by the ST-author 21:

In the SMC-A PP [13] the refinement operation applied for FIA_API.1.1 is not marked appropriately, i.e. as described in the beginning of chapter 7. To comply with the

---

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

[44] [assignment: *authentication mechanism*]

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

[46] Refinement: "(2) INTERNAL AUTHENTICATE with PrK.SMC.AUTD_RPS_CVC to prove the identity of the PIN sender"

description of refinements, point (2) is included as underlined text and marked by a footnote in this security target.

7.1.3 Access Control

The following Security Function Policy (SFP) **SMC Access Control SFP** is defined for the requirements "Subset Access Control (FDP_ACC.1)", "Security attribute based access control (FDP_ACF.1)", "Basic data exchange confidentiality (FDP_UCT.1)" and "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."

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

FDP_ACC.1 Subset Access Control

Hierarchical to: No other components.

FDP_ACC.1.1	The TSF shall enforce the SMC Access Control SFP [47] 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) SMC related Data (EF.SMD), (g) EF.C.SMKT.CA and EF.C.SMKT.AUT (h) Card Authentication Private Keys (PrK.SMC.AUTR_CVC, 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.CA_SMC.CS, EF.C.SMC.AUTD_RPS_CVC (k) PuK.RCA.CS (l) PuK.CAMS_SMC.AUT_CVC 3. operations by commands defined in table 2[48].

Dependencies: FDP_ACF.1 Security attribute based access control

Application note 22:

The subjects and objects are described in section 4.1 Introduction. The public key for CV certificate verification (PuK.RCA.CS) is TSF data.

7.1.3.1 Security attribute based access control (FDP_ACF.1)

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

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1	The TSF shall enforce the SMC Access Control SFP[49] to objects based on the following: authentication status of user[50]
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.SMA, DF.KT 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, EF.C.SMC.AUTD_RPS_CVC,, (e) to execute the command EXTERNAL AUTHENTICATE with PrK.SMC.AUTR_CVC, PrK.SMC.AUTD_RPS_CVC, 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 successfully authenticated HPC is allowed (a) to execute the command INTERNAL AUTHENTICATE using PrK.SMC.AUTR_CVC, (b) to execute the commands UPDATE BINARY and ERASE BINARY with EF.SMD,

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

49 [assignment: *access control SFP*]

50 [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*]

	(c) to perform all actions a terminal is allowed to perform. 3. a successfully 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 4. a successfully 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.[51]
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[52].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: no other access than defined in FDP_ACF.1.2 to the objects listed in FDP_ACC.1.1 is allowed to any subject[53].

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

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

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

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

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

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

FDP_ITC.1.1	The TSF shall enforce the SMC Access Control SFP[54] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *initiate communication via the trusted channel for all functions requiring a trusted channel as defined by SFP_access_rules*[55].

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

FDP_RIP.1 Residual Information Protection

Note by the ST-author 23:

For FDP_RIP.1 an iteration has been performed. The component FDP_RIP.1 of the PP has been covered by FDP_RIP.1/RES_DEAL and FDP_RIP.1/RES_AL.

FDP_RIP.1/ RES_DEAL Residual Information Protection

Hierarchical to: No other components.

FDP_RIP.1.1/ *RES_DEAL*	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from*[56] the following objects: ▪ *secret and private cryptographic keys*[57]

Dependencies: No dependencies.

FDP_RIP.1/ RES_AL Residual Information Protection

Hierarchical to: No other components.

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

55 [assignment: additional importation control rules]

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

57 Version of the PP: *[assignment: list of objects at least including: PINs, secret and private cryptographic keys, data in all files, which are not freely accessible],* Version from the CC Part 2: [assignment: *list of objects*].

FDP_RIP.1.1/ *RES_AL*	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to*[58] the following objects: ▪ *all new created files*[59]

Dependencies: No dependencies.

Note by the ST-author 24:

According to FDP_RIP.1/RES_DEAL PINs, secret and private keys will not be available anymore, when the corresponding resource is deallocated. For example when session keys will be deleted at the end of a trusted channel they will be deleted physically. In other cases data in files might not be physically but logically deleted when dealloacted, but they will be physically deleted, when the memory is allocated e.g. to rewrite EEPROM space. The SFR FDP_RIP.1/RES_AL defines that this must be the case for all other data.

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

FDP_SDI.2 Stored Data Integrity

Hierarchical to: FDP_SDI.1 Stored Data Integrity monitoring

[58] [assignment: *allocation of the resource to, deallocation of the resource from*]
[59] [assignment: *list of objects*].

FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors[60] on all objects, based on the following attributes: • *integrity checked data*[61] .
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[62].

Dependencies: No dependencies.

The following data stored by the TOE have the user data attribute "integrity checked data":

- all cryptographic keys
- security relevant status variables of the card: authentication status for mutual authenticate
- input data for electronic signatures
- user data in files on the card
- access rules for files
- *card life cycle status*

7.1.4 Inter-TSF-Transfer

Application note 25:

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

[60] [assignment*: integrity errors*]

[61] The SMC PP [13] states: *[assignment: user data attributes – the attributes shall be chosen in a way that at least the following data are included:*

- *PINs,*
- *cryptographic keys,*
- *security relevant status variables of the card (e. g. authentication status for the PIN or for mutual authenticate)*
- *input data for electronic signatures*
- *user data in files on the card,*
- *file management information (like access rules for files), and*
- *the card life cycle status]*; Version from the CC part 2 [2]: [assignment: user data attributes]

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

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.

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

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

FDP_UCT.1.1	The TSF shall enforce the SMC Access Control SFP[63] to be able to transmit and receive[64] 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]

Application note 26:

The SMC-A supports secure messaging with TDES encryption (cf. SFR FCS_COP.1/3TDES) after card-to-card authentication.

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

FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

FDP_UIT.1.1	The TSF shall enforce the SMC Access Control SFP[65] to be able to transmit and receive[66] user data in a manner protected from modification, deletion, insertion and replay[67] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[68] has occurred.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

[63] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[64] [selection*: transmit, receive*]
[65] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[66] [selection: *transmit, receive*]
[67] [selection: *modification, deletion, insertion, replay*]

[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

Application note 27:

The SMC-A supports secure messaging with MAC (cf. FCS_COP.1/RMAC) after card-to-card authentication.

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

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[69] 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[70].

Dependencies: No dependencies.

Application note 28:

The specification [15], 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.

7.1.5 Security Management

Application note 29:

The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

---

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

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

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

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Initialization, 2. Personalization, 3. Card management[71].

Dependencies: No Dependencies

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

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[72].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification.

Application note 30:

The Certificate Holder authorization (CHA) Role ID are defined in [16], annex A.3.

Application note 31: 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

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

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

(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.

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

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 [73]

Dependencies: FMT_LIM.2 Limited availability.

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

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 [74]

Dependencies: FMT_LIM.1 Limited capabilities.

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

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

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

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

Dependencies: [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

FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for *identity and role of entities authenticated with introduction keys*[75].

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

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[76] to provide restrictive[77] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the none[78] to specify alternative initial values to override the default values when an object or information is created.

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.

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 [79] the Initialization Data and Pre-personalization Data [80] to the Manufacturer[81].

75 [assignment: *list of security attributes*]
76 [assignment: *access control SFP, information flow control SFP*]
77 [selection, choose one of: *restrictive, permissive, [assignment: other property*]]
78 [assignment: *the authorised identified roles*]

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

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[82] the 1. public keys of the root for CV certificate verification to the Personalisation Agent[83].

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

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[84] the public keys of the root for CV certificate verification[85] to nobody[86].

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

7.1.6 SFR for TSF Protection

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 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

79 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
80 [assignment: *list of TSF data*]
81 [assignment: *the authorised identified roles*]
82 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
83 [assignment: *the authorised identified roles*]
84 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
85 [assignment: *list of TSF data*]
86 [assignment: *the authorised identified roles*]

physical attack (FPT_PHP.3)" on the other. The SFR "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" and "Resistance to physical attack (FPT_PHP.3)" prevent deactivation and manipulation of the security features or misuse of TOE functions.

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 *information about IC power consumption and command execution time* [87] in excess of *non useful information*[88] enabling access to 1. none[89] *and* 1. Card Authentication Private Keys, 2. secure messaging keys[90]
FPT_EMSEC.1.2	The TSF shall ensure any authorized user[91] are unable to use the following interface smart card circuit contacts[92] to gain access to 1. none[93] *and* 2. Card Authentication Private Key, 3. secure messaging keys[94]

Dependencies: No dependencies.

Note by the ST-author 32:

The *STARCOS 3.4 Health SMC-A C1* TOE *prevents* attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such

87 [assignment: *types of emissions*]
88 [assignment: *specified limits*]
89 [assignment: *list of types of TSF data*]
90 [assignment: *list of types of user data*]
91 [assignment: *type of users*]
92 [assignment: *type of connection*]
93 [assignment: *list of types of TSF data*]
94 [assignment: *list of types of user data*]

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 *provides* a smart card interface with contacts according to ISO/IEC 7816-2 [15] 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.

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

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

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[95]

Dependencies: No dependencies

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

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[96] to the TSF[97] by responding automatically such that the SFRs are always enforced.

Dependencies: No dependencies.

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

96 [assignment: *physical tampering scenarios*]

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

Application note 33:

The TOE *implements* 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 will be done 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.

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

FPT_TST.1.1	The TSF shall run a suite of self tests *at the request of the authorised user*[98] to demonstrate the correct operation of the TSF[99].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[100].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of *stored TSF executable code*[101].

Dependencies: No dependencies.

Note by the ST-author 34:

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)" *are* 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.

Application note 35:

[98] [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*]]

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

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

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

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 Manufacturing. 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.

7.2 Security Assurance Requirements for the TOE

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:

AVA_VAN.5.

7.3 Security Requirements Rationale

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 [14]. 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.

The definition of the family FPT_EMSEC is taken from the Protection Profile Secure Signature Creation Device [12], 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.

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.

7.3.1 Security Functional Requirements Coverage

The following Table shows, which SFRs for the *STARCOS 3.4 Health SMC-A C1* 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	*OT.Lifecycle_Security*
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		x									
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						x					
FDP_RIP.1			x								
FDP_SDI.2				x							
FDP_UCT.1						x					
FDP_UIT.1						x					
FTP_ITC.1						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	*OT.Lifecycle_Security*
FMT_SMF.1	x	x									
FMT_SMR.1	x	x									
FMT_LIM.1		x					x				
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_TST.1			x	x				x	x		x

Table 6: Security functional requirements rationale

7.3.2 Security Requirements Sufficiency

The security objective **OT.AC_Pers** “Access control for personalization and management” mainly implemented by following SFR:

(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 SFR **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 SFR **FDP_ACC.1** and **FDP_ACF.1** limit the personalisation activities for user data to the Card Management System,

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

(v) The SFR **FMT_MTD.1/INI** defines that the Manufacturer role shall create the initial roles.

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

(ii) **Service_Asym_Mut_Auth_w/o_SK** is implemented by the SFR **FCS_COP.1/CCA_SIGN**, **FCS_COP.1/CCA_VERIF**, **FCS_RNG.1** and **FIA_UAU.5**.

(iii) The TOE security service Service_Asym_Mut_Auth_with_SM, Service_Asym_Mut_Auth_with_TC, Service_Asym_Mut_Auth_with_Intro, Service_Asym_Mut_Auth_with_TC and Service_Asym_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/TDES**, **FCS_COP.1/RMAC** and **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 SFR **FMT_SMF.1** is capable of performing of the following management functions: Initialization, Personalization, Card Management.

(iv) The SFR **FMT_SMR.1** maintains the roles Card Management System, HPC/SMC, Manufacturer, Personalisation Agent and **FIA_ATD.1** binds identity and role provided by the authentication.

(v) 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.

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 private keys.

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

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

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

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

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

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

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.

The security objective **OT.Trusted_Channel** “Trusted Channel” as part of the TOE security service Service_Asym_Mut_Auth_with_SM is 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 SFR **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 receiver, PIN sender and SMC client.

(ix) The SFR **FDP_ITC.1** addresses import of the public key for transcipherment without security attributes.

The security objective **OT.Prot_Abuse_Func** “Protection against abuse of functionality” is implemented by the following SFR:

(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.

The security objective **OT.Prot_Inf_Leak** “Protection against information leakage” is implemented by the following SFR:

(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.

The security objective **OT.Prot_Malfunction** “Protection against Malfunctions” is implemented by the following SFR:

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

FPT_TST.1 also covers *The following Objective added by the ST author:*

OT.Lifecycle_Security because the manufacturer will carry out tests at the beginning of initialisation in order to verify the correct state of the uninitialised TOE.

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

7.3.3 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 of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	The cryptographic algorithm SHA-256 does not use any cryptographic key. Therefore none of the listed SFR is needed to be defined for this specific instantiation of FCS_COP.1/SHA.
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	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	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	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	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	FCS_CKM.4, FCS_COP.1, justification 1 for non-satisfied

SFR	Dependencies	Support of the Dependencies
	destruction	dependencies
FCS_CKM.1 / Sym_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
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1/Asym_Auth FCS_CKM.1/Sym_Auth, 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 initialization	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]	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]	FTP_ITC.1 and FDP_ACC.1

SFR	Dependencies	Support of the Dependencies
FTP_ITC.1	No dependencies	n.a.
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	fulfilled
FMT_LIM.1	FMT_LIM.2 Limited availability	fulfilled
FMT_LIM.2	FMT_LIM.1 Limited capabilities	fulfilled
FMT_MSA.2	[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	FDP_ACC.1, FMT_SMR.1, see justification 3 for non-satisfied dependencies
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_SMR.1 fulfilled; there is no need 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	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 7: Dependencies of the SMC-A TOE

Justification for non-satisfied dependencies:

No. 1: The TSF according to SFR 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 support the management of logical channels the security target will describe the management security attributes of theses keys (cf. Application note 28).

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.

7.3.4 Rationale for the Assurance Requirements

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.

The *STARCOS 3.4 Health SMC-A C1* TOE shall be shown to be resistant to penetration attacks with high attack potential as described in the threats and security objectives. Therefore the component AVA_VAN.5 was included to meet the security objectives.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: basic design

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

7.3.5 Security Requirements – Mutual Support and Internal Consistency

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.

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 7.3.4 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 7.3.3 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.

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 7.3.3 Dependency Rationale.

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 7.3.3 Dependency Rationale and 7.3.4 Rationale for the Assurance Requirements. Furthermore, as also discussed in section 7.3.4 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 TOE Summary Specification

This chapter describes the TOE Security Functions and the Assurance Measures covering the requirements of the previous chapter.

8.1 TOE Security Functions

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

8.1.1 SF_AccessControl

Before the TSF performs an operation requested by a user, this Security function checks if the operation specific requirements on user identification / authorisation and protection of communication data are fulfilled. This TSF is in charge of SMC Access Control SFP.

This Security Function is composed of:

1. Maintenance of the user security attributes „identity“ and „role“.
2. Maintenance of the „roles“: Manufacturer, Personalisation Agent, Card Management System, HPC/SMC (see 7.1.5)
3. The TOE access rules in life-cycle phase 7 are as defined in the SMC Access Control SFP (see 7.1.3)
4. Performing other TSF-mediated actions in life-cycle phase 7 as defined in the FIA_UAU.1.1.
5. Access rules for the public keys of the root for CVC verification: The ability to create the public keys of the root for CVC verification is restricted to the Personalisation Agent.

This security function covers the following SFRs: FDP_ACC.1, FDP_ACF.1, FDP_ITC.1, FIA_API.1, FIA_ATD.1, FMT_SMF.1, FMT_SMR.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1/RAD_MOD, FMT_MTD.1/RAD_WR

8.1.2 SF_Administration

The administration of the TOE is managed by this Security Function. The TOE administration is done in the initialisation, personalisation and smart card end-usage phase. This TSF contains administration tasks for all of these phases.

1. The TOE manufacturer authenticates with an authentication mechanism for the initialisation phase. Only initialisation data authorised by the TOE manufacturer will be accepted by and loaded into the TOE.

The Personaliser authenticates with an authentication mechanism for the personalisation phase. The mechanism guarantees that only personalisation data will be accepted by and loaded into the TOE.

2. A mechanism to write initialisation data by the TOE manufacturer.
3. A mechanism to write personalisation data by the Personalisation Agent.
4. A mechanism for loading of new applications and management of existing applications by the Card Management System in the usage phase.

This security function covers the following SFRs: FMT_SMF.1, FMT_SMR.1, FDP_ACF.1, FMT_MTD.1/INI, FMT_MTD.1/RAD_WR

8.1.3 SF_Crypto

This Security Function provides the cryptographic support for the other Security Functions or offers cryptographic services to the users.

This Security Function is composed of:

1. Calculating hash values according to SHA-2 (256 bit) that meet FIPS 180-2 [10].
2. 3TDES calculation (encryption and decryption) and Retail-MAC (generation and verification) with 168 bits key sizes.
3. Random number generation, e.g. used for key generation and authentication process. There are two random number generators: (i) the deterministic random number generator (DRNG) is rated K4 (high) according to AIS20 [6]; (ii) a true random number generator (TRNG) based on a physical source according to AIS31 [7].
4. Support for digital signature creation and verification for authentication: Creation and verification of digital signatures according to RSA with key size of 2048 bits module length that is compliant to RSA ISO9796 2 DS1 and RSASSA-PSS. This service can be used to card-to-card authentication of the TOE against another smart card.

This security function covers the following SFRs: FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/SHA, FCS_COP.1/3TDES, FCS_COP.1/RMAC, FCS_RNG.1/DRNG, FCS_RNG.1/PHYS

8.1.4 SF_TrustedCommunication

The TOE supports secure messaging and the establishment of a trusted channel based on mutual symmetric or asymmetric authentication with or without negotiation of symmetric cryptographic keys. The established keys can be stored in persistent way and used as introduction keys.

After successful mutual authentication and establishment of symmetric session keys for secure messaging, the TOE allows for (i) the encryption of plaintext and the decryption of cipher text with the secure messaging encryption key, (ii) the MAC generation and the MAC verification with the secure messaging MAC key.

The mutual authentication is based on a challenge response protocol using the Triple DES algorithm with key sizes of 168 bits. This algorithm is also used for encryption and integrity protection of the communication data.

Via a trusted channel/path the Card Management System can authentically load new applications on the card.

This security function covers the following SFRs: FTP_ITC.1, FCS_CKM.1/Asym_Auth, FCS_CKM.1/Sym_Auth, FDP_UCT.1, FDP_UIT.1, FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FDP_ACF.1

8.1.5 SF_AssetProtection

When e.g. secure messaging keys are no longer needed in the internal memory of the TOE for calculations these parts of the memory are overwritten.

The TOE supports the calculation of block check values for data integrity checking. These block check values are stored with persistently stored assets residing on the TOE as well as temporarily stored hash values for data that is intended to be signed.

The TOE hides information about IC power consumptions and command execution time, to ensure that no confidential information can be derived from this data.

This security function covers the following SFRs: FDP_RIP.1/RES_DEAL, FDP_RIP.1/RES_AL, FDP_SDI.2, FPT_EMSEC.1, FCS_CKM.4

8.1.6 SF_TSFProtection

The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. The TOE is resistant to physical tampering of the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analysing and physical tampering.

The TOE demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections. In the case of inconsistencies in the calculation of the signature and fault injections during the operation of the TSF the TOE preserves a secure state.

This security function covers the following SFRs: FMT_LIM.1, FMT_LIM.2, FPT_PHP.3, FPT_FLS.1, FPT_TST.1.

8.2 Assurance Measures

This chapter describes the Assurance Measures fulfilling the requirements mentioned in chapter 7.2.

The following Table lists the Assurance measures and references the corresponding documents describing the measures.

Assurance Measures	Description
AM_ADV	The representing of the TSF is described in the documentation for functional specification, in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation.
AM_AGD	The guidance documentation is described in the operational user guidance documentation and in the documentation for preparative procedures.
AM_ALC	The life cycle support of the TOE during its development and maintenance is described in the life cycle documentation including configuration management, delivery procedures, development security as well as development tools.
AM_ATE	The testing of the TOE is described in the test documentation.
AM_AVA	The vulnerability assessment for the TOE is described in the vulnerability analysis documentation.

Table 8: References of the Assurance Measures

9 Conventions and Terminology

9.1 Glossary

Term	Definition
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).
Note by the ST-author	Informal note in this ST mostly to describe how an application note of the PP has been covered in the ST.
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).
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 Manufacturer 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 card holder
secure messaging in encrypted	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4

Term	Definition
mode	
Secure Module Card	Smart card providing security services in the health care environment.
SMC-PP	Protection Profile of the Secure Module Card
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]).

9.2 Acronyms

Acronyms	**Term**
APDU	Application Protocol Data Unit
ATR	Answer To Reset
CA	Certification Authority
C.CA_SMC.CS	Certificate of the CSP for CVCs in the health care environment
C.SMC.AUTR_CVC	Card Verifiable Authentication Certificate for role authentication
C.SMC.AUTD_RPS_CVC	Card Verifiable Authentication Certificate as remote PIN sender
C2C-authentication	Card to Card authentication
CA	Certification authority
CAMS	Card Application Management System
CC	Common Criteria
CHA	Certificate Holder Authorization
CHR	Certificate Holder Reference
COS	Card Operating System
CSP	Certification service provider
CVC	Card Verifiable Certificate
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
DF	Dedicated File
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DRNG	Deterministic RNG
DTBS	Data to be signed

Acronyms	**Term**
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable ROM
EF	Elementary File
eHC	Electronic health card
ES	Embedded Software
GDO	Global Data Object
HPC	Health professional card (German: HBA)
HBA	Heilberufsausweis
HCI	Health Care Institution
IC	Integrated Circuit
ICC	Integrated Circuit Card
I/O	Input/Output
IP	Internet Protocol
MAC	Message Authentication Code
MF	Master File
MSE	Manage Security Environment
OE	Objective on the TOE environment
OS	Operating System
OSP	Organizational Security Policy
OT	Objective on the TOE
PP	Protection Profile
PKI	Public Key Infrastructure
PSO	Perform Security Operation
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
PuK.SMC.AUTD_RPS_CVC	Card Authentication Public Key as remote PIN sender
RC	Retry Counter
RCA	Root CA
RFID	Radio Frequency Identification
RNG	Random Number Generator
ROM	Read Only Memory

Acronyms	**Term**
RSA	Rivest Shamir Adleman
SAR	Security assurance requirements
SE	Security Environment
SF	Security Function
SFP	Security Function Policy
SFR	Security functional requirement
SHA	Secure Hash Algorithm
SM	Secure Messaging
SMA	Secure Module Application
SMC	Secure module card
SMC PP	Protection Profile of the Secure module card
SMD	Secure Module Data
SOF	Strength of Function
ST	Security Target
TDES	Triple DES
TOE	Target of Evaluation
TRNG	True RNG
TSF	TOE security functions

10 References

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3 Final, CCMB-2009-07-001, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 3 Final, CCMB-2009-07-002, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 3 Final, CCMB-2009-07-003, July 2009

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB-2009-07-004

[5] Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0, CCDB-007-09-001

[6] Anwendungshinweise und Interpretationen zum Schema, AIS20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 1, 02.12.1999, Bundesamt für Sicherheit in der Informationstechnik

[7] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

Cryptography

[8] BSI TR-03116 Technische Richtlinie für die eCard-Projekte der Bundesregierung. Sicherheitsvorgaben für den Einsatz kryptographischer Verfahren der elektronischen Gesundheitskarte (eGK), des Heilberufeausweises (HBA) und technischer Komponenten der Common Criteria Protection Profile Version 1.95, 29th August 2008 Secure Module Card Bundesamt für Sicherheit in der Informationstechnik 87 of 88 Telematikinfrastruktur des Gesundheitswesens, Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, Version 1.0, 23.03.2007

[9] Federal Information Processing Standards Publication 46-3 DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[10] 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

[11] PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, 2002-06-14

Protection Profiles

[12] Protection Profile Secure Signature Creation Device (SSCD) Type 3, CEN/ISSS by ESIGN Workshop – Expert Group F, Version 1.05, 25 July 2001, registered as BSI-PP-0006-2002

[13] Common Criteria Protection Profile Secure Module Card Type A (PP-SMC-A), BSI-PP-0019-V3, Version 1.2, 17th November 2009

[14] Security IC 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

Other

[15] 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, Bundesapothekenkammer, Deutsche Krankenhaus-Gesellschaft

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

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

[18] Spezifikation der SMC-K, Einführung der Gesundheitskarte, gematik mbH, Version 1.2.0 RC4 (in Bearbeitung), 15.09.2009

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

[20] Einführung der Gesundheitskarte, Registrierung einer CVC-CA der zweiten Ebene, gematik mbH, Version 1.5.0, 18.03.2008

[21] Security Target Lite, P5CC052V0A, BSI-DSZ-CC-0466-2009, Rev. 1.5, 09.07.2009

[22] Certification Report BSI-DSZ-CC-0466-2008 for Smart Card Controller P5CC052V0A with specific IC Dedicated Software from NXP Semiconductors Germany GmbH, 24.06.2008

[23] Assurance Continuity Maintenance Report, BSI-DSZ-CC-0466-2008-MA-01, NXP Smart Card Controller P5CC052VA with specific IC Dedicated Software, 8.September 2009