Security Target Lite STARCOS 3.4 Health HBA C1

Version 2.0/09.06.2011

Author: Giesecke & Devrient GmbH
Document status: Final

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

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

Content

1 Introduction

1.1 TOE Reference

This document refers to the following TOE(s):

1) STARCOS 3.4 Health HBA C1

1.2 ST Reference and ST Identification

Title: Security Target Lite STARCOS 3.4 Health HBA C1

Version Number/Date: Version 2.0/09.06.2011

Origin: Giesecke & Devrient GmbH

TOE: STARCOS 3.4 Health HBA 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 HBA C1
- Generic Application of STARCOS 3.4 Health HBA C1
- STARCOS 3.4 SmartCard Operating System Reference Manual
- Smart Card Application Verifier

HW-Part of TOE: NXP P5CC052V0A (Certificate: BSI-DSZ-CC-0466-2008 [4], Assurance Continuity Maintenance Report: BSI-DSZ-CC-0466-2008-MA-01, [31])

1.3 TOE Overview

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

The related product is the STARCOS 3.4 Operating System (OS) on a Smart Card Integrated Circuit. It is intended to be used Health Professional Card (HBA) in the German telematics system and also as Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC [1] , so the TOE consists of the part of the implemented application software in combination with the underlying

hardware ('Composite Evaluation'). The functional and assurance requirements for SSCDs defined in Annex III of this EU Directive [1] have been included into the Protection Profile (PP) for Health Professional Cards with SSCD Functionality. The 'Security Target Lite STARCOS 3.4 Health HBA C1' is compliant to this PP [2].

STARCOS 3.4 is a fully interoperable ISO 7816 compliant multiapplication Smart Card OS, including a cryptographic library. The EU compliant Electronic Signature Application is designed for the creation of legally binding Qualified Electronic Signatures as defined in the EU Directive [1]. The various features of STARCOS 3.4 allow for additional health system related applications.

The software part of the TOE is implemented on the certified NXP P5CC052V0A [4], [31]. So the TOE consists of the software part and the underlying hardware. The RSA2048 crypto library provided with the underlying hardware is not used in this composite TOE. The corresponding Security Target (Lite) [5] is compliant to the BSI-PP-0002-2001 [6].

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 TOE is CC **EAL4+**.

1.4 Sections Overview

Section 1 provides the introductory material for the Security Target.

Section 2 provides the TOE description.

Section 3 contains the conformance claims.

Section 4 contains the Security Problem Definition

Section 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.

Section 6 contains the Extended component definition.

Section 7 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [9] and Part 3 [10] that must be satisfied.

Section 8 contains the TOE Summary Specification.

Section 9 provides information on applied conventions and used terminology.

Section 10 contains explanations for the PP application notes.

Section 11 provides a list of references used throughout the document.

2 TOE Description

2.1 Overview

The Target of Evaluation (TOE) is the Health Professional Card (HPC, German "Heilberufsausweis"). HPC is a contact based smart card which is conformant to the specification documents [21] and [22].

The TOE consists of

- TOE_IC, consisting of:
  the circuitry of the HPC'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 HPC applications (data structures and their content)
- TOE_GD
  the guidance documentation delivered together with the TOE.

The TOE provides the following main security services:

(1) Authentication of the cardholder by use of a PIN,

(2) Access control for the function (3) to (9) listed below,

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

(4) Asymmetric card-to-card authentication between the HPC and a SMC with either establishing a trusted channel or with storage of introduction keys,

(5) Symmetric card-to-card authentication between the HPC and a SMC with establishing a trusted channel,

(6) Document key decipherment and transcipherment,

(7) Client-server authentication,

(8) Generation of digital signatures[1],

(9) Terminal Support Service for random number generation.

[1] The SSCD generates digital signatures which are qualified electronic signatures if they are based on a valid qualified certificate at the time of signature creation (cf. SigG [27], § No. 3)

2.2 TOE usage and security features for operational use

The TOE is used by an individual acting as accredited health professional

(1) to authenticate themselves for access to the application data of a patient which are handled by the eHC or by the infrastructure of the health care service,

(2) to authorize health employees using a Security Module Card (SMC) for access to medications data and medical data on the eHC or handled by the infrastructure of the health care service in case of emergency,

(3) to decrypt and transcipher keys of encrypted application data,

(4) to sign documents.

The following list provides an overview of the mandatory security services provided by the HPC 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. Note the HPC provides optional security services like the organization-specific authentication application, which are not covered by the current security target.

Service_User_Auth_PIN: The cardholder authenticates himself with his PIN or PUK.

This service is meant as a protection of the other services, which require user authentication. In addition it provides privacy protection because certain data in the card (or secured by the card) can only be accessed after user authentication. The HPC handles different PIN for signature-creation PIN.QES (cf. Service_Signature_Creation) and for other services PIN.CH (cf. Service_Asym_Mut_Auth_w/o_SK, Service_Client_Server_Auth and Service_Key_Decryption).

The HPC supports functions to change the PIN and to unblock the PIN (reset the retry counter). The HPC holds different PIN unblocking keys (PUK) for different PIN. The successful presentation of PUK.CH[2] allows unblocking and changing the PIN.CH. The successful presentation of PUK.QES allows only unblocking the associated PIN. The HPC supports to change the PIN and to unblock the PIN with secure messaging (used for remote PIN entry) and without secure messaging (used for local PIN entry, cf. [24] and TR-03114 [12] for details)

Service_Asym_Mut_Auth_w/o_SK[3]: Mutual Authentication using asymmetric techniques between the HPC and an eHC or a SMC without agreement of a symmetric key ([21], chapter 15, [22], section 6.1.4).

This service is meant for situations, where the eHC requires authentication by a HPC or SMC and the SMC requires authentication by HPC to provide access to protected data.

---

[2] This ST defines the names PUK.CH and PUK.QES, to distinguish between the PUK for PIN.CH, and the PUK for PIN.QES. These names are not defined in the HBA specification [22].

[3] The Abbreviation SK here stands for symmetric key, which is the card security protocol agreeing a symmetric key for a trusted channel (cf. e.g. [21], sec. 15).

This service 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 [21], 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 [21], section 15).

Service_Asym_Mut_Auth_with_SM: Mutual Authentication using asymmetric techniques between the HPC and a SMC with agreement of symmetric keys and establishment of a trusted channel by means of secure messaging after successful authentication. The TOE supports secure messaging by means encryption of data, decryption of data, generation of MAC and verification of MAC (cf. for details to [21], section 6.6). The keys of a secure messaging channel are stored temporarily.

This service is meant for situations, where the HPC and a SMC establish a trusted channel by means of secure messaging, i.e. the communication is secured by a MAC and may additionally be encrypted. 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 [21], 15.4.4). This service uses the commands INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE with algorithmic identifiers '*rsaSessionkey4SM'* (cf. for details to [22], section 7.1.3).

Service_Asym_Mut_Auth_with_Intro: Card-to-Card authentication using asymmetric techniques between the HPC and a SMC with storage of symmetric Introduction Keys after successful authentication (cf. for details to [22], sec 7.1.4). The agreed keys are stored permanently with the identity of the entity holding the same cryptographic key.

This service is meant for situations, where a manageable number of HPCs, SMC-As/SMC-Bs and SMC-Ks frequently interact with each other. 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 SMC CVC certificate is stored as key reference after adjusting the index (first byte of CHR) to the computed key material. This service runs a protocol similar to the Service_Asym_Mut_Auth_with_SM, but the algorithmic identifier is '*rsaSessionkey4Intro*' for both authentication commands (cf. for details to [22], section 7.1.4). The authentication related data contain data elements for key computation. The symmetric introduction keys, which are stored this way, will perform the same tasks as the two asymmetric 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_SM: Mutual Authentication using symmetric techniques between the HPC and an external entity with establishment of a trusted channel with secure massaging.

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, firstly the command INTERNAL AUTHENTICATE with algorithmic identifier ‘*desSessionkey4SM*‘ is received by the HPC to authenticate itself to an external entity by encrypting a random number which was generated by the SMC and included in the command 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*’ (cf. for details to [22], 7.1.4).

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.

Service_Client_Server_Auth: The HPC implements a PKI application, which in particular allows usage the TOE as an authentication token for a client/server authentication (by means of an asymmetric method using X.509 certificates, [22], 10.1.5). The cardholder authenticates himself with his PIN in order to access this service.

This service may for example be useful if the cardholder wants to access a server provided by the health insurance organisation, where confidential data of the cardholder are managed. So it can also be seen as an additional privacy feature.

Service_Key_Decryption: The HPC implements a PKI application, which in particular allows usage of the TOE as a data decryption token for Document Cipher Key Decipherment ([22], section 10.7) and Document Cipher Key Transcipherment ([22], section 10.8). Symmetric document encryption keys, which are encrypted with the cardholder’s public key can only be decrypted with the help of the card. Additionally, the HPC implements transcipherment of symmetric document keys as decryption with the cardholder private key and encryption with some imported public key in one command without export of the symmetric document key. The cardholder authenticates himself with his PIN in order to access this service.

This is meant for situations, where confidential data are stored on a server, but shall only be accessible with the cardholder's permission. So it can also be seen as a privacy feature.

Service_Signature_Creation: The HPC is used as SSCD Type 3 to generate SCD/SVD pair and digital signatures. The generation of the SCD/SVD pair includes storing of the SCD and export of the SVD. These digital signatures are qualified electronic signatures if a qualified certificate for the holder of signature-creation data (SCD) and containing the corresponding signature-verification data (SVD) is valid at the time of signature-creation. The HPC stores the qualified certificate and attribute certificates of the cardholder but the HPC does not check their validity at time of signature-creation. After successful authentication the HPC allows generation (i) exactly 1 digital signature ("single-signature") or (ii) more than 1 signature ("multiple-signature") if the data-to-be-signed are sent by an authorised signature-creation application.

Terminal Support Service: The HPC provides random number generation for the operational environment, e.g. mobile card terminals.

Service_Load_Application: The HPC provides an option for the authorized user Card management system to load and to install new application in form of a new folder including a sub-tree (i.e. dedicated files (DF) in the Root Application (MF)) and a new elementary file (EF) including content in the Health Professional Application (DF.HPA) after delivery to the cardholder (operational state is activated).

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

- Specification German Health Professional Card and Security Module Card - Part 1: Commands, Algorithms and Functions of the COS Platform, Version 2.3.0, 04.07.2008, BundesÄrzteKammer, Kassenärztliche Bundesvereinigung, BundesZahnÄrzteKammer, BundesPsychotherapeutenKammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft
- Specification German Health Professional Card and Security Module Card - Part 2: HPC Applications and Functions, Version 2.3.0, 04.07.2008, BundesÄrzteKammer, Kassenärztliche Bundesvereinigung, BundesZahnÄrzteKammer, BundesPsychotherapeutenKammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft

2.3 Structural view of the TOE

The TOE is realised by a smartcard, consisting of the embedded software residing on the underlying certified IC. The TOE comprises the certified chip, the operating system

STARCOS 3.4, the documentation (Guidance Documentation of STARCOS 3.4 Health HBA C1, Generic Application Specification of STARCOS 3.4 Health HBA C1, Smart Card Application Verifier[4]). The operating system STARCOS 3.4 is implemented in the ROM area of the IC, whereas some parts may also reside in the EEPROM; these parts are optional supplements or corrections to the operating system which may be added after mask production. The file system containing the application data is installed in the EEPROM of the IC. Besides the files for the HPC and SSCD applications there may be additional files for other applications, e.g. for the health system, which do not belong to the TOE. The file system part of the TOE is represented by the Guidance Documentation and the Generic Application Specification that define the security relevant parts of the file system. The Smart Card Application Verifier verifies the correctness of the file system after installation of the TOE.

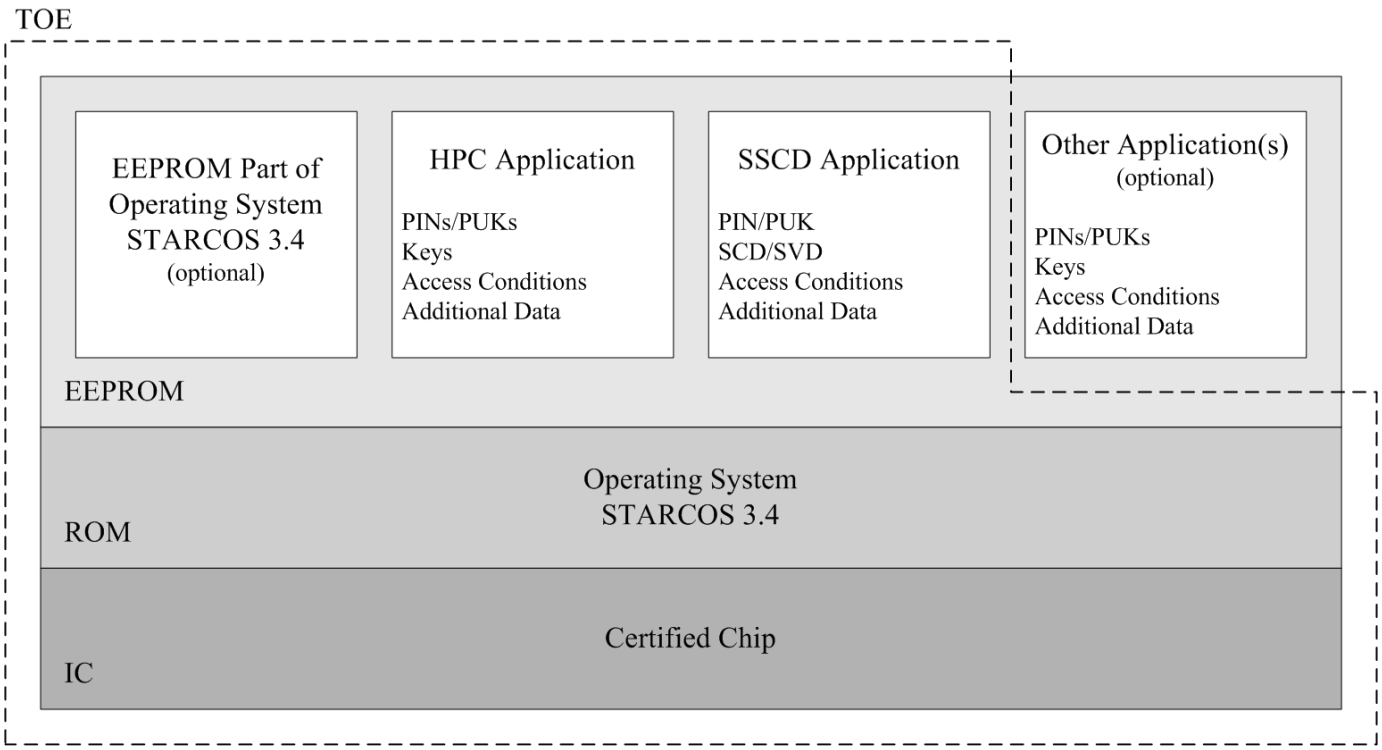


Figure 1: TOE structure (after installation)

[4] The Smart Card Application Verifier and the corresponding representation of Generic Signature Application STARCOS 3.4 Health HBA C1 are not part of the TOE delivery. They are solely used by G&D to verify that the signature application conforms to the requirements of the Generic Signature Application STARCOS 3.4 Health HBA C1.

2.4 TOE life cycle

2.4.1 TOE life cycle phases

The TOE life cycle is shown in Figure 2. Basically, it consists of a Development Phase and the Usage Phase.

The Development Phase comprises the development and the production of the TOE (cf. [8], para.157).

The TOE Development Phase includes

(1) Development of the TOE embedded software (TOE_ES)

(2) Development of the TOE applications (TOE_APP)

(3) Production of the TOE integrated circuit (TOE_IC), including the IC design, development of the IC Dedicated Software, inclusion of the ROM mask part of the embedded software and IC packaging

The Development Phase is subject of the evaluation according to the assurance life cycle (ALC) class. The Development Phase ends with the delivery of the TOE parts for TOE preparation. The measures for delivery of the TOE for preparation are subject to ADO_DEL.

The usage phase of the TOE comprises the preparation phase (i.e. initialisation and personalisation of the TOE) and the operational use.

The preparation phase of the TOE life cycle is processing the TOE from the customer's acceptance of the delivered TOE to a state ready for operational use by the end user. The preparation includes

(1) The initialization of the TOE
   (a) import of the initialisation part of the embedded software
   (b) import of the TOE applications
   (c) optionally generation of key pairs by the TOE, storage of the private keys in the TOE

(2) The personalization of TOE for use by the end user,
   (a) import of end user or card individual data e. g. the installation of PINs and PUKs in the TOE.
   (b) generation of key pairs by the TOE and storage of the private keys in the TOE. Afterwards, the public keys is exported to a CSP which generates a certificate over the public keys. The certificate may later on be imported from the CSP’s directory service.

(3) Testing of the TOE

(4) The preparation may include generation of certificates (e. g. for qualified electronic signatures) and optional loading of certificates or certificate info into the SSCD functionality of the TOE for signatory convenience.

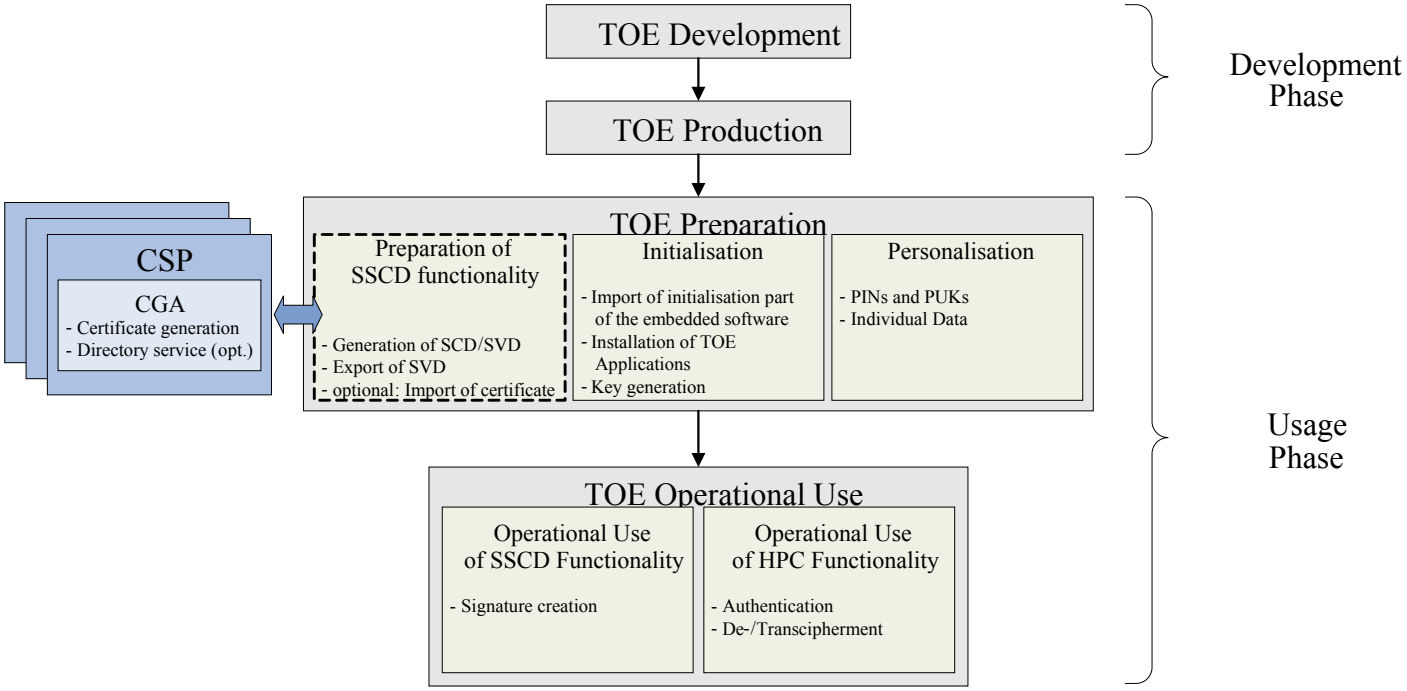


Figure 2: TOE life cycle

The operational phase of the TOE starts when the end user takes control over the TOE. During the operational phase the end user can use the HPC functionality of the TOE and the SSCD functionality as signatory.

Card applications can be managed using a Card Management System during the operational phase.

The TOE life cycle as SSCD ends when the SCD implemented in the TOE is destroyed. This might be done by physically destroying the smart card chip.

2.4.2 Delivery of ROM-Mask and initialisation data

As shown in Figure 1, the software part of the TOE consists of the STARCOS 3.4 operating system located in the ROM of the IC and the file system located in the EEPROM. Parts of the operating system may also reside in the EEPROM. The Operating System Developer (i.e. G&D) creates the ROM mask and sends this representation of the operating system together with secret data allowing secure loading of initialisation data to the Chip Manufacturer (see Figure 3). The Chip Manufacturer manufactures the chips including the operating system and stores the secret data in a special area of the EEPROM of the chip and delivers the chips packaged in modules to the Initialiser. The secret data is used by the OS Developer to secure the initialisation data which is sent afterwards to the Card Initialising Facility. The Card Initialising Facility manufactures the cards, performs the initialisation and then delivers the cards to the Personalising Facility.

With the secured initialisation data secret data is imported into the TOE allowing secure loading of personalisation data. This secret data is sent by the OS Developer to *the card* issuer who uses it to secure the personalisation data and then send the secured personalisation data to the Personalising Facility which performs the personalisation before issuance of the TOE.

During the personalisation before issuance, trust anchors can be imported into the TOE to allow a completion of the personalisation after issuance.

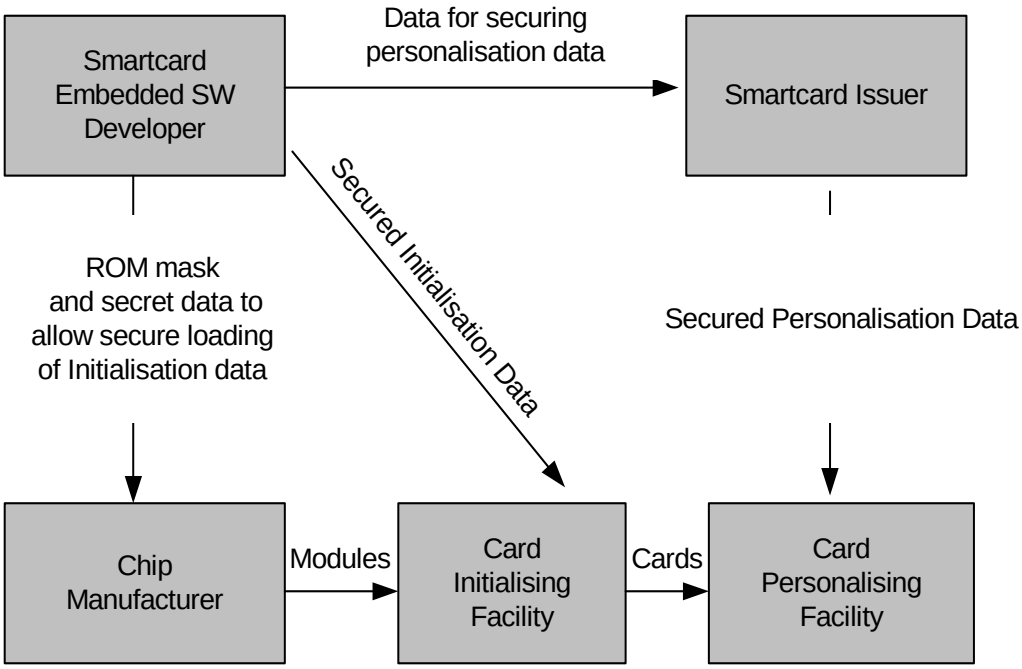


Figure 3: ROM Mask and initialisation data delivery

3 Conformance Claims

3.1 CC Conformance Claim

This Security Target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 3, July 2009, CCMB-2009-07-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; Version 3.1, Revision 3, July 2009, CCMB-2009-07-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 3, July 2009, CCMB-2009-07-003

as follows

- Part 2 extended,
- Part 3 conformant.

3.2 PP Conformance Claim

This ST claims strict conformance to:

- Protection Profile – Health Professional Card (PP-HPC) with SSCD functionality, Version 1.10, 17.November 2009, BSI-CC-PP-0018-V3

3.3 Package Conformance Claim

This ST conforms to assurance package EAL4 augmented with AVA_VAN.5 defined in CC part 3 [10].

3.4 Conformance Claim Rationale

This security target is conformant to the claimed PP [2].

The TOE type is a contact based smart card (see chapter 2.1), which is consistent with the TOE type in the PP [2], chapter 1.2.2.

The Security Problem Definition (chapter 4) is taken directly from the PP [2], 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: *OT.Lifecycle_Security*. The remaining security objectives are identical with those from the PP [2].

The security requirements (chapter) 7 have been taken directly from the PP [2] (chapter 6) and operations as appropriate have been performed.

4 Security Problem Definition

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

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

4.1 Introduction

4.1.1 Assets

The assets to be protected by the TOE are data listed in Table 1 and the security services provided by the TOE as defined above. The data assets known to the TOE environment like public keys shall be protected by the TOE environment as well.

Name of data asset	Description	Operation by commands[5]
Certificate of the Certificate Service Provider (C.CA_HPC.CS)	C.CA_HPC.CS contains the card verifiable certificate of the Certificate Service Provider, issued by the Root CA for Health Care for a Certificate Authority HPC. It contains the public key PuK.CA_HPC.CS for verification of the card verifiable certificates like C.HPC.AUTR_CVC. It is part of the user data provided for the convenience of the IT environment. The integrity of this data shall be protected. If this data is provided by the IT environment it shall be verified	SELECT, READ BINARY

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

Name of data asset	Description	Operation by commands[5]
	by means of PuK.RCA.CS	
Card Authentication Private Key (PrK.HPC.AUTD_ SUK_CVC)	The card authentication private key PrK.HPC.AUTD_SUK_CVC is for C2C-authentications between HPC and SMC-A/B for PIN transfer and between HPC and SMC-K for DTBS transfer to the HPC **with** establishing a trusted channel by means of secure messaging or with storing of introduction keys. It is part of the user data , which confidentiality and integrity shall be protected.	INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE
Card Verifiable Authentication Certificate (C.HPC.AUTD_ SUK_CVC)	C.HPC.AUTD_SUK_CVC contains the card verifiable certificate of the HPC for card-to-card device authentication between HPC and SMC-A/B/K with HPC as signature card capable of stack and comfort signatures (“Stapel- und Komfortsignatur” SUK) to receive PIN data and data to be signed (DTBS). It contains the public key PuK.HPC.AUTD_SUK_CVC as authentication reference data corresponding to the private authentication key PrK.HPC.AUTD_SUK_CVC. It is part of the user data provided for use by external entities as authentication reference data of the HPC and is stored in the file EF.C.HPC.AUTD_SUK_CVC, whose integrity shall be protected.	SELECT, READ BINARY
Card Authentication Private Key (PrK.HPC.AUTR_ CVC)	The card authentication private key PrK.HPC.AUTR_CVC is for C2C-authentications between HPC and eGK/CAMS **with** or **without** establishing a trusted channel by means of secure messaging, and for authoriza-	INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE

Name of data asset	Description	Operation by commands[5]
	tion of SMC-A and SMC-B.	
Card Verifiable Authentication Certificates (C.HPC.AUTR_ CVC)	C.HPC.AUTR_CVC is the card verifiable certificate of the HPC for card-to-card role authentication between HPC and eHC and for SMC-A, SMC-B authorization. It contains the public key PuK.HPC.AUTR_CVC as authentication reference data corresponding to the private authentication key PrK.HPC.AUTR_CVC. It is part of the user data provided for use by external entities as authentication reference data of the HPC and is stored in the file EF.C.HPC.AUTR_CVC, whose integrity shall be protected.	SELECT, READ BINARY
Client-Server Authentication Private Key (PrK.HP.AUT)	The Client-Server Authentication Private Key PrK.HP.AUT is an asymmetric cryptographic key used for the authentication of an client application acting on behalf of the cardholder to a server. It is part of the user data, which confidentiality and integrity shall be protected.	INTERNAL AUTHENTICATE, PSO: COMPUTE DIGITAL SIGNATURE (P2 = ‘9E’ or ‘AC’)
Client-Server Authentication Certificate (C.HP.AUT)	C.HP.AUT is a X.509 Certificate for the Client-Server Authentication, which contains the public key PuK.HP.AUT corresponding to the Client-Server Authentication Private Key PrK.HP.AUT. It is part of the user data provided for use by external entities as authentication reference data of the HPC (cf. to [22], sec. 10.6, for details), which integrity shall be protected.	SELECT, READ BINARY
Decipher Private Key (PrK.HP.ENC)	The Document Cipher Key Decipher Key PrK.HP.ENC is asymmetric private key used for document decryption on behalf of the cardholder. It is part of the user	PSO: DECIPHER, PSO: TRANSCIPHER

Name of data asset	Description	Operation by commands[5]
	data, which confidentiality and integrity shall be protected.	
Encryption Certificate (C.HP.ENC)	C.HP.ENC is the X.509 Certificate for document enciphering, which contains the public document encipher key PuK.HP.ENC corresponding to the private document decipher key PrK.HP.ENC (cf. to [22], sec. 10.7, for details). It is part of the user data provided for use by external entities, which integrity shall be protected.	SELECT, READ BINARY
Signature-creation data (PrK.HP.QES)	Private key as signature-creation data corresponding to the qualified certificates of the Signatory. It is part of the user data, which confidentiality and integrity shall be protected.	PSO: DIGITAL SIGNATURE, PSO: GENERATE ASYMMETRIC KEY PAIR
Qualified certificates (C.HP.QES, C.HP.QES-AC1, C.HP.QES-AC2, C.HP.QES-AC3)	C.HP.QES, C.HP.QES-AC1, C.HP.QES-AC2 and C.HP.QES-AC3 are qualified certificates of the Signatory containing Puk.HP.QES and are stored in EFs of DF.QES (cf. to [22], sec. 9.1, for details). C.HP.QES is the X.509v3 public key certificate of the health professional for the qualified electronic signature service according to SigG/SigV. HP.QES-AC1, -AC2 and -AC3 may be empty They are part of the user data provided for use by external entities. The integrity of these data shall be protected.	SELECT, READ BINARY
Security State Evaluation Counter (EF.SSEC)	stores the maximum values of SSEC in EF.SSEC	SELECT, READ BINARY
Data to be signed (DTBS)	Data to be signed with PrK.HP.QES, i.e. hashed data send with command PERFORM SECURITY OPERATION: COMPUTE DIGITAL SIGNATURE after PrK.HP.QES was selected by	PSO: COMPUTE DIGITAL SIGNATURE

Name of data asset	Description	Operation by commands[5]
	MANAGE SECURITY ENVIRONMENT. (cf. to [22], sec. 9.8, for details)	
Health Professional Data (HPD)	Personal data of the smart cardholder (stored in the file EF.HPD located in DF.HPA). It is part of the user data. The integrity of this data shall be protected.	SELECT, READ BINARY UPDATE BINARY
Display message (DM)	The display messages are contained in independent EF.DMs being located in both the DF.QES and DF.ESIGN. A terminal is allowed to read out the corresponding display message if secure messaging with encoded response data to a authenticated SMC-A, SMC-B or SMC-K (SCD) is established. It is part of the user data which confidentiality and integrity shall be protected.	SELECT, READ BINARY UPDATE 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.HPA, DF.QES, DF.CIA.QES, DF.ESIGN, DF.CIA.ESIGN, and DF.AUTO according to ISO/IEC 7816-4.	SELECT, READ RECORD, SEARCH RECORD, APPEND RECORD, UPDATE RECORD
EF.GDO	EF.GDO contains the DO ICC Serial Number.	SELECT, READ BINARY
EF.VERSION	The EF.Version with linear fixed record structure contains the version numbers of the specification, which the card is compliant to.	SELECT, READ RECORD, SEARCH RECORD, UPDATE RECORD

Name of data asset	Description	Operation by commands[5]
Random number	Random number generation	GET RANDOM

Table 1: Assets of the HPC

TSF data	Description	Operation in terms of commands
Root Public Key of the Certificate Service Provider (PuK.RCA.CS)	The public key PuK.RCA.CS of the Health Care Root CA for verification of the card verifiable certificate of the certificate service provider for card verifiable certificates in the health care environment (cf. to [22], sec. 4.3.11, for details). It is part of the TSF data which integrity shall be protected.	PSO VERIFY CERTIFICATE
Public Key of the CAMS (PuK.CAMS_HPC.AUT_CVC)	The public key PuK.CAMS_HPC.-AUT_CVC used for authenticate an external Card Management System (CAMS)	EXTERNAL AUTHENTICATE
Symmetric Authentication Key(s) (SK.HPC.AUT)	The TOE may store a Symmetric Authentication Key for the Service_Sym_Mut_Auth_with_SM. A Symmetric Authentication Key agreed upon and stored by Service_Asym_Mut_Auth_with_Intro.	INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE
Cardholder Authentication Reference Data for PIN.CH and PUK.CH	The Cardholder Authentication Reference Data are used to verify the user attempt to activate certain functions of the TOE except the QES application and organization-specific applications. This data include PIN.CH and PUK.CH. They are part of the TSF data which confidentiality and integrity shall be protected.	CHANGE RD (Option ‘00’), GET PIN STATUS, RESET RC (Option ‘00’ and ‘01’), VERIFY
Signatory Authentication	The Signatory Authentication Reference Data are used to verify the	CHANGE RD (Option ‘00’), GET PIN STATUS,

Reference Data for PIN.QES and PUK.QES	user attempt to activate the QES application of the TOE. This data include PIN.QES and PUK.QES. They are part of the TSF data which confidentiality and integrity shall be protected.	RESET RC (Option '01'), VERIFY
TOE pre-personalization data	Data stored in the TOE during pre-personalization process. It may contain user data and TSF data.	SELECT, READ BINARY UPDATE BINARY
TOE initialization data	Data stored in the TOE during the initialization process. It may contain user data and TSF data.	

Table 2: TSF data of the HPC

Application note 1: The Card Authentication Private Keys (PrK.HPC.AUTD_SUK_CVC, PrK.HPC.AUTR_CVC), the Client-Server Authentication Private Key (PrK.HP.AUT), and the Document Cipher Key Decipher Key (PrK.HP.ENC) are used as cryptographic keys by the TOE security services provided to the user. Therefore they are assessed as user data. The PKI under the Root CA Health Care is introduced in [22], ch. 6. The public key PuK.RCA.CS is used as authentication reference by TSF for card authentication. The Cardholder Authentication Reference Data (PIN.CH and PUK.CH) and the Signatory Authentication Reference Data (PIN.QES, PUK.QES) are used as authentication reference by TSF for human user authentication.

4.1.2 User and subjects

This security target considers the following users, roles and subjects acting for them.

Name of user and subject acting for them	**Description**
Health Professional	Holder of the HPC for whom the HPC is personalized to use of the HPC applications. The Health Professional may use the HPC in two roles: Cardholder Role and Signatory Role[6].
Cardholder Role	Role, which controls the use of the HPC applications except the QES application and organization-specific applications. The user authorised for this role knows the

[6] The TOE may contain the optional Organization-specific Authentication Application, which additionally foresees the roles in Accordance to the identification and authentication objects PIN.SO and PIN.AUTO.

Name of user and subject acting for them	Description
	user authentication verification data corresponding to PIN.CH and PUK.CH.
Signatory Role	Role, which controls the use of the QES application. The user authorised for this role knows the user authentication verification data corresponding to PIN.QES and PUK.QES.
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. The signatory may use signature-creation application with the role “terminal” (i.e. is not using the role ”Authorised signature-creation application”) to generate only one signature after successful authentication with PIN.QES.
Security Module Card	External entity possessing the private key corresponding to the public key in a card verifiable certificate of the PKI under the Health Care Root CA with a corresponding cardholder authorization of SMC.
Electronic Health Card (eHC)	External entity possessing the private key corresponding to the public key in a card verifiable certificate of the PKI under the Health Care Root CA with a corresponding cardholder authorization of eHC.
Authorised signature-creation application (ASCA)	External entity possessing the private key corresponding to the public key in a card verifiable certificate of the PKI under the Health Care Root CA with a corresponding cardholder authorization of signature-creation application (SCA). The signatory uses an authorized SCA to generate more than one signature after successful authentication with PIN.QES.
Unauthorised user	A user who is trying to interact with the TOE as Card Management System, Cardholder or SMC without being authenticated for this role.

Table 3; User and roles of the TOE

Application note 2: The smart cards in the health care environment possess card verifiable certificates (CVC) with cardholder authorizations (CHA) identifying them as

HPC, eHC and SMC as defined in [21], Chapter 7. The CHA role identifier (ID) is coded in 1 byte.

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 organisational 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.HPC_Spec **Compliance to HPC specifications**

The HPC shall be implemented according to the specifications:

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

Specification German Health Professional Card and Security Module Card - Part 2: HPC Applications and Functions, Version 2.3.0, 04.07.2008, BundesÄrzteKammer, Kassenärztliche Bundesvereinigung, BundesZahnÄrzteKammer, BundesPsychotherapeutenKammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft

OSP.Enc **Document decryption and transcipherment**

The HPC provides services for document cipher key decipherment and document cipher key transcipherment in order to support document encryption, decryption and transcipherment provided by the operational environment. It holds a private key and a certificate for the corresponding public key. The service for transcipherment imports the public key for the encipherment of the deciphered symmetric key.

OSP.CSA **Client-Server-Authentication**

The HPC provides service for digital signature creation in order to support client / server authentication provided by the operational environment. It holds a private key and a certificate for the corresponding public key.

OSP.CSP_QCert Qualified certificate

The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Signature Law [27], i.e., inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

OSP.QSign Qualified electronic signatures

The signatory uses a signature-creation system to sign data with qualified electronic signatures. The qualified electronic signature is based on a qualified certificate (according to SigG [27]) and is created by the HPC as an SSCD. The SCA presents the DTBS to the signatory and sends the DTBS selected by the signatory to the HPC. After successful authentication with the PIN.QES the DTBS are signed. In case that a signatory intends to generate more than one signature after one successful authentication with PIN.QES, the signatory has to use an authorized SCA.

OSP.Sigy_SSCD TOE as secure signature-creation device

The TOE meets the requirements for SSCD laid down in SigG [27] and SigV [26]. This implies the SCD is used for signature creation under sole control of the signatory and the SCD can practically occur only once.

OSP.Sig_Non-Repud Non-repudiation of signatures

The life cycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in his un-revoked certificate.

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.

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. guessing of the user authentication data (PIN) or 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 e.g. to add keys for decipherment of documents. The attacker may misuse the TSF management function to change the user authentication data to a known value.

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.

This threat comprises several attack scenarios e.g. the attacker may try to circumvent the user authentication to use the DECIPHER command for document keys without authorization. The attacker may try to alter the TSF data e.g. to extend the user rights after successful card-to-card authentication.

T.SCD_Divulg Storing, copying, and releasing of the signature-creation data

An attacker stores or copies the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE.

T.SCD_Derive Derive the signature-creation data

An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

T.DTBS_Forgery Forgery of the DTBS-representation

An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intended to sign.

T.Sig_Forgery Forgery of the electronic signature

An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.Intercept Interception of Communication

An attacker with high attack potential tries to intercept the communication between the TOE and SMC 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. Attacker may read the document keys output by the TOE as a DECIPHER command response.

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 addresses 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 disclosure 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 has been 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 of the assumption.

A.Pers_CAMS **Personalization and management of the Smart Card**

During Personalisation and when using the option of Card Management System, the initial personalisation and additional management steps during the end-usage phase shall be performed correctly according to the specifications [22]. Furthermore the correctness, the quality and - if necessary - the confidentiality of all data structures and data on the card shall be ensured.

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

The cardholder of the TOE uses the TOE adequately. In particular he does not tell the PIN (or PINs) to others and does not 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.

A.CGA **Trustworthy certification-generation application**

The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.

A.SCA **Trustworthy signature-creation application**

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

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 security 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_CAMS **Access control for management**

The TOE must ensure that the authorized Card Management System can create, write and update the User data and the TSF data related to cardholder functions only except modification of the cardholder authentication reference data managed by the cardholder. The TOE must ensure that the authorized Administrator can create, write and update the User data and the TSF data related to qualified electronic signature except (i) the use of the SCD, (ii) change of the security attribute “operational” and the modification of the authentication reference data of the signatory.

OT.Data_Confident **Confidentiality of internal data**

The TOE must ensure the confidentiality of the User Authentication Reference Data, the Card Authentication Private Keys, the Decipher Private Key, the Client-Server Authentication Private Key, Signature-creation Data and other confidential user data and TSF data under the TSF scope of control against attacks with high attack potential. The

TOE allows reading the display message only an authenticated corresponding SMC after establishing secure messaging.

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 Decipher Private Key, the Client-Server Authentication Private Key, the Public Key for card verifiable certificate 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.Dec_Trans Document key decryption and transcipherment

The TOE provides document cipher key decipherment with an internal private key and document cipher key transcipherment with internal private key and imported public key. The TOE stores a certificate for the corresponding public key.

OT.DS_CSA Digital signature-creation for client / server authentication

The TOE provides service for digital signature creation with an internal private signature key. It stores a certificate for the corresponding public key.

OT.TSS Terminal support service

The TOE provides service random number generation for the operational environment by means of command GET RANDOM to all users.

OT.AC_Serv Access Control for TOE Security Services

The TOE controls the access to the security services following the rules:

The TOE allows all users to read the certificates of the TOE and the cardholder.

The TOE allows all users to request authentication of the TOE receiver of PIN and SSCD for multiple signatures and to negotiate Introduction keys by means Service_Asym_Mut_Auth_with_SM and Service_Asym_Mut_Auth_with_Intro of PrK.HPC.AUTD_SUK_CVC.

The TOE must ensure that the TOE security services Service_Asym_Mut_Auth_w/o_SK or Service_Asym_Mut_Auth_with_SM by means of key PrK.HPC.AUTR_CVC, Service_Client_Server_Auth, and Service_Key_Decryption can be used by the Cardholder only.

The TOE must ensure that the TOE security service Service_Signature_Creation can be used by the holder of the signature-creation key only.

Application note 3: Note security objective for the TOE **OT.Sigy_SigF** describe the access control for creation of qualified electronic signatures with PrK.HP.QES.

OT.SCD/SVD_Gen SCD/SVD generation

The TOE provides security features to ensure that authorised users only invoke the generation of the SCD and the SVD.

OT.SCD_Unique Uniqueness of the signature-creation data

The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible.

OT.SCD_SVD_Corresp Correspondence between SVD and SCD

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE.

OT.Sig_Secure Cryptographic security of the electronic signature

The TOE generates electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the digital signatures or any other data exported outside the TOE. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.DTBS_Integrity_TOE DTBS-representation integrity inside the TOE

The TOE must not alter the DTBS-representation.

OT.Trusted_Channel Trusted Channel

The TOE establishes a trusted channel for protection of the confidentiality and integrity of the transmitted data (i.e. verification authentication data and data to be signed) between the TOE and the successful authenticated smart card on demand of the external signature-creation application (The TOE allows the use of a trusted channel in the

security environment SE#1 and enforces the use of a trusted channel in SE#2 to generate a digital signature [7]).

OT.TOE_TC_DTBS Trusted channel of TOE for DTBS

If the TOE allows generation of more than 1 signature after successful authentication of the Signatory (i.e. the security environment SE #2 is selected) the TOE shall enforce the use of a trusted channel to the ASCA[8] to detect alteration or masquerade of the DTBS-representation send by the ASCA. The TOE must not generate digital signatures with the SCD for altered DTBS. If the security environment SE #1 is selected (i.e. the TOE does not enforce the use of a trusted channel to the SCA) the TOE shall enforce re-authentication of the Signatory after each signature-creation.

OT.Sigy_SigF Signature generation function for the legitimate signatory only

The TOE provides the signature generation function with Prk.HP.QES for the legitimate Signatory successfully authenticated with PIN.QES only and protects the SCD against the use of others. If the signatory uses a SCA, which is not authorized to send DTBS through a secure messaging channel to the TOE, the signatory is allowed to create only 1 signature after 1 successful authentication with PIN.QES. The signatory is allowed to create more than 1 digital signature after 1 successful authentication with PIN.QES if the authorized SCA successfully authenticated by CVC with CHA profile 51 (SAK) provides the DTBS-representation through a secure messaging channel to the TOE.

OT.Prot_Abuse_Func Protection against abuse of functionality

The TOE prevents 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

---

[7] The smart cards use a technique named “security environment” to distinguish between different access control rules selectable by the external world (i.e. the terminal). This term should not be mistaken of “TOE environment” in Common Criteria.

[8] The ASCA is represented by a SMC in the role Profile 51 for device authentication of secure signature environment of SAK (SMC-K).

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

- 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
- forcing a malfunction of the TOE (e.g. fault injection) and/or
- 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.Tamper_ID Tamper detection

The TOE provides system features that detect physical tampering of a system component, and use those features to limit security breaches.

OT.Prot_Phys_Tamper Protection against physical tampering

The TOE must provide protection of 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.

In addition to the objectives from the PP, the following objective has been introduced into this ST:

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.

OE.Pers_CAMS **Secure initialization, personalization and management**

All data structures and data on the card produced during initialisation, personalisation or additional administration or management steps during the end-usage phase must prevent misuse of the TOE and must be formed correctly according to the specifications [22], and must ensure the integrity and confidentiality of TSF data and user data. The initialisation and personalisation shall follow the security rules for secure signature-creation devices. The Personalisation Agent and if applicable the Card Management System ensure (i) the correctness of the personal data of the smart cardholder (Health Professional Data), (ii) 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 including the access rights of the cardholder, (iii) writing the public key for verification of CV certificates for card-to-card authentication, (iv) the generation of the client-server authentication keys stored on the smart card and the distribution of the corresponding public key in form of X.509 certificates by an public key infrastructure, (v) the generation of the decipher key stored on the smart card and the distribution of the corresponding public key in form of X.509 certificates by an public key infrastructure. The Card Management System must not interfere with the operational application for qualified electronic signature under sole control of the signatory. This includes in particular sufficient cryptographic quality of the cryptographic keys (in accordance with the cryptographic algorithms specified for the HPC [22] and TR-03116 [14] and [30]) 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 mustn't tell the PIN (or PINs) of the HPC to others and mustn't hand the card to unauthorised persons. The the health professionals must use their data systems according to the overall system security requirements in particular by selection of appropriate smart card security environment (i.e. SE#1 or SE#2 for the HPC).

OE.CGA_QCert Generation of qualified certificates

The CGA generates qualified certificates, which include inter alia

(a) the name of the signatory controlling the TOE,

(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,

(c) the advanced signature of the CSP.

It confirms with the qualified certificate that the SCD corresponding to the SVD is stored in a SSCD.

OE.SSCD_Prov_Service Authentic SSCD provided by SSCD Provision Service

The SSCD Provision Service provides, initialises and personalises authentic TOE and delivers it as SSCD to the signatory.

OE.HID_VAD Protection of the VAD

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface.

OE.DTBS_Intend SCA sends data intended to be signed

The SCA

(a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,

(b) sends the DTBS-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE

(c) attaches the signature produced by the TOE to the data or provides it separately.

OE.DTBS_Protect SCA protects the data intended to be signed

The operational environment ensures that the DTBS-representation cannot be altered in transit between the SCA and the TOE. If the signatory want to create more than 1 digital signature after 1 successful authentication with PIN.QES the SCA shall provides a secure messaging channel to the TOE to ensure that the DTBS-representation cannot be altered or masqueraded undetected in transit between the SCA and the TOE.

OE.Trusted_Channel Trusted Channel

The IT environment establishes a trusted channel for protection of the confidentiality and integrity of the transmitted data between the TOE and the successful authenticated smart card by selecting the security environment SE#1 or SE #2 for the TOE.

OE.PKI Public key infrastructure

The IT environment establishes a public key infrastructure providing the smart cards with appropriate card-verifiable certificates and users with X.509 certificates.

5.3 Security Objectives Rationale

	OT.AC_CAMS	**OT.Data_Confident**	**OT.Data_Integrity**	**OT.Dec_Trans**	**OT.DS_CSA**	**OT.TSS**	**OT.AC_Serv**	**OT.SCD/SVD_Gen**	**OT.SCD_Unique**	**OT.SCD_SVD_Corresp**	**OT.Sig_Secure**	**OT.DTBS_Integrity_TO**	**OT.TOE_TC_DTBS**	**OT.Trusted_Channel**	**OT.Sigy_SigF**	**OT.Prot_Abuse_Func**	**OT.Prot_Inf_Leak**	**OT.Prot_Malfunction**	**OT.Tamper_ID**	**OT.Prot_Phys_Tamper**	***OT. Lifecycle_Security***
OSP.HPC_Spec	x	x	x	x	x	x	x	x			x			x	x						

	OT.AC_CAMS	**OT.Data_Confident**	**OT.Data_Integrity**	**OT.Dec_Trans**	**OT.DS_CSA**	**OT.TSS**	**OT.AC_Serv**	**OT.SCD/SVD_Gen**	**OT.SCD_Unique**	**OT.SCD_SVD_Corresp**	**OT.Sig_Secure**	**OT.DTBS_Integrity_TO**	**OT.TOE_TC_DTBS**	**OT.Trusted_Channel**	**OT.Sigy_SigF**	**OT.Prot_Abuse_Func**	**OT.Prot_Inf_Leak**	**OT.Prot_Malfunction**	**OT.Tamper_ID**	**OT.Prot_Phys_Tamper**	***OT. Lifecycle_Security***
OSP.Enc				x			x														
OSP.CSA					x		x														
OSP.CSP_OCert										x											
OSP.QSign								x	x		x	x	x		x						
OSP.Sigy_SSCD								x	x	x	x	x			x						
OSP.Sig_Non-Repud								x	x	x	x				x						
T.Compromise_Internal_Data		x																			
T.Forge_Internal_Data			x																		
T.Misuse	x	x	x				x						x	x	x						
T.Intercept														x							
T.SCD_Divulg		x																			
T.SCD_Derive		x						x			x										
T.DTBS_Forgery												x	x	x							
T.Sig_Forgery									x		x										
T.Abuse_Func																x					
T.Information_Leakage																	x				
T.Malfunction																		x			
T.Phys_Tamper																			x	x	
T.Lifecycle_Flaw																					x

Table 4: TOE Security Objective Rationale

	OE.Pers_CAMS	OE.Users	OE.CGA_QCert	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Trusted_Channel	OE.PKI
T.Misuse	x				x		x		
T.DTBS_Forgery						x	x		
T.Sig_Forgery			x						
T.Intercept								x	
OSP.HPC_Spec								x	x
OSP.CSP_QCert			x						
OSP.QSign			x						
OSP.Sigy_SSCD				x					
OSP.Sig_Non-Repud			x						
A.Pers_CAMS	x								
A.Users		x							
A.CGA			x						
A.SCA						x	x		

Table 5: Rationale for the Security Objective for the environment

The threat **T.Compromise_Internal_Data** “Compromise of confidential User or TSF data” addresses 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 threat is mainly achieved by the security objective **OT.AC_CAMS** “Access control for management” protecting the management functions of the TOE, **OT.AC_Serv** “Access Control for TOE Security Services” and

OT.Sigy_SigF “Signature generation function for the legitimate signatory only” 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 security objective for the TOE **OT.Trusted_Channel** “Trusted Channel” protects the verification authentication data and data to be signed during their transmission between the TOE and successfully authenticated smart cards on demand of the signature-creation application. In case of multiple signatures (i.e. if the TOE allows generation of more than 1 signature after successful authentication of the Signatory) the **OT.TOE_TC_DTBS** “Trusted channel of TOE for DTBS” enforces the use of the trusted channel. The security objective environment **OE.HID_VAD** “Protection of the VAD” protects the verification authentication data of the human user of the TOE and **OE.DTBS_Protect** “SCA protects the data intended to be signed” ensures that the IT environment protects the DTBS and supports the protection enforced by the TOE for DTBS in case of multiple signatures.. **OE.Pers_CAMS** “Secure initialization, personalization and management” ensure secure initialisation, personalisation and management preventing misuse of the TOE.

The threat **T.Intercept** “Interception of Communication” is countered by the security objective **OT.Trusted_Channel** “Trusted Channel” and **OE.Trusted_Channel** “Trusted Channel”.

Note that according to the **OSP.HPC_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 is sensitive and requires the protection in confidentiality and integrity. If the application selects the security environment SE #2 (cf. the specification [21]) 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.

T.SCD_Divulg “Storing,copying, and releasing of the signature-creation data” addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE. This threat is countered by **OT.Data_Confident** “Confidentiality of internal data”, which assures the secrecy of the SCD used for signature generation.

T.SCD_Derive “Derive the signature-creation data” deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. **OT.SCD/SVD_Gen** “SCD/SVD generation” counters this threat by implementing cryptographic secure generation of the SCD/SVD-pair. **OT.Sig_Secure** “Cryptographic security of the electronic signature“ensures cryptographic secure electronic signatures. This threat is also countered by **OT.Data_Confident**

"Confidentiality of internal data", which assures the secrecy of the SCD used for signature generation.

T.DTBS_Forgery (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which than does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The TOE counters this threat by the means of

- **OT.DTBS_Integrity_TOE** "DTBS-representation integrity inside the TOE" by ensuring the integrity of the DTBS-representation inside the TOE.
- **OT.Trusted_Channel** "Trusted Channel" protects the verification authentication data and data to be signed during their transmission on demand of the signature-creation application.
- **OT.TOE_TC_DTBS** "Trusted channel of TOE for DTBS" enforces the use of the trusted channel in case of multiple signatures.

The TOE IT environment addresses T.DTBS_Forgery by the means of

- **OE.DTBS_Intend** "SCA sends data intended to be signed", which ensures that the SCA sent only the intended data for signature-creation,
- **OE.DTBS_Protect**, which protect the DTBS-representation against alteration in transit between the SCA and the TOE.

T.Sig_Forgery "Forgery of the electronic signature)"deals with non-detectable forgery of the electronic signature. The OT.Sig_Secure, OT.SCD_Unique and OE.CGA_Qcert address this threat in general. The **OT.Sig_Secure** "Cryptographic security of the electronic signature" ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. The **OT.SCD_Unique** "Uniqueness of the signature-creation data" ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. The OE.CGA_Qcert "Generation of qualified certificates" prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision about a forged signature.

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 objectives **OT.Prot_Phys_Tamper** "Protection against physical tampering" and OT.Tamper_ID "Tamper Detection".

*The threat **T.Lifecycle_Flaw** "TOE flaw in a particular lifecycle state" is adverted directly by the security objective **OT.Lifecycle_Security** "Lifecycle security".*

The organisational security policy **OSP.HPC_Spec** "Compliance to HPC specifications" is implemented by security objectives for the TOE and the IT environment. The TOE security objectives **OT.SCD/SVD_Gen** "SCD/SVD generation" (cf. [21]), **OT.Sig_Secure** "Cryptographic security of the electronic signature", **OT.DEC_Trans** "Document key decryption and transcipherment", **OT.DS_CSA "**Digital signature-creation for client / server authentication", **OT.Trusted_Channel** "Trusted Channel" and **OT.TSS** "Terminal support service**"** implement the security services described in specified in [21], [22] and [23][9] referenced in the **OSP.HPC_Spec.** The TOE security objectives **OT.AC_CAMS** "Access control for management", **OT.AC_Serv** "Access Control for TOE Functions" and **OT.Sigy_SigF** "Signature generation function for the legitimate signatory only" implement the protection of these security services. **OT.Data_Confident** "Confidentiality of internal data" and **OT.Data_Integrity** "Integrity of internal data" require the protection of the confidentiality and the integrity of the user data and the TSF data the specification relay on against any attacks. The **OE.Trusted_Channel** "Trusted Channel" address the trusted channel of card-tocard authentication. The **OE.PKI** "Public key infrastructure" establishes the public key infrastructure used in the HPC specification [22].

The organisational security policy **OSP.Enc** "Document decryption and transcipherment" is implemented by functionality addressed by **OT.Dec_Trans "**Document key decryption and transcipherment" and controlled by **OT.AC_Serv** "Access Control for TOE Functions".

The organisational security policy **OSP.CSA** "Client-Server-Authentication" is implemented by functionality addressed by **OT.DS_CSA** "Digital signature-creation for client / server authentication" and controlled by **OT.AC_Serv** "Access Control for TOE Functions".

The organisational security policy **OSP.QSign** "Qualified electronic signatures" is implemented by the TOE security objectives

- **OT.SCD/SVD_Gen** "SCD/SVD generation**"** and **OT.SCD_Unique** "Uniqueness of the signature-creation data**"**.

[9] [23] is a supplement of [21].

- **OT.Sig_Secure** “Cryptographic security of the electronic signature”, **OT.DTBS_Integrity_TOE** “DTBS-representation integrity inside the TOE**”** and **OT.Sigy_SigF** “Signature generation function for the legitimate signatory only” implement the signature-creation functionality and the corresponding access control.
- **OT.TOE_TC_DTBS** “Trusted channel of TOE for DTBS” addressing specific security objective in case the TOE shall generate more than 1 signature after successful authentication of the Signatory.
- **OT.Sigy_SigF** “Signature generation function for the legitimate signatory only“provides the signature generation function for the legitimate Signatory successfully authenticated only and protects the SCD against the use of others.

The security objective of the IT environment **OE.CGA_QCert** “Generation of qualified certificates” ensures qualified certificates for the HPC SVD.

The organisational security policy **OSP.Sigy_SSCD** “TOE as secure signature-creation device” is implemented by the TOE security objectives

- **OT.SCD/SVD_Gen** “SCD/SVD generation**”**, **OT.SCD_Unique** “Uniqueness of the signature-creation data**”** and **OT.SCD_SVD_Corresp** “Correspondence between SVD and SCD” implement the requirements for secure generation of the SCD/SVD pair.
- **OT.Sig_Secure** “Cryptographic security of the electronic signature” and **OT.Sigy_SigF** “Signature generation function for the legitimate signatory only” implement the signature-creation functionality.
- **OT.DTBS_Integrity_TOE** “DTBS-representation integrity inside the TOE**”** - the TOE must not alter the DTBS representation.

The security objective of the IT environment **OE.SSCD_Prov_Service** "Authentic SSCD provided by SSCD Provision Service" provides, initialises and personalises authentic TOE and delivers it as SSCD to the signatory.

The organisational security policy **OSP.CSP_QCert** “Qualified certificate” is implemented by functionality directly addressed by **OE.CGA_QCert** “Generation of qualified certificates” and by **OT.SCD_SVD_Corresp** “Correspondence between SVD and SCD”, which implements the requirements for secure generation of the SCD/SVD pair.

The organisational security policy **OSP.Sig_Non-Repud** “Non-repudiation of signatures” is mainly addressed by the

- **OT.SCD/SVD_Gen** “SCD/SVD generation**”**, **OT.SCD_Unique** “Uniqueness of the signature-creation data**”** and **OT.SCD_SVD_Corresp** “Correspondence between SVD and SCD” for generation of the SCD/SVD pair and **OE.CGA_QCert** “Qualified certificate”, which ensures that the SVD in the

qualified certificate can be uniquely traced back to the HPC of the signatory as SSCD,

- **OT.Sig_Secure** “Cryptographic security of the electronic signature”, and **OT.Sigy_SigF** “Signature generation function for the legitimate signatory only” implementing the cryptographically secure digital signatures and the corresponding access control to trace the signature to the signatory’s willful act.

The security objectives for the environment **OE.Pers_CAMS** “Secure initialization, personalization and management” implements the assumption **A.Pers_CAMS** “Personalization and management of the Smart Card” with respect of the concrete user and TSF data described in the specification [21] (cf. to **OSP.HPC_Spec**).

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

The assumption **A.CGA** “Trustworthy certification-generation application” is directly addressed by the security objectives for the IT environment **OE.CGA_QCert** “Generation of qualified certificates”.

The assumption **A.SCA** “Trustworthy signature-creation application” is directly addressed by the security objectives for the IT environment **OE.DTBS_Intend** “SCA sends data intended to be signed” and **OE.DTBS_Protect** “SCA protects the data intended to be signed”.

6 Extended Components Definition

This security target uses components defined as extensions to CC part 2. Some of these components are defined in [19] and [20], other components are defined in this security target.

6.1 Definition of the Family FCS_RNG

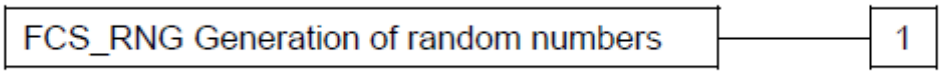
To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This extended family FCS_RNG describes SFR for random number generation used for cryptographic purposes.

The family "Generation of random numbers (FCS_RNG)" is specified as follows.

FCS_RNG Generation of random numbers

Family behavior 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 Random number generation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, physical hybrid, deterministic hybrid*] random number generator, which implements: [assignment: *list of security capabilities*].

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

6.2 Definition of the Family FIA_API

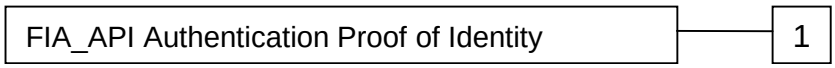
To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external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

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.

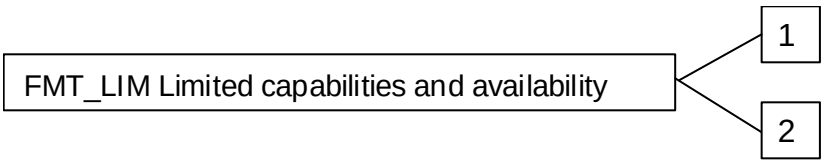
The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

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 the TSF to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 “Limited availability”, requires the TSF to 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.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 The TSF shall be designed and implemented 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].

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.

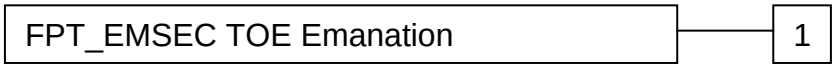
6.4 Definition of the Family FPT_EMSEC

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 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.

Dependencies: No dependencies.

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 that [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*].

7 Security Requirements

The CC allows several operations to be performed on functional components: *refinement*, *selection*, *assignment*, and *iteration* are defined in chapter C.4 of part 1 of the CC. Each of these operations is used in this security target.

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

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Any uncompleted selection that have been completed by the ST author appear *italicized* and underlined and the original text of the HPC PP [2] 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 are denoted by showing as underlined text 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 underlined and the original text of the HPC PP [2] 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 appear in addition *italicized* in the header and the full text.

7.1 Security Functional Requirements for the TOE

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 [9].

Application note 7: The following table provides an overview how the security services (listed in chapter 2.1) match to the SFR.

Security Service	SFR	Comment
Human user authentication	FIA_AFL.1/CH, FIA_AFL.1/CH_PUK, FIA_AFL.1/QES, FIA_AFL.1/QES_PUK,	Human user authentication is performed by means of the authentication reference data PIN and

	FIA_SOS.1, FIA_ATD.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_API.1, FMT_MTD.1/PIN, FMT_MTD.1/Admin, FMT_MTD.1/CH FMT_MTD.1/Sigy	PUK
Card-to-card authentication	FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_RNG.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FMT_MTD.1/WR, FMT_MTD.1/RPK_MOD	Card-to-card authentication according to [21], chapter 15,
Secure messaging	FCS_CKM.1/AKP, FCS_CKM.1/Asym_Auth, FCS_CKM.1/Sym_Auth, FCS_CKM.4, FCS_RNG.1, FCS_COP.1/SHA, FCS_COP.1/3TDES, FCS_COP.1/RMAC, FDP_UCT.1, FDP_UIT.1	Secure messaging key generation is described in [21], Chapter 6.2 and secure messaging encryption and MAC is described in [21], chapter 13.
Client-server authentication	FCS_COP.1/CSA, FDP_ACC.1/CH, FDP_ACF.1/CH	Client-server authentication by means of digital signature-creation [21], sec. 6.6.3, 14.7.4 and 14.8.1
Document key decipherment	FCS_COP.1/RSA_DEC, FCS_COP.1/RSA_TRANS, FDP_ACC.1/CH, FDP_ACF.1/CH	Decryption and transcipherment of document keys according to [21], sec. 6.7, 6.8, 14.8.3 and 14.8.7
Signature creation	FCS_COP.1/Sign, FDP_ACC.1/Sign, FDP_ACF.1/Sign, FDP_UCT.1, FDP_UIT.1	Signature-creation data for digital signatures indented to be used for qualified electronic signatures [21], sec. 6.6.3 and 14.8.1
Terminal Support Service	FCS_RNG.1, FDP_ACC.1/CH,	Generation of random numbers for terminals

	FDP_ACF.1/CH	

Table 6: Overview of SFR used to describe the TOE security services

7.1.1 Cryptographic support (FCS)

The cryptographic algorithms implemented in the TOE shall meet the TR-03116 [14] and [30]. The ST writer shall iterate the relevant SFR components if the TOE supports the optional cryptographic algorithms described in [21].

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.

7.1.1.1 Basic Algorithms

FCS_RNG.1 **Random number generation**

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1/DRNG	The TSF shall provide a *deterministic*[10] random number generator, which implements: *functionality class K4 with SOF-high of AIS20 [28]*[11].
FCS_RNG.1.1/PHYS	The TSF shall provide a *physical*[12] random number generator, which implements: *functionality class P2 with SOF-high of AIS31 [29]*[13].
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.[14,15]
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.[16,17]

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

[11] [assignment: *list of security capabilities*]

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

[13] [assignment: *list of security capabilities*]

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

[15] 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.

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

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

FCS_COP.1.1/ SHA	The TSF shall perform hashing [18] in accordance with a specified cryptographic algorithm SHA-256 [19] and cryptographic key sizes none [20] that meet the following: FIPS 180-2 [16][21].

Application note 8: This SFR requires the TOE to implement the hash function SHA-256 (256 bit hash value) as cryptographic primitive of the digital signature-creation and key derivation according to [21], chapter 6.1.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/	The TSF shall perform digital signature-creation for Card-to-card

[17] see footnote Number 15

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

[19] [assignment: *cryptographic algorithm*]

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

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

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

CCA_SIGN	authentication [22] in accordance with a specified cryptographic algorithm RSA ISO9796-2 DS1 [23] and cryptographic key sizes 2048 bit modulo length[24] that meet the following: [14], [21] [25].

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

Hierarchical to: No other components.

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

FCS_COP.1.1/ CCA_VERIF	The TSF shall perform digital signature-verification for Card-to-card authentication [26] in accordance with a specified cryptographic algorithm RSA ISO9796-2 DS1 [27] and cryptographic key sizes 2048 bit modulo length[28] that meet the following: [14], [21] [29].

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

Hierarchical to: No other components.

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

FCS_COP.1.1/ 3TDES	The TSF shall perform encryption and decryption [30] in accordance with a specified cryptographic algorithm 3TDES in CBC mode [31] and cryptographic key sizes 168 bit [32] that

[23] [assignment: *cryptographic algorithm*]
[24] [assignment: *cryptographic key sizes*]
[25] [assignment: *list of standards*]
[26] [assignment: *list of cryptographic operations*]
[27] [assignment: *cryptographic algorithm*]
[28] [assignment: *cryptographic key sizes*]
[29] [assignment: *list of standards*]
[30] [assignment: *list of cryptographic operations*]
[31] [assignment: *cryptographic algorithm*]
[32] [assignment: *cryptographic key sizes*]

	meet the following: FIPS 46-3 [15] and [21] [33].

Application note 9: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data and for the Service_Sym_Mut_Auth_with_SM. The key is agreed between the TSF according to the FIA_UAU.4.

Note by the ST author 1: The key length of 168 bit denotes the effective key length. The actual key length is 192 bit, but 24 bit are used for parity adjustment.

FCS_COP.1/RMAC Cryptographic operation – Retail MAC

Hierarchical to: No other components.

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

FCS_COP.1.1/ RMAC	The TSF shall perform generation and verification of message authentication code [34] in accordance with a specified cryptographic algorithm Retail MAC [35] and cryptographic key sizes 168 bit [36] that meet the following: ANSI X9.19 with DES and [21] [37].

Application note 10: This SFR requires the TOE to implement the cryptographic primitive for secure messaging in with encryption and message authentication code over the transmitted data and for the Service_Sym_Mut_Auth_with_SM. The key is agreed or defined as the key for secure messaging encryption. The key size of 168 bit is chosen to resist attacks with high attack potential.

7.1.1.2 Key Management

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

FCS_CKM.1/AKP Cryptographic key generation – Asymmetric key pair

Hierarchical to: No other components.

[33] [assignment: *list of standards*]
[34] [assignment: *list of cryptographic operations*]
[35] [assignment: *cryptographic algorithm*]
[36] [assignment: *cryptographic key sizes*]
[37] [assignment: *list of standards*]

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

FCS_CKM.1.1/ AKP	The TSF shall generate cryptographic keys **for RSA**[38] in accordance with a specified cryptographic key generation algorithm *G&D_RSAKeyGen*[39] and specified cryptographic key sizes 2048 bit[40] that meet the following: [14][21][41].

Application note 11: The HPC specification [21] requires the TOE to implement the command GENERATE ASYMMETRIC KEY PAIR in part 1 for qualified electronic signatures. The TOE supports the generation of asymmetric key pairs for

- qualified electronic signatures (cf. Service_Signature_Creation, key pair PrK.HPC.QES and Puk.HP.QES) (cf [21], sec.6.4[42]).

The TOE may support the generation of additional asymmetric key pairs as allowed by the access rules. In particular, asymmetric key pairs for the organization-specific authentication application may be generated in this manner. However, the key pairs for mutual card-to-card authentication, client/server authentication and document cipher key decipherment will be not generated on-card but will be personalised.

The missing operations in the element FCS_CKM.1.1 have been performed according to the implemented key generation algorithms and the intended method of use. The ST writer consulted the notified body [27] for the admissible algorithms, cryptographic key sizes and other parameters for algorithms and standards for the generation of SCD / SVD pairs by SSCD and other key pairs.

FCS_CKM.1/Asym_Auth	**Cryptographic key generation - Asymmetric card-to-card authentication with key agreement**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

[38] Refinement: “for RSA”

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

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

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

[42] [21], sec.6.4, does not require the prime numbers q and p of the RSA modulus to meet $0.1 < |\log_2 p - \log_2 q| < 30$ as described in [14], which may cause fail assessment in the TOE evaluation.

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 [43] and specified cryptographic key sizes 168 bit[44] that meet the following: [14], [21] [45].

Application note 12: The **asymmetric** card-to-card authentication with key agreement [21], chap. 15, is used for **Service_Asym_Mut_Auth_with_Intro** with algorithmic identification rsaSessionkey4Intro and **Service_Asym_Mut_Auth_with_SM** with algorithmic identification rsaSessionkey4SM. The TOE is equipped with its Card Authentication Private Key and has received and verified the Card Authentication Public Key of the communication partner. The key agreement method is the same for both algorithmic identification rsaSessionkey4Intro and rsaSessionkey4SM but result in symmetric keys for different usage: (i) introduction keys are permanently stored in the TOE and used for symmetric authentication (with or without symmetric key agreement), and (ii) temporarily stored symmetric secure messaging keys, where SMK.ENC and SMK.MAC are different. The introduction keys may be used further on for **Service_Sym_Mut_Auth_with_SM** according to FCS_CKM.1/Sym_Auth and symmetric internal or external authentication. The **symmetric** card-to-card authentication with key agreement is used for **Service_Sym_Mut_Auth_with_SM**. The TOE is equipped with symmetric secret keys SK.HPC.AUT and agrees secure message keys which are used for encryption and message 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

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

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

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

	generation algorithm symmetric mutual card-to-card authentication with key agreement 3TDES and SHA-256 [46] and specified cryptographic key sizes 168 bit[47] that meet the following: [14], [21] [48].

Application note 13: The TOE is equipped with symmetric secret keys SK.HPC.AUT and agrees 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.

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

FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting with 0x00*[49] that meets the following: *none*[50].

Application note 14: 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.

7.1.1.3 Cryptographic operation

FCS_COP.1/Sign	Cryptographic operation – Digital Signature for QES
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or

[46] [assignment: *cryptographic key generation algorithm*]
[47] [assignment: *cryptographic key sizes*]
[48] [assignment: *list of standards*]
[49] [assignment*: cryptographic key destruction method*]
[50] [assignment*: list of standards*]

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ Sign	The TSF shall perform digital signature-creation for QES[51] in accordance with a specified cryptographic algorithm SHA-256 and *RSASSA_PKCS1_V1_5_SIGN or RSA_ISO9796_2_DS2_SIGN or RSASSA_PSS_SIGN*[52] and cryptographic key sizes 2048 bit modulo length [53] that meet the following: [14], [21][54]..

FCS_COP.1/CSA	**Cryptographic operation – Digital Signature-Creation for Client-Server Authentication**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ CSA	The TSF shall perform digital signature-creation for client-server authentication [55] in accordance with a specified cryptographic algorithm RSASSA_PSS_SIGN [56] and cryptographic key sizes 2048 bit modulo length[57] that meet the following: [14], PKCS#1 [18], [21], sec. 6.6.3.1.5 [58].

Application note 15: The TOE to implements the RSA for the cryptographic primitive of the digital signature-creation for the client-server authentication mechanism according to [22], sec. 10.6. The private key PrK.HP.AUT shall be selected using MANAGE SECURITY ENVIRONMENT.

---

[51] [assignment: *list of cryptographic operations*]
[52] [assignment: *cryptographic algorithm*]
[53] [assignment: *cryptographic key sizes*]
[54] [assignment: *list of standards*]
[55] [assignment: *list of cryptographic operations*]
[56] [assignment: *cryptographic algorithm*]
[57] [assignment: *cryptographic key sizes*]
[58] [assignment: *list of standards*]

FCS_COP.1/RSA_DEC Cryptographic operation – RSA Decryption

Hierarchical to: No other components.

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

FCS_COP.1.1/ RSA_DEC	The TSF shall perform decryption [59] in accordance with a specified cryptographic algorithm RSAES_OAEP_DECRYPT and RSAES_PKCS1_v1_5_DECRYPT [60] and cryptographic key sizes 2048 bit modulo length[61] that meet the following: [14],[18],[21][62].

Application note 16**:** The TOE implements the RSA for the cryptographic primitive of the RSA decryption to [21], sec. 14.8.3, and [22], sec. 10.7. The private key PrK.HP.ENC shall be selected using MANAGE SECURITY ENVIRONMENT.

FCS_COP.1/RSA_TRANS Cryptographic operation – RSA Transcipherment

Hierarchical to: No other components.

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

FCS_COP.1.1/ RSA_TRANS	The TSF shall perform encryption and transcipherment [63] in accordance with a specified cryptographic algorithm

[59] [assignment: *list of cryptographic operations*]
[60] [assignment: *cryptographic algorithm*]
[61] [assignment: *cryptographic key sizes*]
[62] [assignment: *list of standards*]
[63] [assignment: *list of cryptographic operations*]

	RSAES_OAEP_ENCRYPT and RSAES_PKCS1_v1_5_ENCRYPT [64] and cryptographic key sizes 2048 bit modulo length[65] that meet the following: [14],[18],[21][66].

Application note 17: The TOE implements the RSA for the cryptographic primitive of the RSA transcipherment to [21] , sec. 14.8.7, and [22], sec. 10.8. The private key PrK.HP.ENC shall be selected using MANAGE SECURITY ENVIRONMENT and the public key shall be imported together with data to be transciphered in the command PSO: TRANSCIPHER.

7.1.2 Identification and Authentication

The TOE shall meet the requirement "Authentication failure handling (FIA_AFL.1)" as specified below (Common Criteria Part 2).

FIA_AFL.1/CH Authentication failure handling – PIN.CH

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1.1/CH	The TSF shall detect when 3[67] unsuccessful authentication attempts occur related to consecutive failed human user authentication with PIN.CH [68].
FIA_AFL.1.2/CH	When the defined number of unsuccessful authentication attempts has been *met*[69], the TSF shall block the PIN.CH for authentication until successful unblocked with resetting code PUK.CH [70].

FIA_AFL.1/CH_PUK Authentication failure handling – PUK.CH

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

---

[64] [assignment: *cryptographic algorithm*]

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

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

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

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

[69] [selection: *met or surpassed*]

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

FIA_AFL.1.1/ CH_PUK	The TSF shall detect when 10[71] authentication attempts occur related to human user authentication to unblock PIN.CH[72].
FIA_AFL.1.2/ CH_PUK	When the defined number of authentication attempts has been *met*[73], the TSF shall block the PUK.CH[74].

FIA_AFL.1/QES Authentication failure handling – PIN.QES

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1.1/ QES	The TSF shall detect when 3[75] unsuccessful authentication attempts occur related to consecutive failed human user authentication with PIN.QES for the QES application [76].
FIA_AFL.1.2/ QES	When the defined number of unsuccessful authentication attempts has been *met*[77], the TSF shall block the PIN.QES for authentication until successful unblocked with resetting code PUK.QES [78].

FIA_AFL.1/QES_PUK Authentication failure handling – PUK.QES

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1.1/ QES_PUK	The TSF shall detect when 10[79] authentication attempts occur related to human user authentication to unblock PIN.QES[80].
FIA_AFL.1.2/ QES_PUK	When the defined number of authentication attempts has been *met*[81], the TSF shall block the PUK.QES[82].

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

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

[73] [selection: *met or surpassed*]

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

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

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

[77] [selection: *met or surpassed*]

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

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

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

[81] [selection: *met or surpassed*]

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

Application note 18: The components FIA_AFL.1/CH, FIA_AFL/CH_PUK, FIA_AFL.1/QES and FIA_AFL.1/QES_PUK address the human user authentication for the health care applications respective for QES application. The cardholder reference data PIN.CH is a global PIN for the MF (cf. [22], sec. 4.3.9) with retry counter and PUK.CH is its resetting code with usage counter. The signatory reference data is the PIN.QES in DF.QES (cf. [22], sec. 9.1.3) with retry counter and PUK.QES is its resetting code with usage counter.

The TOE shall meet the requirement "Verification of secrets (FIA_SOS.1)" as specified below (Common Criteria Part 2).

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets (1) **operational PIN.CH**[83] meet minimum length of 5 digits and maximum 8 digits[84], (2) **PUK.CH meet length of 8 digits,** (3) **operational PIN.QES meet minimum length of 6 digits and maximum 8 digits,** (4) **PUK.QES meet minimum length of 8 digits and maximum 12 digits**[85].

Application note 19: The refinement lists the requirements for different secrets (instead of 4 times iteration of the component).

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.

Dependencies: No dependencies.

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

[83] Refinement: "(1) operational PIN.CH"

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

[85] Refinement: "(2) PUK.CH meet length of 8 digits, (3) operational PIN.QES meet minimum length of 6 digits and maximum 8 digits, (4) PUK.QES meet minimum length of 8 digits and maximum 12 digits"

	keys (2) role of other authenticated users [86].

Application note 20: The component FIA_ATD.1 applies to (i) the human user authentication, i.e. the cardholder which identity is given in the Health Professional Data (EF.HPD), and to (ii) the card-to-card authentication where the identity (i.e. the ICCSN.ICC) and the role (i.e. Role ID) are encoded in the CV certificate (cf. [21] chapter 7, [22] sec. 4.3.7 and Annex A.3, for details).

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.

Dependencies: No dependencies.

FIA_UID.1.1	The TSF shall allow (1) reading the ATR, (2) reading EF.ATR, EF.DIR, EF.GDO, EF.VERSION, EF.HPD, EF.SSEC, DF.CIA.ESING and DF.CIA.QES residing EFs (EF.CIAInfo, EF.DO, EF.AOD, EF.PrKD, and EF.CD) and EF containing certificates EF.C.*.*, (3) reading security status information using command GET PIN STATUS and GET SECURITY STATUS KEY, (4) execution of the command GET RANDOM, (5) execution of INTERNAL AUTHENTICATE with PrK.HPC.AUTD_SUK_CVC, PrK.HPC. AUTR_CVC and PrK.HP.AUT according to FIA_API.1, (6) *execution of the commands GET PROTOCOL DATA, HASH, MANAGE CHANNEL, SELECT FILE, execution of self tests according to FPT_TST.1*[87] on behalf of the user to be performed before the user is

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

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

	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.

Application note 21: The ST writer performed the missing operation in FIA_UID.1.1. According to the specification [22] the list of data objects with read access condition includes but is not limited to the Health Professional related Data, the Card Verifiable Authentication Certificates and the X.509 Certificates. If the option of the card management system for the end-usage phase is used the card management system may create DF and EF in MF and DF and define their access conditions.

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.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1	The TSF shall allow (1) reading the ATR, (2) reading EF.ATR, EF.DIR, EF.GDO, EF.HPD, EF.SSEC, EF.CIAInfo, EF.DO, EF.AOD, EF.PrKD, EF.CD and EF containing certificates EF.C.*.*, (3) reading security status information using command GET PIN STATUS and GET SECURITY STATUS KEY, (4) execution of the command GET RANDOM, (5) identification as cardholder by selecting the password reference or providing certificate for the authentication attempt, (6) execution of INTERNAL AUTHENTICATE with PrK.HPC.AUTD_SUK_CVC according to FIA_API.1, (7) *execution of the commands GET PROTOCOL DATA, HASH, MANAGE CHANNEL, SELECT*

	FILE, execution of self tests according to FPT_TST.1[88] 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.

Application note 22: The ST performed the missing operation in FIA_UAU.1.1. According to the specification [22] the list of data objects with read access condition includes but is not limited to the Health Professional Data, the Card Verifiable Authentication Certificates and the X.509 Certificates. The card management system may create DF and EF in MF and DF, and define their access conditions.

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.

Dependencies: No dependencies.

FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to Card-to-Card Authentication Mechanism (1) execution of the command EXTERNAL AUTHENTICATE with symmetric or asymmetric key, (2) execution of the command EXTERNAL AUTHENTICATE as part of the Service_Asym_Mut_Auth_w/o_SK, (3) execution of the command EXTERNAL AUTHENTICATE as part of the Service_Asym_Mut_Auth_with_SM, (4) execution of the command EXTERNAL AUTHENTICATE as part of the Service_Sym_Mut_Auth_with_SM with Introduction key, (5) secure messaging channel [89].

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

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

Application note 23: The command EXTERNAL AUTHENTICATE may be used as part of the card-to-card authentication mechanisms with authentication of the external entity to the TOE (without authentication of the TOE to this external entity) or as part of mutual authentication for services Service_Asym_Mut_Auth_w/o_SK, Service_Asym_Mut_Auth_with_SM, and Service_Sym_Mut_Auth_with_SM. Note the command EXTERNAL AUTHENTICATE with agreement of Introduction keys does not change the security status of the TOE and therefore is not an authentication by itself but need an additional symmetric EXTERNAL AUTHENTICATE with this symmetric key (cf. to Service_Asym_Mut_Auth_with_Intro). It uses freshly generated random data (see also FCS_RNG.1) as challenge to prevent reuse of a response generated in a successful authentication attempt. The secure messaging uses Send Sequence Counter for MAC calculation and verification of the command sequence (cf. [21], sec. 12.1).

The TOE shall meet the requirements of "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) Human user authentication with PIN.CH and PUK.CH, (2) Human user authentication with PIN.QES and PUK.QES, (3) execution of the command EXTERNAL AUTHENTICATE as part of the Service_Asym_Mut_Auth_w/o_SK, (4) execution of the command EXTERNAL AUTHENTICATE as part of the Service_Asym_Mut_Auth_with_SM, (5) execution of the command EXTERNAL AUTHENTICATE as part of the Service_Sym_Mut_Auth_with_SM, (6) secure messaging channel[90] 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 Cardholder with Cardholder Authentication Reference Data for PIN.CH, (2) The TSF shall authenticate the Cardholder with Authentication

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

	Reference Data for PUK.CH to authorize changing and unblocking PIN.CH. (3) The TSF shall authenticate the Signatory with Authentication Reference Data for PIN.QES to authorize signature-creation and changing PIN.QES. (4) The TSF shall authenticate the Signatory with Authentication Reference Data for PUK.QES to authorize unblocking PIN.QES. (5) The TSF shall authenticate the Security Module Card with Root Public Key of the Certificate Service Provider and Card verifiable certificate with a corresponding cardholder authorization of SMC as PIN sender (CHA profile 54), (6) The TSF shall authenticate the Authorized signature-creation application with Root Public Key of the Certificate Service Provider and Card verifiable certificate with a corresponding cardholder authorization of signature-creation application (CHA profile 51)[91].

Application note 24: Note the authentication according to clause (5) and (6) may be performed by (i) asymmetric authentication with symmetric secure messaging key agreement or (ii) asymmetric authentication with agreement of introduction keys and symmetric authentication with these introduction keys. In the later case the CHA profile in the CVC of the asymmetric key passes on to the introduction key.

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

FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions successfully established secure messaging [92].

Application note 25: The specification [21] 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

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

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

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 a (1) INTERNAL AUTHENTICATE with PrK.HPC.AUTR_CVC[93] to prove the identity of the role HPC[94] (2) INTERNAL AUTHENTICATE with PrK.HPC.AUTD_SUK_CVC to prove the identity of the SSCD for multiple-signature and PIN receiver (CHA profile 53), (3) INTERNAL AUTHENTICATE with PrK.HP.AUT to prove the identity of the HPC client[95].

Application note 26: The refinement adds a list of authentication mechanisms and roles as defined in clause 1 for FIA_API.1.1 (instead of 3 times iteration of the component). The role HPC is represented by one of the CHA profile 2 to 5 or 7. Note the client / server authentication uses the command INTERNAL AUTHENTICATE as well but with other algorithm identification.

Note by the ST-author 2:

In the PP [2] 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 description of refinements for this security requirement, points (2), and (3) are included as underlined text in the security target and marked by a footnote.

[93] [assignment: *authentication mechanism*]

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

[95] Refinement: “(2) INTERNAL AUTHENTICATE with PrK.HPC.AUTD_SUK_¬CVC to prove the identity of the SSCD for multiple-signature and PIN receiver (CHA profile 53), (3) INTERNAL AUTHENTICATE with PrK.HP.AUT to prove the identity of the HPC client”

7.1.3 Access Control

The TOE shall meet the requirements "Subset Access Control (FDP_ACC.1)" and "Security attribute based access control (FDP_ACF.1)"as specified below (Common Criteria Part 2).

FDP_ACC.1/Sign	**Subset access control – Signature-creation**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ Sign	The TSF shall enforce the Signature-creation SFP[96] on (1) subjects: (a) signatory, (b) signature-creation application, (c) terminal; (2) objects: (a) Signature-creation data PrK.HP.QES with security attribute "SCD operational", (b) DTBS-representation, (c) Display message (EF.DM in DF.QES), (3) operations: (a) generate SCD/SVD pair by means of the command PSO: GENERATE ASYMMETRIC KEY PAIR, (b) signature-creation for the DTBS-representation with Signature-creation data by means of the command PSO: COMPUTE DIGITAL SIGNATURE, (c) Display message by means of the commands SELECT and READ BINARY, (d) writing Display message by means of the commands SELECT and UPDATE BINARY[97]

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

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

Application note 27: The subjects and objects are described in section 4.1 Introduction. The User Authentication Reference Data (PIN.QES and PUK.QES) and the public key for CV certificate verification (PuK.RCA.CS) are TSF data. The private keys, the certificates and the display message for creation of qualified signature (contained in the DF.QES) are out of scope of this security target for HPC.

FDP_ACF.1/Sign	**Security attribute based access control– Signature-creation**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/_Sign	The TSF shall enforce the Signature-creation SFP[98] to objects based on the following: (1) subjects: (a) Administrator, (b) Signatory with authentication status, (c) Cardholder with authentication status, (d) Authorized signature-creation application, (e) an (unauthorised) terminal; (2) objects: (a) Signature-creation data PrK.HC.QES, (b) Signature-verification data, (c) DTBS-representation, (d) display message (EF.DM in DF.QES),[99] .
FDP_ACF.1.2/_Sign	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) the Administrator is allowed to generate the SCD/SVD pair by means of the command GENERATE ASYMMETRIC KEY PAIR with non-operational PrK.HP.QES, (2) the Signatory after successful authentication with PIN.QES is allowed

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

[99] [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*]

	(a) to create 1 signatures using operational PrK.HP.QES by means of the command PSO: COMPUTE DIGITAL SIGNATURE in security environment #1, (b) to create *n* signatures using operational PrK.HP.QES by means of the command PSO: COMPUTE DIGITAL SIGNATURE in security environment #2; (3) the Terminal is allowed to send DTBS for creation of 1 signature after one authentication of signatory with PIN.QES by means of the command PSO: COMPUTE DIGITAL SIGNATURE in security environment #1. (4) the Authorized signature-creation application is allowed (a) to send DTBS for creation of *n* signatures after one authentication of signatory with PIN.QES by means of the command PSO: COMPUTE DIGITAL SIGNATURE in security environment #2; (b) to read the Display message in DF.QES by means of the commands SELECT and READ BINARY; (5) The SMC authenticated with profile 51 is allowed to read the display message EF.DM in DF.QES. (6) The Autorized signature-creation application with profile 54 is allowed to read the display message and EF.DM in DF.QES. (7) the Cardholder is allowed to write the Display message in DF.QES by means of the commands SELECT and UPDATE BINARY [100].
FDP_ACF.1.3/_Sign	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[101].
FDP_ACF.1.4/_Sign	The TSF shall explicitly deny access of subjects to objects based on the rule:

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

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

	(1) to create signature with non-operational PrK.HP.QES (2) to read or export or modify the PrK.HP.QES. [102]

Application note 28: The SFR FDP_ACC.1/Sign, FDP_ACF.1/Sign, FMT_MSA.1 and FMT_MSA.3 use the security attribute "SCD operational" of the signature-creation data PrK.HP.QES to enforce the Signature-creation SFP describing the sole control of the Signatory on the signature-creation with the SCD. Even if the SCD/SVD pair is generated by the certification service provider, the SCD stored on the HPC before delivery to the signatory and the Administrator creates the authentication data for the signatory the signatory shall be the only one can create digital signature with the SCD. The security attribute "SCD operational" has two possible values "non-operational" and "operational". The SCD is "non-operational" until the Signatory takes sole control on the TOE as SSCD (cf. FMT_MSA.3). Nobody can create signatures with non-operational SCD (cf. FDP_ACF.1.4/Sign, clause 2). Only the Signatory can make the SCD "operational" (cf. FMT_MSA.1) and create signature with operational SCD (cf. FDP_ACF.1.2/Sign, clause 1).

The HPC specification part 1 requires the HPC operating system to support the generation of the SCD/SVD pair (PrK.HP.QES / Puk.HP.QES). This functionality may be used in the phase 6 "Smartcard Personalisation". The HPC specification part 2 addresses only the phase 7 "Smartcard End-usage**"** of the HPC and therefore prevents the execution of the command GENERATE ASYMMETRIC KEY PAIR (cf. [22], sec. 9.1.2). The phase transition may be implemented in different ways (e.g. by means of the security attribute "key available" set to TRUE, which prevents key generation if the key already exist, cf. [21](N1057)). The security attribute "SCD operational" is implemented by transport status of PIN.QES (cf. [22], sec. 9.1.3).

FDP_ACC.1/CH Subset Access Control – Cardholder Functions

Hierarchical to: Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/CH	The TSF shall enforce the HC Access Control SFP [103] on (1) the subjects (a) the Card Management System (CAMS), (b) the Cardholder (CH), (c) the SMC, (d) the Authorised Signature-Creation Application

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

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

	(ASCA), (e) an (unauthorised) Terminal; (2) the objects (a) Health Professional related Data (EF.HPD), (b) Global Data Object (EF.GDO), (c) EF.ATR, (d) EF.DIR (e) EF.Version (f) Security State Evaluation Counter (EF.SSEC) (g) Display Message (EF.DM in DF.ESIGN) (h) PrK.HPC.AUTR_CVC, and PrK.HPC.AUTD_SUK_CVC (i) PuK.RCA.CS and PuK.CAMS_HPC.AUT_CVC (j) Client-Server Authentication Private Key (PrK.HP.AUT), (k) Decipher Private Key (PrK.HP.ENC), (l) Card Verifiable Certificates (C.HPC.AUTD_SUK_CVC, C.HPC.AUTR_CVC, C.CA_HPC.CS), (m) X.509 certificates (C.HP.AUT, C.HP.ENC, C.HP.QES-AC1, C.HP.QES-AC2, and C.HP.QES-AC3) (n) PIN.CH and PIN.QES[104] (3) the operation by commands defined in table 1[105].

Application note 29: The subjects and objects are described in section 4.1 Introduction. The User Authentication Reference Data (PIN.CH and PUK.CH) and the public key for CV certificate verification (PuK.CA_NN_HPC.CS) are TSF data. The private keys, the certificates and the display message for creation of qualified signature (contained in the DF.QES) are out of scope of this security target for HPC.

FDP_ACF.1/CH Security attribute based access control – Cardholder Functions

Hierarchical to: No other components.

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

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

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

FDP_ACF.1.1/CH	The TSF shall enforce the HC Access Control SFP [106] to objects based on the following: (1) the subjects (a) the Card Management System with authentication status, (b) the Cardholder with authentication status, (c) the SMC with authentication status and profile in the CHA of the used CVC, (d) the ASCA with authentication status and profile in the CHA of the used CVC, (e) an (unauthorised) Terminal; (2) the objects as listed in FDP_ACC.1/CH[107].
FDP_ACF.1.2/CH	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) An (unauthorised) Terminal is allowed (a) to read by means of commands SELECT and READ BINARY the EF.ATR, EF.GDO, EF.SSEC and EF.HPD, (b) to read by means of commands SELECT and READ BINARY the Card Verifiable Certificates (C.HPC.AUTD_SUK_CVC, C.HPC.AUTR_CVC, and C.CA_HPC.CS), (c) to read by means of commands SELECT and READ BINARY the X.509 certificates (C.HP.AUT,

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

[107] [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.HP.ENC, C.HP.QES-AC1, C.HP.QES-AC2 and C.HP.QES-AC3), (d) to read by means of commands SELECT, READ RECORD and SEARCH RECORD the EF.DIR and EF.VERSION, (e) to execute the command INTERNAL AUTHENTICATE using PrK.HPC.AUTD_SUK_CVC for card-to-card authentication by means Service_Asym_Mut_Auth_with_SM and Service_Asym_Mut_Auth_with_Intro , (f) to execute CHANGE REFERENCE DATA, GET PIN STATUS, RESET RETRY COUNTER and VERIFY using PIN.CH and PIN.QES (g) to execute the command EXTERNAL AUTHENTICATE using PrK.HPC.AUTR_CVC, PrK.HPC.AUTD_SUK_CVC, and PuKCAMS_HPC.AUT_CVC (h) to execute the command PSO: VERIFY CERTIFICATE using PuK.RCA.CS, (i) execute the command GET RANDOM; (2) The Cardholder is allowed (a) to update by means of command SELECT and UPDATE BINARY the EF.HPD, EF.DM (in DF.ESIGN), (b) to update by means of commands SELECT and UPDATE BINARY the X.509 certificates (C.HP.QES-AC1,

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

	C.HP.QES-AC2, and C.HP.QES-AC3), (c) to execute the command INTERNAL AUTHENTICATE using PrK.HPC.AUTR_CVC for the card-to-card authentication, (d) to execute the document key decipherment Service_Data_Decryption using PrK.HP.ENC by means of the command PSO: DECIPHER, (e) to execute the document key transcipherment Service_Data_Decryption using PrK.HP.ENC and imported public key by means of the command PSO: TRANSCIPHER, (f) to execute the client-server authentication Service_Client_Server_Auth using PrK.HP.AUT by means of the command INTERNAL AUTHENTICATE and PSO: COMPUTE DIGITAL SIGNATURE, (g) all actions a terminal is allowed to perform. (3) The SMC authenticated with profile 51 is allowed to read the display message EF.DM in DF.ESIGN. (4) The Autorized signature-creation application with profile 54 is allowed to read the display message EF.DM in DF.ESIGN. (5) The Card Management System is allowed (a) to execute commands APPEND RECORD, UPDATE RECORD for EF.DIR, (b) to execute commands UPDATE RECORD for EF.VERSION[108].

FDP_ACF.1.3/CH	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[109].
FDP_ACF.1.4/CH	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[110].

Application note 30: The specification [22] describes details of the access control rules in chapter 4, 8, 9 and 10.

Application note 31: FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1 require the TOE to protect User Data transmitted between the TOE and a remote device by secure messaging with encryption and message authentication codes after successful mutual authentication. The services Service_Asym_Mut_Auth_with_SM and Service_Sym_Mut_Auth_with_SM include authentication mechanisms with key agreement (cf. FCS_CMK.1/Asym_Auth and FCS_CKM.1/Sym_Auth), the TDES encryption (cf. SFR FCS_COP.1/3TDES) and the Retail-MAC (cf. SFR FCS_COP.1/RMAC). The rules for the data transfer are defined in the security policy HC 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.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1	The TSF shall enforce the Signature-creation SFP and HC Access Control SFP [111] to transmit and receive[112] user data in a manner protected from unauthorised disclosure.

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

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

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

[112] [selection: *transmit, receive*]

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.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

FDP_UIT.1.1	The TSF shall enforce the Signature-creation SFP and HC Access Control SFP [113] to transmit and receive [114] user data in a manner protected from modification, deletion, insertion and replay [115] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [116] has occurred.

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

FDP_ITC.1.1	The TSF shall enforce the Signature-creation SFP and HC Access Control SFP [117] 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

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

[114] [selection: *transmit, receive*]

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

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

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

	outside the TOE: *initiate communication via the trusted channel for all functions requiring a trusted channel as defined by SFP_access_rules*[118]

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

FDP_ETC.1 Export 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]

FDP_ETC.1.1	The TSF shall enforce the Signature-creation SFP and HC Access Control SFP [119] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from*[120] the following objects: *PINs, secret and private cryptographic keys, data stored in files*[121] [122] [123].

Application note 32: For secret user data deletion upon allocation is sufficient. The ST writer considers also data in all files, which are not freely accessible as the possible completion of the assignment: *list of other objects*.

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

---

[118] [assignment: additional importation control rules]

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

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

[121] [assignment: *list of objects at least including: PINs, secret and private cryptographic keys]*

[122] [assignment: *list of other objects*]

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

FDP_SDI.2 Stored Data Integrity monitoring and action

Hierarchical to: FDP_SDI.1. Stored Data Integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors [124] on all objects, based on the following attributes: *integrity checked data*[125] [126].
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[127].

Application note 33: The integrity checked data includes cryptographic keys, input data for electronic signatures and user data stored in the card.

7.1.4 Security Management

Application note 34: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

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.

Dependencies: No dependencies.

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: Initialization, Personalization, Card Management, Modification of the PIN.CH ,

[124] [assignment: *integrity errors*]

[125] *[assignment: user data attributes – the attributes shall be chosen in a way that at least the following data are included: cryptographic keys, input data for electronic signatures,user data in files on the card*]

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

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

	Modification of the PIN.QES, Modification of the security attribute "SCD operational" of the signature-creation data PrK.HC.QES [128].

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.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1	The TSF shall maintain the roles Manufacturer, Personalisation Agent, Card Management System, Administrator, Cardholder, Signatory, Authorised signature-creation application, SMC as PIN sender, eGK, Terminal[129].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Application note 35: The cardholders authenticate themselves with PIN.CH and with PUK.CH for unblocking and changing PIN.CH. The Signatory cardholders authenticate themselves with PIN.QES and with PUK.QES for unblocking PIN.QES. The Certificate Holder Authorization (CHA) Role ID in the CVC defines the roles of Signature-creation application with profile 51 (e.g. SMC-K), SMC as PIN sender with profile 54, and eGK with profile 0[130]. A Terminal is a role of all unauthenticated user.

Application note 36: 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

(i) 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

(ii) 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).

---

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

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

[130] Note the assignment of roles to CVC CHA profile is informative only in [22] and [25].

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1	The TSF shall be designed and implemented 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 [131].

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.

Dependencies: FMT_LIM.1 Limited capabilities.

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 [132].

The TOE shall meet the requirements of "Management of security attributes (FMT_MSA.1)" as specified below (Common Criteria Part 2).

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

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

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

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

FMT_MSA.1.1	The TSF shall enforce the Signature-creation SFP[133] to restrict the ability to modify[134] the security attributes SCD operational[135] to Signatory[136].

Application note 37: If the Administrator generates SCD/SVD key pairs without the Signatory being authenticated the same time the security attribute of the SCD "SCD operational" shall be set to "non-operational" after generation of the SCD. If the Signatory generates SCD/SVD key pairs the security attribute of the SCD "SCD operational" may be set to "operational" during generation of the SCD.

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

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 *the security attribute "SCD operational"*[137].

The TOE shall meet the requirements of "Static attribute 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

[133] [assignment: *access control SFP(s), information flow control SFP(s)*]
[134] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[135] [assignment: *list of security attributes*]
[136] [assignment: *the authorised identified roles*]
[137] [assignment: *list of security attributes*]

FMT_MSA.3.1	The TSF shall enforce the HC Access Control SFP and Signature-creation SFP[138] to provide restrictive[139] default values for security attributes that are used to enforce the SFP. **The initial value of the SCD security attribute "SCD operational" is "non-operational"[140].**
FMT_MSA.3.2	The TSF shall allow the Administrator[141] to specify alternative initial values to override the default values **except of the security attribute "SCD operational"[142]** 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.

Application note 38: The following seven SFRs address the protection of the management of the TSF data: Initialization Data, Pre-personalization Data, User Authentication Reference Data (i.e. PIN and PUK), Public Key for CVC Verification. Note that the Card Authentication Private Keys, the Client-Server Authentication Keys, the Decipher Private Key and the HPC Electronic Signature Private Key are user data under protection according to SFR FDP_ACF.1.

FMT_MTD.1/INI	**Management of TSF data – Writing of Initialization Data and Pre-personalization Data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles

FMT_MTD.1.1/ INI	The TSF shall restrict the ability to write [143] the Initialization Data and Pre-personalization Data [144] to the Manufacturer [145].

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

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

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

[140] Refinement: "The initial value of the SCD security attribute "SCD operational" is "non-operational""

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

[142] Refinement: "except of the security attribute "SCD operational""

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

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles

FMT_MTD.1.1/ WR	The TSF shall restrict the ability to create [146] the User Reference Authentication Data, and public keys of the root for CVC verification [147] to the Personalisation Agent [148].

FMT_MTD.1/Admin Management of TSF data - Administrator

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/ Admin	The TSF shall restrict the ability to create[149] the PIN.CH, PUK.CH, PIN.QES, PUK.QES[150] to Administrator[151].

FMT_MTD.1/CH Management of TSF data – Cardholder

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/ CH	The TSF shall restrict the ability to modify and unblock [152] the PIN.CH[153] to Cardholder[154].

FMT_MTD.1/Sigy Management of TSF data – Signatory

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

[145] [assignment: *the authorised identified roles*]
[146] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[147] [assignment: *list of TSF data*]
[148] [assignment: *the authorised identified roles*]
[149] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[150] [assignment: *list of TSF data*]
[151] [assignment: *the authorised identified roles*]
[152] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[153] [assignment: *list of TSF data*]
[154] [assignment: *the authorised identified roles*]

FMT_MTD.1.1/ Sigy	The TSF shall restrict the ability to modify and unblock [155] the PIN.QES[156] to Signatory[157].

Application note 39: The SFR FMT_MTD.1/Admin addresses the first writing of the authentication reference data of the Cardholder (i.e. PIN and PUK) and the SFR FMT_MTD.1/WR of the technical components (i.e. public keys of the PKI roots) e.g. in the personalisation process. The modification of existing authentication reference data is separated into different roles and addressed by different SFR FMT_MTD.1/CH and FMT_MTD.1/Sigy. Note, the specification [22] does not describe detailed access conditions for the public keys because their implementation is specific for the operating system. The cardholder modifies his or her PIN.CH as special case of the User Authentication Reference Data by means of (i) the command CHANGE REFERENCE DATA and providing the old and the new PIN or (ii) the command RESET RETRY COUNTER and providing the PUK and the new PIN. He or she unblocks the PIN by means of (i) the command RESET RETRY COUNTER and providing the PUK and the new PIN or (ii) the command RESET RETRY COUNTER and providing the PUK (without a new PIN). In contrast to the Signatory who is not allowed to set a new PIN.QES when using RESET RETRY COUNTER.

FMT_MTD.1/RPK_MOD	**Management of TSF data – Modification of Authentication Reference Data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles

FMT_MTD.1.1/ RPK_MOD	The TSF shall restrict the ability to modify [158] the public keys of the root for CV certificate verification [159] to none [160].

FMT_MTD.1/PIN	**Management of TSF data – Protection of Human User Authentication Data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles

[155] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[156] [assignment: *list of TSF data*]
[157] [assignment: *the authorised identified roles*]
[158] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[159] [assignment: *list of TSF data*]
[160] [assignment: *the authorised identified roles*]

FMT_MTD.1.1/ PIN	The TSF shall restrict the ability to read [161] the PIN.QES [162], **read the PIN.CH** **disable the PIN.QES,** **disable the PUK.QES,** **disable the PIN.CH,** **disable the PUK.CH,** **modify the PUK.QES,** **modify the PUK.CH[163]** to none [164].

Application note 40: The refinement of the element FMT_MTD.1.1/PIN provides a list of restrictions in the same style. The specification [21] introduced the command DISABLE VERIFICATION REQUIREMENT, which changes the attribute *flagEnabled* of a password so that the COS acts as if the security status of the password is permanently set. Therefore it is necessary to prevent this command for PIN.QES, PUK.QES, PIN,CH and PUK.CH.

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

The TOE shall meet the requirement “TOE Emanation (FPT_EMSEC.1)” as specified below (CC extended):

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

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

[163] Refinement “(2) read the PIN.CH (3) disable the PIN.QES, (4) disable the PUK.QES, (5) disable the PIN.CH, (6) disable the PUK.CH, (7) modify the PUK.QES, (8) modify the PUK.CH”

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

FPT_EMSEC.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_EMSEC.1.1	The TOE shall not emit *information about IC power consumption and command execution time*[165] in excess of *non useful information*[166] enabling access to PIN.CH, PUK.CH, PIN.QES and PUK.QES[167] and Signature-creation private key (SCD), Card Authentication Private Keys, Client-Sever Authentication Private Key, Document Cipher Key Decipher Key, secure messaging keys symmetric authentication keys[168].
FPT_EMSEC.1.2	The TSF shall ensure that any authorized user [169] are unable to use the following interface smart card circuit contacts [170] to gain access to PIN.CH, PUK.CH, PIN.QES and PUK.QES [171] and Signature-creation private key (SCD), Card Authentication Private Key, Client-Sever Authentication Private Key, Document Cipher Key Decipher Key, secure messaging keys, symmetric authentication keys[172].

Application note 41: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks

[165] [assignment*: types of emissions*]
[166] [assignment: *specified limits*]
[167] [assignment: *list of types of TSF data*]
[168] [assignment: *list of types of user data*]
[169] [assignment: *type of users*]
[170] [assignment: *type of connection*]
[171] [assignment: *list of types of TSF data*]
[172] [assignment: *list of types of user data*]

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 HPC / SMC has to provide a smart card interface with contacts according to ISO/IEC 7816-2 [21] 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.

Dependencies: No dependencies.

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: exposure to operating conditions where therefore a malfunction could occur, failure detected by TSF according to FPT_TST.1 [173].

Application note 42: Those parts of the TOE which support the security functional requirements "TSF testing (FPT_TST.1)" and "Failure with preservation of secure state (FPT_FLS.1)" shall be protected from interference of the other security enforcing parts of the HPC chip Embedded Software. The security enforcing functions and health application data shall be separated in a way preventing any interference.

The TOE shall meet the requirements of "Passive detection of physical attack (FPT_PHP.1)" as specified below (Common Criteria Part 2).

FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

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

FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

The TOE shall meet the requirements of "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.

Dependencies: No dependencies.

FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing [174] to the TSF [175] by responding automatically such that the SFRs are always enforced.

Application note 43: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the SFRs are always enforced. 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 "Inter-TSF basic TSF data consistency (FPT_TDC.1)" as specified below (Common Criteria Part 2).

FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret CVC[176] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use [21], chapter 7,[177] when interpreting the TSF data from another trusted IT product.

[174] [assignment: *physical tampering scenarios*]

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

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

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.

Dependencies: No dependencies.

FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, at the conditions Reset of the TOE*[178] [179] to demonstrate the correct operation of the TSF [180]..
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[181].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of *stored TSF executable code*[182].

Application note 44: If HPC 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" Manufacture 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. The security target writer performed the operation claimed by the concrete product under evaluation.

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

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

[178] [selection*: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*]

[179] [assignment*: conditions under which self test should occur*]

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

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

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

7.1.6 SFR for Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit another trusted IT product [183] 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 [184].

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 component:

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 [19]. 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

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

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

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 [20], 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 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_CAMS	OT.Data_Confident	OT.Data_Integrity	OT.Dec_Trans	OT.DS_CSA	OT.TSS	OT.AC_Serv	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.Sig_Secure	OT.DTBS_Integrity_TOE	OT.TOE_TC_DTBS	OT.Trusted_Channel	OT.Sigy_SigF	OT.Prot_Abuse_Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Tamper_ID	OT.Prot_Phys_Tamper	OT.Lifecycle_Security
FCS_RNG.1						x	x	x	x					x	x						
FCS_COP.1/SHA							x							x	x						
FCS_COP.1/CCA_SIGN							x							x	x						

	OT.AC_CAMS	OT.Data_Confident	OT.Data_Integrity	OT.Dec_Trans	OT.DS_CSA	OT.TSS	OT.AC_Serv	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.Sig_Secure	OT.DTBS_Integrity_TOE	OT.TOE_TC_DTBS	OT.Trusted_Channel	OT.Sigy_SigF	OT.Prot_Abuse_Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Tamper_ID	OT.Prot_Phys_Tamper	OT.Lifecycle_Security
FCS_COP.1/ CCA_VERIF							x							x	x						
FCS_COP.1/3TDES														x							
FCS_COP.1/RMAC														x							
FCS_CKM.1.1/AKP								x	x	x											
FCS_CKM.1/Asym_Auth							x							x	x						
FCS_CKM.1/Sym_Auth														x							
FCS_CKM.4														x							
FCS_COP.1/Sign											x										
FCS_COP.1/CSA					x																
FCS_COP.1/RSA_DEC				x																	
FCS_COP.1/ RSA_TRANS				x																	
FIA_AFL.1/CH							x														
FIA_AFL.1/CH_PUK							x														
FIA_AFL.1/QES															x						
FIA_AFL.1/QES_PUK															x						
FIA_SOS.1							x								x						
FIA_ATD.1							x								x						
FIA_UID.1	x					x	x								x						
FIA_UAU.1	x					x	x								x						
FIA_UAU.4							x						x	x	x						
FIA_UAU.5							x						x		x						
FIA_UAU.6							x						x	x	x						
FIA_API.1					x		x								x						
FDP_ACC.1/Sign		x	x					x					x		x						
FDP_ACF.1/Sign		x	x					x					x		x						
FDP_ACC.1/CH	x	x	x	x	x	x	x							x							
FDP_ACF.1/CH	x	x	x	x	x	x	x							x							
FDP_UCT.1							x							x	x						
FDP_UIT.1							x							x	x						

	OT.AC_CAMS	OT.Data_Confident	OT.Data_Integrity	OT.Dec_Trans	OT.DS_CSA	OT.TSS	OT.AC_Serv	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.Sig_Secure	OT.DTBS_Integrity_TOE	OT.TOE_TC_DTBS	OT.Trusted_Channel	OT.Sigy_SigF	OT.Prot_Abuse_Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Tamper_ID	OT.Prot_Phys_Tamper	OT.Lifecycle_Security
FDP_ITC.1				x																	
FDP_ETC.1													x								
FDP_RIP.1		x											x								
FDP_SDI.2			x									x									
FMT_SMF.1	x						x								x						
FMT_SMR.1	x						x						x		x						
FMT_LIM.1		x	x				x								x	x					
FMT_LIM.2		x	x				x								x	x					
FMT_MSA.1															x	x					
FMT_MSA.2				x	x		x	x					x		x	x					
FMT_MSA.3							x														
FMT_MTD.1/INI	x																				
FMT_MTD.1/WR	x						x						x								
FMT_MTD.1/Admin	x						x								x						
FMT_MTD.1/CH	x	x					x														
FMT_MTD.1/Sigy	x	x													x						
FMT_MTD.1/PIN	x	x					x								x						
FMT_MTD.1/RPK_MOD							x						x		x						
FPT_EMSEC.1		x		x	x						x		x				x				
FPT_FLS.1		x	x														x	x			
FPT_PHP.1																			x		
FPT_PHP.3		x	x														x	x		x	
FPT_TDC.1													x								
FPT_TST.1																	x	x			x
FTP_ITC.1													x	x							

Table 7: Security functional requirements rationale

7.3.2 Security Functional Requirements Sufficiency

The security objective **OT.AC_CAMS** "Access control for management" mainly implemented by following SFRs:

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

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

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

(iv) The SFRs **FMT_MTD.1/WR** limits the creation of the authentication reference data of the Cardholder and the PKI root for the card-to-card authentication to the Personalisation Agent.

(v) The SFR **FMT_MDT.1/INI** defining that the Card Management System role shall be created by the Manufacturer.

(vi) **FMT_MTD.1/CH** and **FMT_MTD.1/PIN** limiting the access to authentication reference data of the cardholder.

(vii) **FMT_MTD.1/Admin, FMT_MTD.1/Sigy** and **FMT_MTD.1/PIN** limiting the access to authentication reference data of the signatory.

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

(i) The SFRs **FMT_MTD.1/CH** and **FMT_MTD.1/PIN** protect the confidentiality of the PIN.CH and PUK.CH authentication reference data as Cardholder against reading, disabling and unauthorized modification.

(ii) The SFRs **FMT_MTD.1/Sigy** and **FMT_MTD.1/PIN** protect the confidentiality of the PIN.QES and PUK.QES authentication reference data as Signatory against reading, disabling and unauthorized modification.

(iii) The SFRs **FDP_ACC.1/Sign, FDP_ACF.1/Sign, FDP_ACC.1/CH** and **FDP_ACF.1/CH** protect the confidentiality the private keys against reading.

(iv) The SFRs **FDP_ACC.1/CH** and **FDP_ACF.1/CH** ensure that only authenticated SMC and ASCA may read the EF.DM in DF.ESIGN and the EF.DM in DF.QES, while the cardholder may modify them.

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

(vi) The SFRs **FMT_LIM.1** and **FMT_LIM.2** prevents misuse of test functionality in order to compromise user or TSF data.

(vii) The SFRs **FPT_EMSEC.1**, **FPT_FLS.1** and **FPT_PHP.3** 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 SFRs **FDP_ACC.1/Sign, FDP_ACF.1/Sign, FDP_ACC.1/CH** and **FDP_ACF.1/CH** protect the integrity of the user data under the TSC.

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

(iii) The SFRs **FMT_LIM.1** and **FMT_LIM.2** prevents misuse of test functionality in order to manipulate user or TSF data.

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

The security objective **OT.DEC_TRANS** "Document key decryption and transcipherment" addresses document cipher key decipherment with an internal private key and document cipher key transcipherment with internal private key and imported public key. It is implemented by the SFRs:

(i) The SFRs **FCS_COP.1/RSA_DEC** and **FCS_COP.1/RSA_TRANS** provide the cryptographic operations.

(ii) The SFRs **FDP_ACC.1/CH** and **FDP_ACF.1/CH** enforces access control for the service.

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

(iv) The SFR **FMT_MSA.2** enforces secure security attributes of the private key.

(v) The SFR **FPT_EMSEC.1** protects the confidentiality of the private key during cryptographic operation.

The security objective **OT.DS_CSA** "Digital signature-creation for client / server authentication" address service for digital signature creation with an internal private signature key and is implemented by the SFRs:

(i) The SFR **FCS_COP.1/CSA** provides the cryptographic operation.

(ii) The SFR **FIA_API.1** describes digital signature-creation for client / server authentication as authentication of the TOE to a server.

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

(iv) The SFR **FMT_MSA.2** enforces secure security attributes of the private key.

(v) The SFR **FPT_EMSEC.1** protects the confidentiality of the private key during cryptographic operation.

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. 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/CH** and **FDP_ACF.1/CH** enforce access control for the service allowing the terminal to use this service.

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 human user authentication and the access control for these security services is implemented by following SFRs:

(i) The SFRs **FCS_RNG.1**, **FCS_COP.1/SHA**, **FCS_COP.1/CCA_Sign**, **FCS_COP.1/CCA_Verif** and **FCS_CKM.1/Asym_Auth** provide the necessary cryptographic primitives for user authentication used to enforce **OT.AC_Serv**.

(ii) The SFR **FMT_SMF.1** is capable of performing of the following management functions: Initialization, Personalization, Card Management, Modification of the PIN.CH , Modification of the PIN.QES and Modification of the security attribute "SCD operational" of the signature-creation data PrK.HC.QES.

(iii) The SFR **FMT_SMR.1** defines the Card Management System, the Cardholder, the SMC, the Authorised signature-creation application and a Terminal as known roles of the TOE and **FIA_ATD.1** binds identity and role provided by the authentication.

(iv) The SFR **FMT_MTD.1/PIN** enforces the user authentication by prevention of disabling the PIN:CH and PUK.CH.

(v) The SFR **FIA_SOS.1** enforces the quality and **FIA_AFL.1/CH** as well as **FIA_AFL.1/CH_PUK** protect against guessing of PIN.CH and PUK.CH.

(vi) The SFR **FMT_MTD.1/CH** limits the management of the authentication reference data to the Cardholder. These authentication reference data have initially been created by the administrator as specified by the SFR **FMT_MTD.1 / Admin**.

(vii) The SFRs **FIA_UAU.4**, **FIA_UAU.5** and **FIA_UAU.6** implement the authentication mechanism used to enforce **OT.AC_Serv**.

(viii) The SFR **FIA_API.1** implements the authentication of the TOE to users addressed by **OT.AC_Serv**.

(ix) The SFRs **FIA_UID.1** and **FIA_UAU.1** allow the use of identified TSF mediated actions before identification and authentication of the user.

(x) The SFRs **FDP_ACC.1/CH** and **FDP_ACF.1/CH** define the access controls rules for the use of the security services according to the HC Access Control SFP.

(xi) The SFRs **FDP_UCT.1** and **FDP_UIT.1** enforce the HC Access Control SFP for import and export of user data.

(xii) 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.

(xiii) The SFRs **FMT_MSA.2** and **FMT_MSA.3** allow the management of security attributes.

(xiv) The SFR **FMT_MTD.1/RPK_MOD** prevents modification of the root public key as reference authentication data for users addressed in **FDP_ACC.1/CH** (except cardholder).The SFR **FMT_MTD.1/WR** restricts the ability to create the User Reference Authentication Data, and public keys of the root for CVC verification to the Personalisation Agent.

The security objective **OT.SCD/SVD_Gen** "SCD/SVD generation" requires the TOE to ensure that authorised users only invoke the generation of the SCD and the SVD. It is implemented by the following SFRs:

(i) The SFRs **FDP_ACC.1/Sign** and **FDP_ACF.1/ Sign** limits the SCD/SVD generation to the Administrator.

(ii) The SFR **FCS_RNG.1** provides random number generation, the SFR **FCS_CKM.1/AKP** provides generation of the cryptographic key for RSA.

(iii) The SFR **FMT_MSA.2** requires secure security attributes in order to prevent re-generation of SCD/SVD pairs if SCD/SVD pair exists already.

The security objective **OT.SCD_Unique** "Uniqueness of the signature-creation data" is implemented by SFR **FCS_CKM.1/AKP** to generate the cryptographic key pair and **FCS_RNG.1** providing random numbers with sufficient entropy.

The security objective **OT.SCD_SVD_Corresp** "Correspondence between SVD and SCD**"** is implemented directly by the **FCS_CKM.1/AKP** to generate the cryptographic key pair.

The security objective **OT.Sig_Secure** "Cryptographic security of the electronic signature**"** is implemented by the SFR **FCS_COP.1/Sign**. In addition the SFR **FPT_EMSEC.1** protects the confidentiality of the private key during cryptographic operation.

The security objective **OT.DTBS_Integrity_TOE** "DTBS-representation integrity inside the TOE" is implemented directly by **FDP_SDI.2**.

The security objective **OT.TOE_TC_DTBS** "Trusted channel of TOE for DTBS**"** is implemented by the following SFRs:

(i) The SFRs **FIA_UAU.4**, **FIA_UAU.5** and **FIA_UAU.6** implement the different authentication mechanism used to enforce **OT.TOE_TC_DTBS.**

(ii) The SFRs **FDP_ACC.1/Sign** and **FDP_ACF.1/Sign** enforcing the access control rule (cf. ACF_ACF.1.2/Sign clause 2).

(iii) The SFR **FMT_SMR.1** defines the rule of the Authorised signature-creation application.

(iv) The SFR **FDP_ETC.1** enforces the Signature-creation SFP and HC Access Control SFP when exporting user data, controlled under the SFP(s), outside of the TSC

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

(vi) The SFR **FMT_MSA.2** requires secure security attributes in order to enforce the Signature-creation SFP.

(vii) The SFR **FMT_MTD.1/WR** restricts the ability to create the User Reference Authentication Data, and public keys of the root for CVC verification to the Personalisation Agent.

(viii) The SFR **FMT_MTD.1/RPK_MOD** prevents modification of the root public key as reference authentication data for users addressed in **FDP_ACC.1/Sign** (except cardholder).

(ix) The SFR **FPT_EMSEC.1** protects the confidentiality of the private key during cryptographic operation.

(x) The **FPT_TDC.1** provides the capability to consistently interpret CVC when shared between the TSF and another trusted IT product.

(xi) The SFR **FTP_ITC.1** provides the protection of the confidentiality and integrity of the transmitted data.

The security objective **OT.Trusted_Channel** "Trusted Channel" as part of the TOE security services Service_Asym_Mut_Auth_with_SM and Service_Sym_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 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.**

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

(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 SFRs **FDP_ACC.1/CH** and **FDP_ACF.1/CH** define the access controls rules for the use of the security services according to the HC Access Control SFP.

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

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

The security objective **OT.Sigy_SigF** "Signature generation function for the legitimate signatory only**"** is implemented by the following SFRs:

(i) The SFRs **FCS_RNG.1**, **FCS_COP.1/SHA**, **FCS_COP.1/CCA_Sign**, **FCS_COP.1/CCA_Verif** and **FCS_CKM.1/Asym_Auth** provide the necessary cryptographic primitives for user authentication used to enforce **OT.Sigy_SigF**.

(ii) The SFR **FMT_SMR.1** defines the Administrator, the Signatory, the SMC, the Authorised signature-creation application and a Terminal as known roles of the TOE and **FIA_ATD.1** binds identity and role provided by the authentication.

(iii) The SFR **FMT_SMF.1** defines the security management function Modification of the PIN.QES (the legitimate Signatory must be successfully authenticated with PIN.QES).

(iv) The SFR **FMT_MTD.1/PIN** enforces the user authentication by prevention of disabling the PIN.QES and PUK.QES.

(v) The SFR **FIA_SOS.1** enforces the quality and **FIA_AFL.1/QES** as well as **FIA_AFL.1/QES_PUK** protects against guessing of PIN.QES and PUK.QES.

(vi) The SFR **FMT_MTD.1/Sigy** limits the management of the authentication reference data to the Signatory. These authentication reference data have initially been created by the administrator as specified by the SFR **FMT_MTD.1 / Admin**.

(vii) The SFRs **FIA_UAU.4**, **FIA_UAU.5** and **FIA_UAU.6** implement the authentication mechanism used to enforce **OT.Sigy_SigF**.

(viii) The SFR **FIA_API.1** implements the authentication of the TOE to users addressed by **OT.Sigy_SigF**.

(ix) The SFRs **FIA_UID.1** and **FIA_UAU.1** allow the use of identified TSF mediated actions before identification and authentication of the user.

(x) The SFR **FDP_ACC.1/Sign** and **FDP_ACF.1/Sign** define the access controls rules for the use of the security services according to the Signature-creation SFP.

(xi) The SFRs **FDP_UCT.1** and **FDP_UIT.1** enforce the Signature-creation SFP for import and export of user data.

(xii) 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.

(xiii) The SFR **FMT_MSA.1** "Management of security attributes" restricts the ability to modify the security attributes SCD operational to Signatory.

(xiv) The SFR **FMT_MSA.2** requires secure security attributes in order to enforce the Signature-creation SFP.

(xv) The SFR **FMT_MTD.1/RPK_MOD** prevents modification of the root public key as reference authentication data for users addressed in **FDP_ACC.1/Sign** (except cardholder).

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

(i) 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.

(ii) The SFR **FMT_MSA.1** "Management of security attributes" restricts the ability to modify the security attributes SCD operational to Signatory.

(iii) The SFR **FMT_MSA.2** requires secure security attributes in order to enforce the Signature-creation SFP.

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

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

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

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

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

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

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

(iii) ***FPT_TST.1*** *also covers* ***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.Tamper_ID** “Tamper Detection” is implemented directly by the SFR **FPT_PHP.1** "Passive detection of physical attack"**.**

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 SFRs are 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	FCS_CKM.4, FCS_COP.1/CCA_SIGN is used for authentication of the TOE to other entities and therefore the key is TSF-data. The private key is written during initialisation (cf. OE.Pers_CAMS).
FCS_COP.1/CCA_VERIF	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with	FCS_CKM.4, FCS_COP.1/CCA_VERIF is used for authentication

SFR	Dependencies	Support of the Dependencies
	security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	and therefore the keys are TSF-data. The root public key is written during initialization (cf. OE.Pers_CAMS) and the other public keys are imported according to FPT_TDC.1.
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/Asym_Auth or FCS_CKM.1/Sym_Auth according to the used authentication method, FCS_CKM.4
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/Asym_Auth or FCS_CKM.1/Sym_Auth according to the used authentication method, FCS_CKM.4
FCS_CKM.1/AKP	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4	FCS_COP.1/Sign, FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
	Cryptographic key destruction	
FCS_CKM.1/Asym_Auth	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Generated keys are used for FCS_COP.1/3TDES and FCS_COP.1/RMAC in case of SM keys and FCS_CKM.1/Sym_Auth in case of introduction keys. FCS_CKM.4
FCS_CKM.1/Sym_Auth	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/3TDES, FCS_COP.1/RMAC, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1
FCS_COP.1/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	FCS_CKM.1/AKP, FCS_CKM.4
FCS_COP.1/CSA	[FDP_ITC.1 Import of user data without security attributes, or	FCS_CKM.1/AKP, FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
	FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	
FCS_COP.1/RSA_DEC	[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 SFR FCS_COP.1/RSA_DEC uses keys, which are loaded or generated during the personalisation and not updated or deleted over the life time of the TOE. Therefore none of the listed SFRs needed to be defined for this specific instantiations of FCS_COP.1.
FCS_COP.1/RSA_TRANS	[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 SFR FCS_COP.1/RSA_TRANS uses private keys, which are loaded or generated during the personalisation and not updated or deleted over the lifetime of the TOE. Therefore none of the listed SFRs needed to be defined for this specific instantiations of FCS_COP.1. The public key is imported according to FDP_ITC.1.
FIA_AFL.1/CH	FIA_UAU.1 Timing of authentication	fulfilled

SFR	Dependencies	Support of the Dependencies
FIA_AFL.1/CH_PUK	FIA_UAU.1 Timing of authentication	fulfilled
FIA_AFL.1/QES	FIA_UAU.1 Timing of authentication	fulfilled
FIA_AFL.1/QES_PUK	FIA_UAU.1 Timing of authentication	fulfilled
FIA_SOS.1	No dependencies	n. a.
FIA_ATD.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.
FIA_API.1	No dependencies	n. a.
FDP_ACC.1/Sign	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/Sign
FDP_ACF.1/Sign	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.1/Sign, FMT_MSA.3
FDP_ACC.1/CH	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/CH
FDP_ACF.1/CH	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/CH, FMT_MSA.3
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	FTP_ITC.1 FDP_ACC.1/Sign and FDP_ACC.1/CH

SFR	Dependencies	Support of the Dependencies
	information flow control]	
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 FDP_ACC.1/Sign and FDP_ACC.1/CH
FDP_ITC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/Sign and FDP_ACC.1/CH, FMT_MSA.3
FDP_ETC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/Sign and FDP_ACC.1/CH
FDP_RIP.1	No dependencies	n. a.
FDP_SDI.2	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	fulfilled
FMT_LIM.2	FMT_LIM.1	fulfilled
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/Sign, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 Subset	FDP_ACC.1/CH,

SFR	Dependencies	Support of the Dependencies
	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/Sign, FMT_SMR.1, FMT_MSA.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/INI	FMT_SMF.1 Specification of Management Functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/WR	FMT_SMF.1 Specification of Management Functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/Admin	FMT_SMF.1 Specification of Management Functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/CH	FMT_SMF.1 Specification of Management Functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/Sigy	FMT_SMF.1 Specification of Management Functions,	fulfilled

SFR	Dependencies	Support of the Dependencies
	FMT_SMR.1 Security roles	
FMT_MTD.1/RPK_MOD	FMT_SMF.1 Specification of Management Functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/PIN	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.1	No dependencies	n. a.
FPT_PHP.3	No dependencies	n. a.
FPT_TDC.1	No dependencies	n. a.
FPT_TST.1	No dependencies	n. a.
FTP_ITC.1	No dependencies	n. a.

Table 8: Dependency rationale overview

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 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 HPC specification. The chosen SFRs of classes FIA and FDP support (i) the access control policy HC Access Control SFP as defined in the objective OT.AC_CAMS and OT.AC_Serv and (ii) the access control policy Signature-creation SFP as defined in the objective OT.Sigy_SigF. The chosen SFRs of class FMT support the secure management of TSF data in a way, which is consistent to the policy HC Access Control SFP and Signature-creation SFP. The SFRs of all these classes (FCS, FIA, FDP, FMT) together provide the HPC services as defined in the TOE description (chapter 2.1). The remaining SFRs, chosen from class FPT define low level protection of the TOE against any attempt to bypass the security policy S HC Access Control SFP and Signature-creation SFP and 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 gives the overview description of the different TOE Security Functions composing the TSF.

8.1 SF_AccessControl

The TOE provides access control mechanisms that allow among others the maintenance of different users and roles. After activation or reset no user is authenticated.

The ability to execute TSF commands and access TSF data is bound to access rules which are (among other aspects) based on the authentication status of the corresponding subject:

The cardholder can authenticate himself using the PIN.CH. After 3 unsuccessful consecutive authentication attempts the PIN.CH is blocked and can only be unblocked using the PUK.CH, which can be used maximally 10 times.

The signatory uses the PIN.QES which will be blocked after 3 unsuccessful attempts; it can be unblocked using the PUK.QES (maximally 10 times).

After having successfully verified the PIN.CH, a cardholder can

1. authenticate himself at a server using the client-server authentication service
2. make a mutual card-to-card (C2C) authentication with other entities: a Security Module Card (SMC) (e.g. in the role of a PIN sender) as well as an electronic Health Card (eHC)
3. execute document key decipher- and transcipherment

A CAMS can be authenticated using symmetric or asymmetric authentication.

After successful verification of the PIN.QES, a signatory can create 1 qualified electronic signature in the security environment No.1 and up to 250 signatures in security environment No.2 (the so-called “Stapelsignatur”).

The access control mechanisms ensure that only the Administrator can generate the qualified signature key pair or export the public signature key in an authentic way for certification or store a transport value for the PIN.QES. The SVD is exported without associated security attributes. The SVD is exported in the personalisation phase. The integrity and authenticity of the SVD can be ensured by symmetric or asymmetric cryptography.

The Manufacturer authenticates with an authentication mechanism for the initialisation phase. Only initialisation and pre-personalisation data authorised by the Manufacturer will be accepted by and loaded into the TOE.

The Personalisation Agent authenticates with an authentication mechanism for the personalisation phase. The mechanism guarantees that only personalisation data authorised by the Personalisation Agent (particularly, user reference authentication data and public keys of the root for CVC verification) will be accepted by and loaded into the TOE.

The access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication.

Some actions are only allowed if a trusted channel is used (see 8.4).

This security function covers the following SFRs:

FDP_ACC.1/Sign, FDP_ACC.1/CH, FDP_ACF.1/Sign, FDP_ACF.1/CH, FDP_ETC.1, FDP_ITC.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_AFL.1/CH, FIA_AFL.1/CH_PUK, FIA_AFL.1/QES, FIA_AFL.1/QES_PUK, FIA_ATD.1, FIA_SOS.1, FIA_API.1, FMT_MTD.1/INI, FMT_MTD.1/WR, FMT_MTD.1/Admin, FMT_MTD.1/CH, FMT_MTD.1/Sigy, FMT_MTD.1/RPK_MOD, FMT_MTD.1/PIN, FPT_TDC.1

8.2 SF_Management

The ability to carry out management actions are restricted by access control (see 8.1). They guarantee that management can only be performed by the attributed roles, namely the ones defined in “FMT_SMR.1 Security roles**”**.

The following management actions are possible:

1. Initialisation, pre-personalisation and personalisation
2. Modification of PIN.CH and PUK.CH (restricted to the cardholder)
3. Modification of PIN.QES and PUK.QES (restricted to the signatory)
4. Setting the security attribute “SCD operational” (restricted to the signatory)
5. loading new applications and data by a card management system (CAMS) according to the access rules

This security function covers the following SFRs:

FDP_ACF.1/Sign, FDP_ACF.1/CH, FMT_SMF.1, FMT_SMR.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3

8.3 SF_Protection

When keys or PINs are no longer needed in the internal memory of the TOE, 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.

The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. It 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.

Test features of the TOE after TOE delivery are restricted to self-test functionality.

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

8.4 SF_TrustedCommunication

The TOE supports the establishment of a trusted channel/path based on mutual authentication with negotiation of symmetric cryptographic keys used for the protection of the communication data with respect to confidentiality and integrity. The mutual authentication is based on a challenge response protocol using symmetric or asymmetric algorithms as defined in [21]. 3TDES with a key size of 168 bit is used for encryption and integrity protection of the communication data. Via a trusted channel/path the Administrator can authentically export the public signature key for certification, import the certificate or certificate information for the public signature key and load new applications and data on the card. The remote entry of PIN data is also secured by a trusted channel. The negotiated session keys may be either ephemeral or permanent; in the latter case, they are denoted as “introduction keys”.

This security function covers the following SFRs: FDP_ACF.1/Sign, FDP_ACF.1/CH, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1

8.5 SF_Crypto

The TOE supports the following cryptographic operations:

1. 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 [28]; (ii) a true random number generator (TRNG) based on a physical source according to AIS31 [29].
2. Onboard generation of RSA keypairs with key length 2048 bit. To this end, the TOE uses random numbers generated by its P2 (high) physical random number generator.
3. Generation of secure hash values with the SHA-256 algorithm according to the FIPS 180-2 standard [16].
4. Encryption, decryption and key generation/agreement with 3TDES in CBC mode, using 168 bit keys in accordance with [15] and [21]. This makes use of the IC's Triple-DES co-processor.
5. RSA encryption and decryption with cryptographic key sizes of 2048 bit, to be used for ciphering, generation of signatures and several authentication mechanisms. Digital signatures created with this function can be regarded as qualified signatures if they are based on a valid qualified certificate at the time of signature creation, i.e. if they were created using SCD with a corresponding SVD which had been exported to a CSP, certified and made available as a qualified certificate.
6. Generation and verification of a message authentication code (Retail MAC), using 168 bit keys in accordance with [21].
7. Digital signatures as well as the corresponding signature verification. The signatures can be used for card-to-card authentication or for qualified signatures if they are based on a qualified certificate at the time of signature creation.
8. Secure destruction of keys: Overwriting all keys stored in EEPROM with zero values.

This security function covers the following SFRs:

FCS_RNG.1/DRNG, FCS_RNG.1/PHYS, FCS.COP.1/SHA, FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/3TDES, FCS_COP.1/RMAC, FCS_COP.1/Sign, FCS_COP.1/CSA, FCS_COP.1/RSA_DEC, FCS_COP.1/RSA_TRANS, FCS_CKM.1/AKP, FCS_CKM.1/Asym_Auth, FCS_CKM.1/Sym_Auth, FCS_CKM.4

8.6 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 9: References of Assurance Measures

9 Conventions and Terminology

9.1 Conventions

The document follows the rules and conventions laid out in Common Criteria 3.1, part 1 [8], Annex B “Specification of Protection Profiles”.

9.2 Terminology

Administrator means an user that performs TOE initialisation, TOE personalisation, or other TOE administrative functions.
Advanced electronic signature (defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control, and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Authentication data is information used to verify the claimed identity of a user. The TOE provides role-based authentication of the roles Admin and Signatory without further identification of the user.
Certificate means an electronic attestation, which links the SVD to a person and confirms the identity of that person (as defined in the Directive [1], article 2, clause 9).
Certificate info means information associated with a SCD/SVD pair that consists either: a signer's public key certificate, or one or more hash values of a signer's public key certificate together the identifier of the hash function used to compute these hash values, and some information which allows the signer to disambiguate between several signers certificates."
Certification generation application (CGA) means a collection of application elements which receives the SVD from the SSCD for generation of the certificate, obtaining the data included in the certificate and creating the signature of the certificate.
Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (as defined in the Directive [1], article 2(11))

Data to be signed (DTBS) means the complete electronic data to be signed (including both user message and signature attributes).
Data to be signed or its unique representation (DTBS/R) means the data received by a secure signature creation device as input in a single signature-creation operation Note: DTBS/R is either a hash-value of the data to be signed (DTBS), or an intermediate hash-value of a first part of the DTBS complemented with a remaining part of the DTBS, or the DTBS.
Directive: The Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] is also referred to as the 'Directive' in the remainder of the ST.
Notified body: The Member States shall notify to the Commission and the other Member States about the national bodies (referred as notified bodies in this ST) which are responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4) (cf. Directive [1], article 11(1b)). Note the bodies referred to in Article 3(4) determine the conformity of secure signature-creation-devices with the requirements laid down in Annex III.
Qualified certificate means a certificate, which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1] (cf. the Directive [1], article 2.10).
Qualified electronic signature means an advanced signature which is based on a qualified certificate and which is created by an SSCD according to the Directive [1], article 5, paragraph 1.
Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.
SSCD-provisioning service service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD
Secure signature-creation device (SSCD) means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive [1]. (The term SSCD is defined in the Directive [1], article 2.5 and 2.6).
Signatory means a person who holds an SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents (as defined in the Directive [1], article 2.3).

Signature attributes means additional information that is signed together with the user message.
Signature-creation application (SCA) means the application used to create an electronic signature, excluding the SSCD. I.e., the SCA is a collection of application elements (a) to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision, (b) to send a DTBS-representation to the TOE, if the signatory indicates by specific non-misinterpretable input or action the intent to sign, (c) to include the digital signature generated by the TOE into the electronic signature.
Signature-creation-data (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature (as defined in the Directive [1], article 2.4). In the context of this ST the SCD means the private key used to create the signature.
Signature-creation system (SCS) means the overall system that creates an electronic signature. The signature-creation system consists of the SCA and the SSCD.
Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature (as defined in the Directive [1], article 2.7). In the context of this ST the SVD means the public key corresponding to the SCD implemented on the SSCD and used to verify the signature.
Signed data object (SDO) means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.
SSCD provision service means a service that prepares and provides an SSCD to subscribers. For a Type 3 SSCD the SSCD provision service runs a collection of application elements which installs the SRAD in the SSCD, requests the generation of one or more SCD / SVD key pairs by the SSCD, requests the SVD from the SSCD, and provides the SVD to the CGA to create the certificate or certificates by the appropriate Certification Authorities. In most cases the SSCD provision service will be a part of the Certification-service-provider.
User means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user’s biometric characteristics.

10 PP Application Notes

10.1 Glossary and Acronyms

Term	Definition
Advanced electronic signature	an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. Advanced electronic signatures are based on certificate and uses digital signature.
Application note	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Card Application Management System	Card Application Management System (CAMS) allows the loading of a new application or the creation of a new EF on MF level or DF.HPA after issuing of the HPC.
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 Software	IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
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 HPC's chip is an integrated circuit.
Personalization	The process by which personal data are brought into the TOE before it is handed to the cardholder
Qualified electronic signature	Advanced electronic signature generated by an secure-signature creation device and based on an qualified certificate.
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to

	ISO/IEC 7816-4
Security Module Card	Smart card providing security services in the health care environment.
Security environment #1	Default SE for use of the signature function in single signature mode. A use of a trusted channel is not required. It is possible to establish a trusted channel though.
Security environment #2	SE for use of the signature function in stack and comfort signature mode. A trusted channel is used between HPC/SMC-K for transmission of data to be signed in a health professional environment (verified by the card).
Trusted channel	Common Criteria [8], para. 89: a means by which a TSF and a remote trusted IT product can communicate with necessary confidence. HPC specification [21], Kap. 15: communication using secure messaging while the HPC is using a secure messaging key desSessionKey4SM to receive and to answer commands and the SMC is using a trusted channel key desSessionKey4TC to encrypt commands,, to calculate MAC for commands to decrypt command responses and to verify MAC of command responses.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [8]).
User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [8]).

Acronyms

Acronyms	**Term**
2TDES	2-key Triple-DES (using keys with an effective length of 112 bit)
3TDES	3-key Triple-DES (using keys with an effective length of 168 bit)
ASCA	Authorised signature-creation application
ATR	Answer To Reset

CA	Certification authority
CAMS	Card Application Management System
CBC	Cipher Block Chaining
CC	Common Criteria
CGA	Certification generation application
CH	Card Holder
CHA	Certificate Holder Authorization
CHR	Certificate Holder Reference
COS	Card Operating System
CSP	Certification service provider
CVC	Card verifiable certificate
CVC.CA_HPC.CS	Certificate of the Certificate Service Provider for card verifiable certificates in the health care environment
CVC.HPC.AUT	Certificate of the public key PuK.HPC.AUT corresponding to the private key PrK.HPC.AUT of the HPC
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
DF	Dedicated File
DFA	Differential Fault Analysis
DM	Display Message
DO	Data Object
DPA	Differential Power Analysis
DTBS	Data to be signed
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable ROM
EF	Elementary File
eHC	Electronic health card
ES	Embedded Software
GDO	Global Data Object
HBA	Heilberufsausweis (German for HPC)
HPA	Health professional application
HPC	Health professional card

IC	Integrated Circuit
ICC	Integrated Circuit Card
ICCSN	ICC Serial Number
I/O	Input/Output
IT	Information Technology
MAC	Message Authentication Code
MF	Master File
OE	Objective on the TOE environment
OS	Operating System
OSP	Organisational Security Policy
OT	Objective on the TOE
PIN	Personal Identification Number
PIN.CH	Global PIN of human user authentication for all HPC security services except the application for qualified signature
PIN.QES	DF-specific PIN of human user authentication used only for protection of the SigG/SigV-related private electronic signature key of the health professional.
PKI	Public Key Infrastructure
PP	Protection Profile
PrK.HP.AUT	Private key for client-server authentication
PrK.HP.ENC	Private key to decipher document encryption keys
PrK.HP.QES	Private key for qualified signature
PrK.HPC.AUT	Private key for card-to-card authentication between TOE and external SMC or eHC
PrK.HPC.AUTD_SUK_CVC	Private key for C2C authentication between HPC and SMC for DTBS-Transfer with establishing a trusted channel
PrK.HPC.AUTR_CVC	Private key for C2C authentication between HPC and eHC/CAMS with or without establishing a trusted channel and for authorization of SMC-A and SMC-B
PSO	Perform Security Operation

PUK	PIN Unblocking Key
PuK.CAMS_HP	Public key used for authentication of an external CAMS
PuK.CA_NN_HPC.CS	Public Key of the Certificate Service Provider for card verifiable certificates in the health care environment
PUK.CH	Reset code for PIN.CH
PUK.QES	Reset code for PIN.QES
PuK.RCA.CS	Root public key for verification of the card verifiable certificate of the certificate service provide for card verifiable certificates in the health care environment
QES	Qualified electric signature
RAD	Reference authentication data
RC	Retry Counter
RD	Reference Data
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
SAR	Security assurance requirements
SCA	Signature-creation application
SCD	Signature-creation data
SCS	Signature-creation system
SDO	Signed data object
SE#1	Security environment #1
SE#2	Security environment #2
SF	Security Function
SFP	Security Function Policy
SFR	Security functional requirement
SHA	Secure Hash Algorithm
SK	Secret Key
SK.HPC.AUT	Stored symmetric authentication key (introduction key)
SM	Secure Messaging

SMC	Security module card
SOF	Strength of Function
SSCD	Secure signature-creation device
SSEC	Security State Evaluation Counter
SSL	Security sockets layer
ST	Security Target
SVD	Signature-verification data
TOE	Target of Evaluation
TRNG	True RNG
TSC	TOE Scope of Control
TSF	TOE Security Functionality
TSFI	TSF Interface
VAD	Verification authentication data

11 References

[1] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[2] Protection Profile – Health Professional Card (PP-HPC) with SSCD functionality, Version 1.10, 17.November 2009, BSI-CC-PP-0018-V3

[3] EUROPEAN STANDARD, EN 14890-1:2008, Application Interface for smart cards used as secure signature creation devices – Part 1: Basic services

[4] 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

[5] Security Target Lite, P5CC052V0A, Rev. 1.5, 09.07.2009

[6] Smart Card IC Platform Version 1.0, Juli 2001, BSI-PP-0002-2001

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

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

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

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

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

[12] BSI TR-03114 Technische Richtlinie für die Stapelsignatur mit dem Heilberufsausweis, Bundesamt für Sicherheit in der Informationstechnik, Version 2.0, 19.10.2007

[13] BSI TR-03115 Technische Richtlinie für die Komfortsignatur mit dem Heilberufsausweis, Bundesamt für Sicherheit in der Informationstechnik, Version 2.0, 19.10.2007

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

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

[16] 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

[17] ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2005

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

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

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

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

[22] Specification German Health Professional Card and Security Module Card - Part 2: HPC Applications and Functions, Version 2.3.0, 04.07.2008, BundesÄrzteKammer, Kassenärztliche Bundesvereinigung, BundesZahnÄrzteKammer, BundesPsychotherapeutenKammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft

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

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

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

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

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

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

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

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

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