Bundesamt
für Sicherheit in der
Informationstechnik

# Common Criteria Protection Profile
# Secure Module Card (PP-SMC)

Common Criteria

BSI-PP-0019

Approved by the
Federal Ministry of Health

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

**Foreword**

This 'Protection Profile — Security Module Card (PP-SMC)' is issued by Bundesamt für Sicherheit in der Informationstechnik, Germany.

The document has been prepared as a Protection Profile (PP) following the rules and formats of Common Criteria version 2.2 [1], [2], [3] with final interpretations of the CCIMB.

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

CONTACT ADDRESS

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

**Tel +49 1888 9582-0**
**Fax +49 1888 9582-400**

**Email bsi@bsi.bund.de**

**Table of Content**

# 1 PP Introduction

## 1.1 PP reference

1 Title: Protection Profile — Secure Module Card (PP-SMC))

| | |
|---|---|
| Sponsor: | Bundesamt für Sicherheit in der Informationstechnik |
| Editors: | Wolfgang Killmann, T-Systems GEI GmbH |
| CC Version: | 2.1 (with Final Interpretation of CCIMB as of 04.04.2005) |
| Assurance Level: | The minimum assurance level for this PP is EAL4 augmented. |
| General Status: | final version |
| Version Number: | 1.0 |
| Registration: | BSI-PP-0019 |
| Keywords: | electronic health card, secure module card |

## 1.2 PP Overview

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

- Authentication of the card holder by use of a PIN,
- Mutual Authentication between the Security Module Card (SMC) and a Health Professional Card (HPC) or an electronic Health Card (eHC) with and without establishment of a trusted channel,
- Document key decipherment for an external application,
- Client-server authentication for a client,
- Creation of advanced electronic signature for the card holder.

## 1.3 Conformance Claim

3 This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, August 1999, version 2.1, CCIMB-99-031

- Common Criteria for Information Technology Security Evaluation, Part 2: Introduction and general model, August 1999, version 2.1, CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, August 1999, version 2.1, CCIMB-99-033

including the

- Final Interpretation of CCIMB as of 04.04.2005

as follows

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

# 2 TOE Description

## 2.1 TOE definition

4 The Target of Evaluation (TOE) is the Secure Module Card (SMC) Type B. The SMC is a contact based smart cards which is conformant to the specification documents [20] [22]. The physical characteristics shall comply with ISO/IEC 7816-1 and related standards.

5 The **TOE** comprises of

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

**TOE_ES**
- the IC Embedded Software (operating system)

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

and

**TOE_GD**
- the guidance documentation delivered together with the TOE.

**TOE usage and security features for operational use**

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

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

(2) to support trusted channel in interaction with SMC or a server,

(3) to provide PKI services as creation of digital signatures, decryption and client-server authentication for the health institution.

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

(1) Authentication of the card holder by use of a PIN,

(2) Access control for the function (3) to (8) listed below,

(3) Asymmetric card-to-card authentication between the SMC and a HPC supporting the management of access control authorization for access to eHC data,

(4) Asymmetric card -to-card authentication between the SMC and a eHC to get access to data under control of the eHC without establishment of a trusted channel,

(5) Symmetric card-to-card authentication between the HPC and a security module with establishment of a trusted channel,

(6) Creation of digital signatures for advanced electronic signatures,

(7) Document key decipherment,

(8) Client-server authentication,

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

## 2.2 TOE usage and security features for operational use

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

9 **Service_User_Auth_PIN**: The card holder authenticates himself with his PIN.

This service is meant as a support service for some of the other services, which may 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 ([22], Annex A).

Functions to change the PIN or to unblock the PIN (reset the retry counter), when it was blocked (because of successive false PIN entries) are supporting this service. For the letter the PIN unblocking code (PUC) is used, this authentication will be called **Service_User_Auth_PUC**.

10 The user have to be successfully authenticated to get access to the TOE services Service_Elec_Signature, Service_Client_Server_Auth and Service_Key_Decryption.

11 **Service_Asym_Mut_Auth_w/o_SM**[1]: Mutual Authentication using asymmetric techniques between the SMC and a eHC or HPC without establishment of a trusted channel (cf. [20], Annex E).

This service is meant for situations, where the SMC requires authentication by a HPC to allow the use of the SMC authentication data and to perform the authentication to the eHC for access to protected data. 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. for details to [20], Annex E.2). This service uses the commands INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE with algorithmic identifier '1E'. The algorithmic identifier '1E' enforces the answer provided by the command INTERNAL AUTHENTICATE and the answer expected by the command EXTERNAL AUTHENTICATE to be signed by private key of the entity which authenticates themselves (cf. for details to [20], Annex E.2).

12 **Service_Asym_Mut_Auth_with_SM**: Mutual Authentication using asymmetric techniques between the SMC and a eHC or HPC with establishment of a trusted channel after successful authentication. The TOE supports secure messaging by means encryption of data, decryption of data, generation of MAC and verification of MAC.

This service is meant for situations, where the SMC and a HPC or another security module, which provides similar functionality, to establish a trusted channel by means of secure messaging, i.e. the communication is encrypted and/or secured by a MAC. 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. for details to [20], Annex E.3). This service uses the commands INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE with algorithmic identifier '1F'. The algorithmic identifier '1F' enforces the answer provided by the command INTERNAL AUTHENTICATE and the answer expected by the command EXTERNAL AUTHENTICATE to be signed by private key of the entity which authenticates themselves (cf. for details to [20], Annex E.3) and encrypted with the public key of the entity verifying the authentication attempt.

13 **Service_Sym_Mut_Auth_with_SM**: Mutual Authentication using symmetric techniques between the SMC and an external entity with establishment of a trusted channel with secure massaging.

This service is meant for situations, where the SMC communicates with an external entity, which shares symmetric keys agreed with the SMC by means of Service_Sym_Mut_Auth_with_SM and stored in the SMC for future use. The HPC uses of the protocol with the commands GET CHALLENGE and the command MUTUAL AUTHENTICATE to verify the authentication attempt of the security module and to authenticate themselves to an external entity (cf. for details to [20], Annex E.4). The successful authentication establish a communication channel protected by secure messaging but does not change the security status of the HPC for access control.

[1] The Abbreviation SM here stands for Secure Messaging, which is the card security protocol realising a trusted channel.

14 **Service_SM_Support**: The SMC provides (i) the encryption of plaintext and the decryption of cipher text with the secure messaging encryption key, (ii) the MAC generation and the MAC verification with the secure messaging MAC key and (iii) the production of secured commands with cryptographic checksum data objects and with cryptogram data objects and (iv) processing of secured responses where these keys are established by card-to-card authentication (cf. [20], sec. 6.6).

The SMC service intermediates between an application communication in plain text and a remote smart card (e.g. HPC) communicating by means of secure messaging or encryption or using MAC.

15 **Service_Elec_Signature**: The SMC implements a PKI application, which in particular makes it possible to use the TOE as an signature-creation device for advanced electronic signatures.

This application would be technically suitable for the creation of digital signature for qualified electronic signatures but the certificate of the SMC is not a qualified one and the application does not require user authentication (as wilful act) for each signature to be created (cf. for details to [22], sec. 7.5).

16 **Service_Client_Server_Auth**: The SMC implements a PKI application, which in particular allows to use the TOE as an authentication token for a client/server authentication (by means of an asymmetric method using X.509 certificates, cf. for details to [22], sec. 7.6). The card holder authenticates himself with his PIN in order to access this service.

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

17 **Service_Key_Decryption**: The SMC implements a PKI application, which in particular allows to use the TOE as a data decryption token. Symmetric document encipherment keys, which are themselves encrypted with the Card Holders Public Key can only be decrypted with the help of the card (cf. for details to [22], sec. 7.6). The card holder 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 card holders permission. So it can also be seen as a privacy feature.

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

Specification German Health Professional Card and Security Module Card - Pharmacist & Physician – Part 1: Commands, Algorithms and Functions of the COS Platform, Version 2.1, 07.11.2005, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychoterapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Deutsche Krankenhaus-Gesellschaft

German Health Professional Card and Security Module Card Specification - Pharmacist & Physician - Part 3: SMC Applications and Functions, Version 2.1 draft, 19.11.2005, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer,

Bundespsychoterapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Deutsche Krankenhaus-Gesellschaft

## 2.3 TOE life cycle

19 The following description is a short summary of the SMC life cycle model based on a common model normally used for smart cards. The TOE life cycle is described in terms of the seven life cycle phases as usually defined for smart cards, see for example the SSVG-PP [16]. They are summarized in the following table.

| Phase | | Description |
|---|---|---|
| 1 | **Smartcard Embedded Software Development** | The **Smartcard Embedded Software Developer** is in charge of<br>• the development of the Smartcard Embedded Software of the TOE,<br>• the development of the TOE related Applications<br>• the specification of the IC initialisation and pre-personalisation requirements (though the actual data for the IC initialisation and pre-personalisation come from Phase 4, 5 resp. 6).<br>The purpose of the Smartcard Embedded Software and Applications designed during phase 1 is to control and protect the TOE and its different configurations during phases 4 to 7 (product usage).The global security requirements of the TOE are such that it is mandatory during the development phase to anticipate the security threats of the other phases. |
| 2 | **IC Development** | The **IC Designer**<br>• designs the IC,<br>• develops the IC Dedicated Software,<br>• provides information, software or tools to the Smartcard Embedded Software Developer, and<br>• receives the Smartcard Embedded Software from the developer through trusted delivery and verification procedures.<br>From the IC design, IC Dedicated Software and Smartcard Embedded Software, the **IC Designer**<br>• constructs the smartcard IC database, necessary for the IC photomask fabrication. |
| 3 | **IC Manufacturing and Testing** | The **IC Manufacturer** is responsible for<br>• producing the IC through three main steps:<br>- IC manufacturing,<br>- IC testing, and<br>- IC pre-personalisation. |

| | | |
|---|---|---|
| | | The **IC Mask Manufacturer**<br>• generates the masks for the IC manufacturing based upon an output from the smartcard IC database. |
| **4** | **IC Packaging and Testing** | The **IC Packaging Manufacturer** is responsible for<br>• the IC packaging (production of modules) and<br>• testing. |
| **5** | **Smartcard Product Finishing Process** | The **Smartcard Product Manufacturer** is responsible for<br>• the initialisation of the TOE (in form of the initialisation of the modules of phase 4) and<br>• its testing.<br>The smartcard product finishing process comprises the embedding of the initialised modules for the TOE and the card production what may be done alternatively by the Smartcard Product Manufacturer or by his customer (e. g. Personaliser or Card Issuer)**.** |
| **6** | **Smartcard Personalisation** | The **Personaliser** is responsible for<br>• the smartcard personalisation and<br>• final tests.<br>The personalization of the smart card includes the printing of the (card holder specific) visual readable data onto the physical smart card, and the writing of (card holder specific) TOE User Data and TSF Data into the smart card. |
| **7** | **Smartcard End-usage** | The **Smartcard Issuer** is responsible for<br>• the smartcard product delivery to the smartcard end-user (the card holder), and the end of life process.<br>• The authorized personalization agent (Card Management System) are allowed to add data, modify or delete an SMC application.<br>• The TOE is used as SMC by the smart card holder in the Operational use phase |

Table 1: Smart Card Life Cycle Overview

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

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

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

- TOE operational use.

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

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

24 The data structures and the access rights to the health application data as defined in the SMC specification [20] are covered by the evaluation.

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

26 **Application note 1**: The following examples and remarks may help ST writers to define the boundary of TOE development.

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

   - Phase 5 completely belongs to the TOE development, i.e. the TOE is delivered as an IC already embedded in the plastic card and containing all software and at least the data structures as defined in the specification [22].

   - The TOE is delivered as an initialised module, i.e. it contains all software and at least the data structures as defined in the specification [22], but isn't embedded in a plastic card yet.

   - The TOE is delivered in (at least) two parts: The hardware as a module or already embedded in a plastic card on the one hand and a file containing parts of the initialisation data on the other hand. Both parts together again contain all software and at least the data structures as defined in the specification [22] (which in particular means that all of this is evaluated during ADV activities). In this case the evaluation must also show as a result that the functions used by the customer (Card Management System / card issuer) for loading the initialisation data into the hardware provide sufficient protection against modification and (where applicable) disclosure of these data.

b. The following remarks may show how some CC assurance activities apply to parts of the life cycle[2]:

[2] These activities already follow from the CC definitions. Therefore it is not necessary to define them as refinements to the CC assurance components. However these explicit notes may serve as a help for ST

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

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

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

- The guidance documentation delivered by the TOE developer as part of the TOE delivery procedures are covered by AGD and ADO_IGS. Since the Card Management System / card issuer is the first "user" of the TOE after delivery, the guidance documentation is mainly directed to him. He may be defined as the administrator of the TOE or as a special user role. Since the guidance documentation in particular needs to describe all measures necessary for secure use of the TOE, it needs to contain information on the following issues:

  - Secure handling of the personalisation of the TOE

  - Secure handling of delivery of the personalised TOE from the Card Management System / card issuer to the card holder.

  - Security measures for end-usage, which the Card Management System / card issuer needs to communicate to the card holder. A simple example for this may be the requirement for the card holder, to handle his PIN(s) securely. Since the documents accompanying the card during transport from card issuer to card holder will probably not be available at the time of evaluation, the guidance documents for the Card Management System / card issuer need to contain this information connected with the requirement that the card issuer covers all such issues in his delivery documents.

# 3 Security Problem Definition

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

- **assets**, which the TOE shall protect,

---

writers and TOE developers to understand the connection between the life cycle model and some CC requirements.

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

## 3.1 Introduction

**Assets**

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

| Name of asset[3] | Description |
|---|---|
| Card Verifiable Authentication Certificate of the Card Management System (CVC.SMC_ADMIN.AUT) | The Card Verifiable Authentication Certificate of the Card Management System CVC.SMC_ADMIN.AUT is used authenticate the Card Management System as part of the PKI HP-ADMIN and to authorize for administration of the TOE especially for creation of new application. This data may be stored in the MF of the TOE as user data provided for the convenience of the IT environment. If this data is provided by the IT environment it shall be verified by means of PuK. HP_AD-MIN.CS. |
| Root Public Key of the Certificate Service Provider (PuK.RCA_HC.CS) | The root public key PuK.RCA_HC.CS for verification of the card verifiable certificate of the certificate service provide for card verifiable certificates in the health care environment. It is part of the TSF data which integrity shall be protected. |
| Certificate Service Provider self-signed Certificate (CVC.CA_SMC.CS) | The certificate of the Certificate Service Provider for card verifiable certificates in the health care environment CVC.CA_SMC.CS containing the public key PuK.CA_SMC.CS for verification of the card verifiable certificates like CVC.SMC.AUT. It is part of the user data provided for the convenience of the IT environment. |
| Public Key of the Certificate Service Provider | The public key of the Certificate Service Provider for card verifiable certificates in the health care environment |

[3] Note the names of the keys and certificates are not consolidated between [0], [0] and [0] yet.

| Name of asset[3] | Description |
|---|---|
| (PuK.CA_SMC.CS) | PuK.CA_SMC.CS used for verification of the card verifiable certificate CVC.HPC.AUT and CVC.eHC.AUT. It is part of the TSF data which integrity shall be protected. |
| Card Authentication Private Keys (PrK.SMC.AUT) | The Card Authentication Private Key PrK.SMC.AUT are asymmetric cryptographic key used for the authentication of a SMC to a eHC or a HPC on behalf of the card holder. It is part of the user data. |
| Card Verifiable Authentication Certificates (CVC.SMC.AUT) | Card verifiable certificate CVC.SMC.AUT for the Card Authentication Public Keys PuK.SMC.AUT as authentication reference data corresponding to the Authentication Private Key PrK.SMC.AUT and used for the card-to-card authentication of the SMC to the eHC and to the HPC **without** establishing a trusted channel by means of secure messaging.. It contains encoded access rights (Role ID) and is signed by the SMC card issuer. It is part of the user data provided for use by external entities as authentication reference data of the HPC. It is stored in the file EF.CVC.SMC.AUT which integrity shall be protected. |
| Card Verifiable Authentication Certificates (CVC.SMC.TCE) | Card verifiable certificate CVC.SMC.TCE for the Card Authentication Public Keys PuK.SMC.AUT as authentication reference data corresponding to the Authentication Private Key PrK.SMC.AUT and used for the card-to-card authentication of the SMC to the eHC and to the HPC **with** establishing a trusted channel by means of secure messaging.. It contains encoded access rights (Role ID) and is signed by the SMC card issuer. It is part of the user data provided for use by external entities as authentication reference data of the HPC. It is stored in the file EF.CVC.SMC.TCE which integrity shall be protected. |
| Client-Server Authentication Private Key (PrK.HCI.AUT) | The Client-Server Authentication Private Key PrK.HCI.AUT is a asymmetric cryptographic key used for the authentication of a client application acting on behalf of the card holder to a server. It is part of the user data. |
| Client-Server Authentication Certificate (C.HCI.AUT) | X.509 Certificate C.HCI.AUT for the Client-Server Authentication Public Key corresponding to the Client-Server Authentication Private Key (cf. to [22], sec. 5.2, for details). It is part of the user data provided for use by external entities as authentication reference data of the SMC. |
| Decipher Private Key (PrK.HCI.ENC) | The Document Cipher Key Decipher Key PrK.HCI.ENC is asymmetric private key used for document decryption on behalf of the card holder. It is part of the user data. |

| Name of asset[3] | Description |
|---|---|
| Encryption Certificate (C.HP.ENC) | X.509 Certificate C.HCI.ENC for the Document Cipher Key Encipher Public Key PuK.HCI.ENC corresponding to the Document Cipher Key Decipher Key PrK.HCI.ENC (cf. to [22], sec. 5.2, for details). It is part of the user data provided for use by external entities. |
| Advanced Electronic Signature Private Key (PrK.HCI.ASIG) | Private key PrK.HCI.ES used for digital signature-creation. It is part of the user data and needs protection in confidentiality and integrity. |
| Advanced Electronic Signature Public Key Certificates (C.HCI.ASIG) | The certificate C.HCI.ASIG of the Digital Signature Public Key PuK.HCI.ASIG corresponding to the Digital Signature Private Key PrK.HCI.ASIG used for the verification of the advanced electronic signatures of the health institution. They are part of the user data provided for external entities. |
| TOE initialization data | Data stored in the TOE during the initialization process. It is part of the TSF data. |
| TOE personalization data | Data stored in the TOE during personalization process. It contains user data and TSF data. |
| User Authentication Reference Data (PIN.SMC, PUC.SMC, PIN.ASIG, PUC.ASIG) | The User Authentication Reference Data are used to verify the card holder attempt to activate certain functions of the TOE. This data include the PIN PIN.SMC and the reset retry counter PUC.SMC, which are in particular not used for advanced electronic signatures. The PIN PIN.ASIG and the reset retry counter PUC.ASIG are used for advanced electronic signatures only. They are part of the TSF data. |

Table 2: Assets of the HPC

29 **Application note 2:** The User Authentication Reference Data (PIN.SMC, PUC.SMC, PIN.ASIG, PUC.ASIG) and the Public Key for CV Certification Verification (PuK.CSP.CS-CV) are used as authentication reference by TSF for human user and card authentication. The Card Authentication Private Keys (PrK.SMC.AUT), the Client-Server Authentication Private Key (PrK.HCI.AUT), the Document Cipher Key Decipher Key (PrK.HI.KE) and the Digital Signature Private Key (PrK.HCI.ES) are used as cryptographic keys by the TOE security services provided to the user. Therefore they are assed as user data.

**Subjects**

30 This protection profile considers the following subjects:

| Name of subject | Description |
|---|---|
| Card Management System | Person(s) responsible for the personalization of the TOE for the Card Holder and for the Card Application Management System (CAMS). |
| Card Holder | Person for whom the SMC is personalized and which controls the use of the SMS. He or she knows rightfully the user authentication data (PIN and PUC). |
| Health Professional Card | The Health Professional Card (HPC) authenticating themselves to the SMC by means of card-2-card authentication with a card verifiable certificate with corresponding card holder authorisation defining its access rights. |
| Terminal | External entity communicating with the TOE without successful authentication by sending commands to the TOE and receiving responses from the TOE according to ISO/IEC 7816 . |
| Unauthorized subject | All subjects who is trying to interact with the TOE as Card Management System, Card Holder or HPC without being authenticated for this role. |

Table 3: Subjects

31 **Application note 3:** The smart cards in the health care environment possess card verifiable certificate (CVC) with card holder authorizations (CHA) identifying them as HPC, eHC and SMC as defined in [22], Annex F. The CHA role identifier (ID) is coded in 1 byte were

- the first nibble (i.e. 4 higher value bits) the area of the health care environment like “Arzt” (physician) or “Apotheker” (pharmacist),
- the second nibble (i.e. 4 lower value bits) the component type: ‘0’ for eHC, ‘1’ for a card management system, ‘A’ for HPC of a health professional, ‘B’ for a HPC of Medical or Pharmaceutical assistant, ‘C’ for a SMC of a health institution, ‘D’ for a SMC in a self service terminal.

“Related CHA” are CHA with the same first nibble, i.e. these smart cards are used in the same health care area. E.g. CHA ‘1A’ “Arzt” (physician) relates to ‘1C’ “Arztpraxis oder Krankenhaus” (medical practice or hospital), but ‘1A’ does not relate to ‘3C’ “Apotheke” (pharmacy).

## 3.2 Organisational Security Policies

32 OSPs will be defined in the following form:

**OSP.name Short Title**

Description.

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

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

The SMC shall be implemented according to the specifications:

Specification German Health Professional Card and Security Module Card - Pharmacist & Physician – Part 1: Commands, Algorithms and Functions of the COS Platform, Version 2.1, 07.11.2005, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychoterapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Deutsche Krankenhaus-Gesellschaft

German Health Professional Card and Security Module Card Specification - Pharmacist & Physician - Part 3: SMC Applications and Functions, Version 2.1 draft, 19.11.2005, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychoterapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Deutsche Krankenhaus-Gesellschaft

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

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

## 3.3 Threats

36 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.

37 Threats will be defined in the following form:

**T.name Short Title**

Description.

### 3.3.1 Threats mainly addressing TOE_ES and TOE_APP

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

39 **T.Compromise_Internal_Data Compromise of confidential User or TSF data**

An attacker with high attack potential try 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).

40 **T.Forge_Internal_Data Forge of User or TSF data**

An attacker with high attack potential try 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.

41 **T.Misuse Misuse of TOE functions**

An attacker with high attack potential try 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 circumvent the user authentication to use the DECIPHER command for document keys without authorization or to sign data with an digital signature as advanced electronic signature. The attacker may try alter the TSF data e.g. to extend the user rights after successful card-to-card authentication.

42 **T.Intercept Interception of Communication**

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

This threat comprises several attack scenarios. The Health Professional using the TOE reads from and writes onto eHC patients data like medication or medical data which an attacker may read or forge during transmission. Attacker may read the document keys output by the TOE as DECIPHER command response.

### 3.3.2 Threats mainly addressing TOE_IC and TOE_ES

43 **T.Abuse-Func Abuse of Functionality**

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

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

44 **T.Information_Leakage Information Leakage from smart card**

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

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

45 **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.

46 **T.Phys-Tamper Physical Tampering**

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

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

## 3.4 Assumptions

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

48 The assumptions will be defined in the following form:

**A.name Short Title**

Description.

49 **A.Pers_Agent Personalization and management of the smart card**

The Card Management System performs the personalisation and additional management steps correctly during the end-usage phase according to the specifications [20] [22]and ensures the correctness, the quality and - if necessary - the confidentiality of all data structures and data on the card.

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

The card holder of the TOE uses the TOE adequately. In particular he doesn't tell the PIN (or PINs) of the eHC to others and doesn't hand the card to unauthorised persons. The Card Management System and the health professionals use their data systems according to the overall system security requirements.

# 4 Security Objectives

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

### 4.1.1 Security Objectives for the TOE

52 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.

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

**OT.name short title**

Description of the objective.

54 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).

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

The TOE must ensure that the User data and the TSF data can be created, written and updated by authorized Card Management system only except the card holder authentication reference data managed by the card holder.

56 **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, and other confidential user data and TSF data under the TSF scope of control.

57 **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 CV Certification Verification, the Card Verifiable Authentication Certificates, the Certificate Service Provider self-signed Certificate, and other user data and TSF data under the TSF scope of control.

58 **OT.Trusted_Channel Trusted Channel**

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

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

The TOE provides the TOE security services Service_User_Auth_PIN, Service_Asym_Mut_Auth_w/o_SM, Service_Asym_Mut_Auth_with_SM Service_Sym_Mut_Auth_with_SM, Service_Client_Server_Auth and Service_Key_Decryption, the Service_SM_Support and the Service_Elec_Signature. The TOE shall provide the services the. Service_Asym_Mut_Auth_w/o_SM, Service_Client_Server_Auth, Service_Key_Decryption and the Service_Elec_Signature to the card holder only.

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

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

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

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

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

62 **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.

63 **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.

64 **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 (refer to the objective OT.Phys-Manipulation) provided that detailed knowledge about the TOE´s internals.

65 **OT.Prot_Phys-Tamper Protection against physical tampering**

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

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

with a prior

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

66 **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. This is addressed by the security objective OD.Assurance.

### 4.1.2 Security Objectives for the Development and Manufacturing Environment

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

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

**OD.name short title**

Description of the objective.

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

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

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

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

### 4.1.3 Security Objectives for the Operational Environment

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

**OE.name short title**

Description of the objective.

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

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

All data structures and data on the card produced during personalisation or additional administration steps during the end-usage phase must be performed correctly according to the specifications [20] [22] and are handled correctly regarding integrity and confidentiality of these data. The Card management system ensure (i) the generation of the card-to-card authentication keys stored on smart card and the distribution of the corresponding public key in form of CV certificates including the access rights of the card holder, (ii) writing the public key for verification of CV certificates for card-to-card authentication, (iii) the generation of the client-server authentication keys stored on smart card and the distribution of the corresponding public key in form of X.509 certificates by an public key infrastructure, (iv) 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. This includes in particular sufficient cryptographic quality of cryptographic keys (in accordance with the cryptographic algorithms specified for the SMC) and their confidential handling.

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

The card holder of the TOE needs to use the TOE adequately. In particular he must not tell the PIN (or PINs) of the SMC to others and must not hand the card to unauthorised persons. The Card Management System and the health professionals must use their data systems according to the overall system security requirements.

# 5 Extended Components Definition

75 This protection profile uses components defined as extensions to CC part 2. Some of these components are defined in [16], other components are defined in this protection profile.

## 5.1 Definition of the Family FCS_RND

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

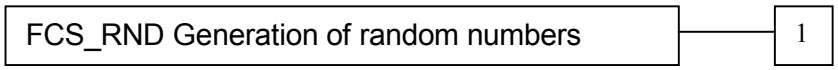
77 The family “Generation of random numbers (FCS_RND)” is specified as follows.

**FCS_RND Generation of random numbers**

Family behaviour

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

Component levelling:




FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management : FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

Dependencies: No dependencies.

## 5.2 Definition of the Family FMT_LIM

78 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.

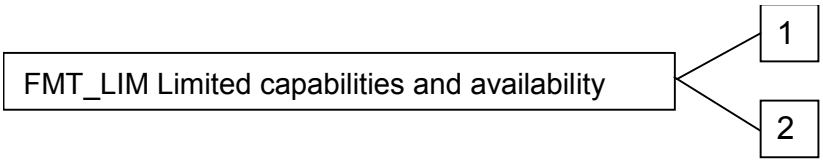
79 The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

**FMT_LIM Limited capabilities and availability**

Family behaviour

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

Component levelling:




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

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

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

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

**FMT_LIM.1 Limited capabilities**

Hierarchical to: No other components.

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

Dependencies: FMT_LIM.2 Limited availability.

81 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.

82 Application note 7: 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.

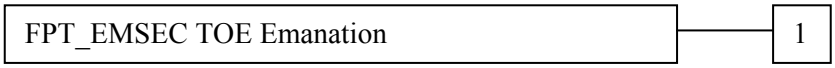
## 5.3 Definition of the Family FPT_EMSEC

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

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:




FPT_EMSEC.1 TOE emanation has two constituents:

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

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

**FPT_EMSEC.1 TOE Emanation**

Hierarchical to: No other components.

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

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

Dependencies: No dependencies.

# 6 Security Requirements

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

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

86 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicized*.

87 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicized*.

88 The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

## 6.1 Security Functional Requirements for the TOE

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

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

| Security Service | SFR | Comment |
|---|---|---|
| Human user authentication | FIA_AFL.1, FIA_ATD.1, FIA_UID.1, FIA_UAU.1, | Human user authentication is performed by means of the |

| Security Service | SFR | Comment |
|---|---|---|
| | FMT_MTD.1/PIN, FMT_MTD.1/RAD_WR | authentication reference data PIN and PUC |
| Card-to-card authentication | FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_RND.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FMT_MTD.1/RAD_WR, FMT_MTD.1/RAD_MOD | Card-to-card authentication according to [20], Annex E,<br>- verification of digital signatures of certificates according to ISO 9796-2 (without random numbers)<br>- RSA with private key for INTERNAL AUTHEN-TICATE and RSA with public key for EXTERNAL AUTHEN-TICATE with DSI according [20], Annex E |
| Authorization of SMC for access to data on eHC | FDP_ACC.1, FDP_ACF.1, FIA_UAU.4 | Access control for the certificate with special encoded access rights to open the eHC |
| Client-server authentication | FCS_COP.1/CSA | Digital signature-creation according to PKCS#1, EMSA-PKCS1-v1_5 [15] |
| Secure messaging | FCS_CKM.1, FCS_CKM.4, FCS_RND.1, FCS_COP.1/SM_ENC, FCS_COP.1/SM_MAC, FDP_UCT.1, FDP_UIT.1 | Secure messaging key generation is described in [20], Annex E and secure messaging encryption and MAC is described in [20], Annex C. |
| Document key decipherment | FCS_COP.1/RSA_DEC | Decryption of document keys according to PKCS#1, version 2.0, and ISO/IEC 7816-4, cf. [20], 9.7 and Annex E.3 for details |
| Creation of digital signatures | FCS_COP.1/SHA, FCS_COP.1/SIGN_AS, FDP_ACC.1, FDP_ACF.1, | For the cryptographic algorithms cf. to [6] |

Table 4: Overview of SFR used to describe the TOE security services

### 6.1.1 Cryptographic support (FCS)

#### 6.1.1.1 Cryptographic key generation (FCS_CKM.1)

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

92 **FCS_CKM.1/ASYM Cryptographic key generation - Asymmetric card-to-card authentication with key agreement**

Hierarchical to: No other components.

FCS_CKM.1.1/ASYM: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm asymmetric card-to-card authentication with key agreement [4] and specified cryptographic key sizes 112 bit [5] that meet the following: [20], Annex E [6].

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

93 **FCS_CKM.1/SYM Cryptographic key generation - Symmetric card-to-card authentication with key agreement**

Hierarchical to: No other components.

FCS_CKM.1.1/SYM: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm symmetric card-to-card authentication with key agreement [7] and specified cryptographic key sizes 112 bit [8] that meet the following: [20], Annex E [9].

---

4 [*assignment: cryptographic key generation algorithm*]

5 [*assignment: cryptographic key sizes*]

6 [assignment: *list of standards*]

7 [*assignment: cryptographic key generation algorithm*]

8 [*assignment: cryptographic key sizes*]

9 [assignment: *list of standards*]

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

94 **Application note 9:** The [20], Annex E, describes 2 card-to-card authentication protocols to generate the Triple-DES encryption key (SMK.ENC) and the Retail-MAC message authentication keys (SMK.MAC) for secure messaging as described in [20], Annex D. The **asymmetric** card-to-card authentication with key agreement [20], Annex E2, is used for **Service_Asym_Mut_Auth_with_SM**. The TOE is equipped with its Card Authentication Private Key PrK.HPC.AUT and has received and verified the Card Authentication Public Key of the communication partner. In this case SMK.ENC and SMK.MAC are different. The **symmetric** card-to-card authentication with key agreement [20], Annex E2, is used for **Service_Sym_Mut_Auth_with_SM**. The TOE is equipped with a symmetric secret key SK.HPC.AUT and agrees one secure message key which is used for encryption and message authentication, i.e. SMK.ENC = SMK.MAC. The algorithms use the random number RND.HPC generated by TSF as required by FCS_RND.1.

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

96 **FCS_CKM.4 Cryptographic key destruction**

Hierarchical to: No other components.

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

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

97 **Application note 10:** The TOE shall destroy the Triple-DES encryption key (SMK.ENC) and the Retail-MAC message authentication keys (SMK.MAC) for secure messaging after reset or termination of secure messaging session or reaching fail secure state according to FPT_FLS.1.

#### 6.1.1.2 Cryptographic operation (FCS_COP.1)

98 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.

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

Hierarchical to: No other components.

| | |
|---|---|
| FCS_COP.1.1/ SHA | The TSF shall perform hashing [10] in accordance with a specified cryptographic algorithm SHA-1 and SHA-2 (256 bit) [11] and cryptographic key sizes none [12] that meet the following: FIPS 180-2 [13]. |

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

100 **Application note 11:** This SFR requires the TOE to implement the hash functions SHA-1 (160 bit hash value) and SHA-2 (256 bit hash value) [20], sec. 4, table 6a, for the cryptographic primitive of the authentication mechanism according to [20], Annex E. The SMC uses SHA-1 for creation of digital signatures, cf. [20], Annex E. The SHA-1 has a security level of 80 bit which may be not sufficient to resist high attack potential for the expected operational time frame.

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

Hierarchical to: No other components.

| | |
|---|---|
| FCS_COP.1.1/ CCA_SIGN | The TSF shall perform digital signature-creation [14] in accordance with a specified cryptographic algorithm RSA [15] and cryptographic key sizes 1024 bit module length [16] that meet the following: [20], Annex E [17]. |

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

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

102 **Application note 12:** This SFR requires the TOE to implement the RSA for the cryptographic primitive of the digital signature-creation for the card-to-card authentication mechanism (i.e. INTERNAL AUTHENTICATE, algorithm identifier '1E' and '1F') according to [20], Annex E. This annex specifies RSA module length of 1024 bit which may be not sufficient to resist high attack potential for the expected operational time frame (cf. e.g. to [6]). The RSA module length of 1280 bit is announced for future specification in [20], chapter 11). The ST should extend the operation of the key length in FCS_COP.1/CCA_SIGN.1.1 if the TOE supports RSA module length more than 1024 bit as well.

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

Hierarchical to: No other components.

FCS_COP.1.1/CCA_VERIF: The TSF shall perform digital signature-verification [18] in accordance with a specified cryptographic algorithm RSA [19] and cryptographic key sizes 1024 bit module length[20] that meet the following: [20], Annex E [21].

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

104 **Application note 13:** This SFR requires the TOE to implement the RSA for the cryptographic primitive of the digital signature-verification for the card-to-card authentication mechanism (i.e. INTERNAL AUTHENTICATE, algorithm identifier '1E' and '1F') according to [20], Annex E. This annex specifies RSA module length of 1024 bit which may be not sufficient to resist high attack potential for the expected operational time frame (cf. e.g. to [6]). The RSA module length of 1280 bit is announced for future specification in [20], chapter 11). The ST should extend the operation of the key length in FCS_COP.1/CCA_VERIF.1.1 if the TOE supports RSA module length more than 1024 bit as well.

---

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

[19] [assignment: *cryptographic algorithm*]

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

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

105 **FCS_COP.1/CSA Cryptographic operation – Digital Signature-Creation for Client-Server Authentication**

Hierarchical to: No other components.

| | |
|---|---|
| FCS_COP.1.1/ CSA | The TSF shall perform digital signature-creation [22] in accordance with a specified cryptographic algorithm RSA [23] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: PKCS#1, EMSA-PKCS1-v1_5 [15] [24]. |

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

106 **Application note 14:** This SFR requires the TOE to implement the RSA for the cryptographic primitive of the digital signature-creation for the client-server authentication mechanism according to [22], sec. 7.6. The [20], , chapter 11, does not specify the RSA module length for the digital signature-creation for the client-server authentication mechanism. Therefore the ST writer shall perform the missing operation in FCS_COP.1/CSA.

107 **FCS_COP.1/RSA_DEC Cryptographic operation – RSA Decryption**

Hierarchical to: No other components.

| | |
|---|---|
| FCS_COP.1.1/ RSA_DEC | The TSF shall perform decryption [25] in accordance with a specified cryptographic algorithm RSA [26] and cryptographic key sizes 1024 bit module length[27] that meet the following: PKCS#1, RSAES-PKCS1-v1_5 [15] [28]. |

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

[23] [assignment: *cryptographic algorithm*]

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

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

[26] [assignment: *cryptographic algorithm*]

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

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

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

108 **Application note 15:** This SFR requires the TOE to implement the RSA for the cryptographic primitive of the RSA decryption to [20], sec. 11 and [22], sec. 7.6. Note that 1024 bit RSA module (cf. [20], sec. 11) has a security level of 80 bit only which may be not sufficient to resist high attack potential for the expected operational time frame.

109 **FCS_COP.1/TDES Cryptographic operation – TDES Encryption / Decryption**

Hierarchical to: No other components.

FCS_COP.1.1/ TDES: The TSF shall perform encryption and decryption [29] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode [30] and cryptographic key sizes 112 bit [31] that meet the following: FIPS 46-3 [8] and [20], Annex G [32].

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

110 **Application note 16:** This SFR requires the TOE to implement the cryptographic primitive for secure messaging in with encryption of the transmitted data and for the Service_SM_Support. The key is agreed between the TSF according to the FIA_UAU.4. The key size of 112 bit is chosen to resist attacks with high attack potential.

111 **FCS_COP.1/MAC Cryptographic operation – Retail MAC**

Hierarchical to: No other components.

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

[30] [assignment: *cryptographic algorithm*]

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

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

| | |
|---|---|
| FCS_COP.1.1/ MAC | The TSF shall perform generation and verification of message authentication code [33] in accordance with a specified cryptographic algorithm Retail MAC [34] and cryptographic key sizes 112 bit [35] that meet the following: ANSI X9.19 with DES and [20], Annex G [36]. |

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

112 **Application note 17:** 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_SM_Support. The key is agreed or defined as the key for secure messaging encryption. The key size of 112 bit is chosen to resist attacks with high attack potential.

113 **FCS_COP.1/SIGN_AS Cryptographic operation – Digital Signature-Creation for Advanced Electronic Signatures**

Hierarchical to: No other components.

| | |
|---|---|
| FCS_COP.1.1/ SIGN_AS | The TSF shall perform digital signature-creation [37] in accordance with a specified cryptographic algorithm RSA [38] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. |

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

114 **Application note 18:** This SFR requires the TOE to implement the RSA for the cryptographic primitive for SMC the creation of advanced electronic signature. The advanced electronic signature-creation function provided by the SMC shall have a high strength which result in (i)

---

33 [assignment: *list of cryptographic operations*]

34 [assignment: *cryptographic algorithm*]

35 [assignment: *cryptographic key sizes*]

36 [assignment: *list of standards*]

37 [assignment: *list of cryptographic operations*]

38 [assignment: *cryptographic algorithm*]

the minimum key size of 2048 bit and (ii) support of ISO/IEC 9796-1 with random numbers or PKCS#1 as recommended in [6].

#### 6.1.1.3 Random Number Generation (FCS_RND.1)

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

116 **FCS_RND.1 Quality metric for random numbers**

Hierarchical to: No other components.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

Dependencies: No dependencies.

117 **Application note 19:** This SFR requires the TOE to generate random numbers used for (i) the authentication protocols as required by FIA_UAU.4, and (ii) the key agreement FCS_CKM.1 for secure messaging. The quality metric shall be chosen to ensure the strength of function high.

### 6.1.2 Identification and Authentication

#### 6.1.2.1 Authentication failure handling (FIA_AFL.1)

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

119 **FIA_AFL.1 Authentication failure handling**

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*], "*an administrator configurable positive integer within* [assignment*: range of acceptable values*]*"*] unsuccessful authentication attempts occur related to consecutive failed human user authentication with the PIN [39].

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall block the PIN for authentication until successful unblock with resetting code for this PIN [40].

Dependencies: FIA_UAU.1 Timing of authentication.

120 **Application note 20:** The component FIA_AFL.1/PIN address the human user authentication by means of the PIN.SMC for the health care application and of the PIN.ASIG for digital signature generation with signature key PrK.HCI.ASIG in DF.ASIG. The reference data for the PIN.SMC is stored EF.PIN under MF [22], sec. 7.3.2, and the PIN.ASIG is stored EF.PIN in DF.ASIG [22], sec. 7.5,. The security target writer shall select the parameters with respect to the high strength of the authentication function, e.g. in case of 3 authentication attempts the PIN shall have at least 6 digits. The specification [20], sec. 4, describes the VERIFY command to authenticate with the PIN, the CHANGE REREENCE DATA command to change a unblocked PIN and the RESET RETRY COUNTER command to unblock and optionally change the PIN.

#### 6.1.2.2 User attribute definition (FIA_ATD.1)

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

122 **FIA_ATD.1 User attribute definition**

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: identity and role [41].

Dependencies: No dependencies.

123 **Application note 21:** The component FIA_ATD.1 applies to (i) the human user authentication, i.e. the card holder, 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. [20] Annex B for details).

#### 6.1.2.3 Timing of identification (FIA_UID.1)

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

125 **FIA_UID.1 Timing of identification**

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

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

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow

(1) reading the ATR

(2) reading data with access condition ALWAYS,

(3) [assignment: *list of TSF-mediate actions*] [42]

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

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

Dependencies: No dependencies.

126 **Application note 22:** The ST writer shall perform 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 Card Verifiable Authentication Certificates and the X.509 Certificates. The card management system may create DF and EF in MF and DF ,and define their access conditions.

#### 6.1.2.4 Timing of authentication (FIA_UAU.1)

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

128 **FIA_UAU.1 Timing of authentication**

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow

(1) reading the ATR

(2) reading data with access condition ALWAYS,

(3) identification by providing the users certificate,

(4) execution of the command INTERNAL AUTHENTICATE with PrK.SMC.AUT, algorithm '1F' in SE#2,

(5) [assignment: *list of TSF mediated actions*] **[43]**

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.

---

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

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

Dependencies: FIA_UID.1 Timing of identification.

129 **Application note 23:** The ST writer shall perform 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.

#### 6.1.2.5 Single-use authentication mechanisms (FIA_UAU.4)

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

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

Hierarchical to: No other components.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

(1) execution of the command EXTERNAL AUTHENTICATE as part of the Service_Asym_Mut_Auth_w/o_SM with PrK.HPC.AUT in SE#1,

(2) execution of the command EXTERNAL AUTHENTICATE as part of the Service_Asym_Mut_Auth_with_SM with PrK.HPC.AUT in SE#2,

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

(4) execution of the command EXTERNAL AUTHENTICATE [44].

Dependencies: No dependencies.

132 **Application note 24:** The command EXTERNAL AUTHENTICATE may be used as part of the mutual card-to-card authentication mechanisms Service_Asym_Mut_Auth_w/o_SM, Service_Asym_Mut_Auth_with_SM and Service_Sym_Mut_Auth_with_SM or independent on mutual authentication. It uses the fresh generated by the TOE random data RND.ICC (see also FCS_RND.1) as challenge to prevent reuse of a response generated in a successful authentication attempt.

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

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

134 **FIA_UAU.6 Re-authenticating**

Hierarchical to: No other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions successful established secure messaging [45].

Dependencies: No dependencies.

135 **Application note 25:** The specification [20] states in Annex C.2: "After an authentication procedure is completed and a trusted channel is established, all commands and responses shall be transferred in the SM mode. If session keys are established for a certain logical channel and the card receives a command without SM for this logical channel, then the session keys for that logical channel are no longer available. Furthermore, the security status with respect to the authentication procedure with SM key transport/agreement shall no longer usable." The re-authentication of the external entity is necessary for each received command and is successful if the received command contains a valid MAC. If the re-authentication fails the security state gained by the card-to card authentication establishing the secure messaging shall be reset.

### 6.1.3 Access Control

#### 6.1.3.1 Complete Access Control (FDP_ACC.2)

136 The following Security Function Policy (SFP) **SMC Access Control SFP** is defined for the requirements "Complete Access Control (FDP_ACC.2)", "Security attribute based access control (FDP_ACF.1)", "Basic data exchange confidentiality (FDP_UCT.1)" and "Basic data exchange confidentiality (FDP_UCT.1)".

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

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

138 **FDP_ACC.2 Complete Access Control**

Hierarchical to: No other components.

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

FDP_ACC.2.1 The TSF shall enforce the SMC Access Control SFP [46] on

1. the subjects
   (a) the Card Management System,
   (b) the Card Holder,
   (c) the HPC,
   (d) the Terminal and
2. the objects
   (a) Master File (MF), Dedicated Files (DF) and Elementary Files (EF),
   (b) Card Authentication Private Keys (PrK.SMC.AUT),
   (c) Client-Server Authentication Private Key (PrK.HCI.AUT),
   (d) Decipher Private Key (PrK.HCI.ENC),
   (e) Advanced Electronic Signature Private Key (PrK.HCI.ASIG),
   (f) Global Data Object (EF.GDO),
   (g) SMC related Data (EF.SMC),
   (h) Card Verifiable Certificates (CVC.SMC.AUT, CVC.SMC.TCE, CVC.CA_SMC.CS),
   (i) X.509 certificates (C.HCI.AUT, C.HCI.ENC, C.HCI.ASIG) [47]

   and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

139 **Application note 26:** The subjects and objects are described in section 3.1 Introduction. The User Authentication Reference Data (PIN.CH and PUC.CH, PIN.ASIG and PUC.ASIG) and the public key for CV certificate verification (PuK.CA_SMC.CS, PuK.CA_SMC.CS) are TSF data.

### 6.1.3.2 Security attribute based access control (FDP_ACF.1)

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

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

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

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

Hierarchical to: No other components.

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

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

1. The Card Management System is allowed
   (a) to load applications and to create Dedicated Files (DF) and Elementary Files (EF) in the Master File (MF) or Dedicated Files (DF),
   (b) to create and to write the Global Data Object (EF.GDO),
   (c) to create the SMC related Data (EF.SMC),
   (d) to create and to write Card Authentication Private Keys (PrK.SMC.AUT),
   (e) to create and to write Client-Server Authentication Private Key (Pr.HCI.AUT),
   (f) to create and to write Decipher Private Key (PrK.HCI.ENC),
   (g) to create and to write Advanced Electronic Signature Private Key (PrK.HCI.ES),
   (h) to create, to write and to read Card Verifiable Certificates (CVC.SMC.AUT, CVC.SMC.TCE, CVC.CA_SMC.CS),
   (i) to create, to write and to read X.509 certificates (C.HCI.AUT, C.HCI.ENC, C.HCI.ASIG);
2. the Card Holder is allowed
   (a) to read the SMC related Data (EF.SMC),
   (b) to read the Card Verifiable Certificate (CVC.SMC.AUT, CVC.SMC.TCE, CVC.CA_SMC.CS),
   (c) to read the X.509 certificates (C.HCI.AUT, C.HCI.ENC, C.HCI.ASIG)
   (d) to execute the Service_Asym_Mut_Auth_w/o_SM using PrK.SMC.AUT,
   (e) to execute the Service_Asym_Mut_Auth_with_SM using PrK.SMC.AUT,
   (f) to execute the document key decipherment Service_Data_Decryption using PrK.HCI.ENC

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

[49] [assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes*, *or named groups of SFP-relevant security attributes*]

(g) to execute the client-server authentication Service_Client_Server_Auth using PrK.HCI.AUT,

(h) to execute the document signing Service_Elec_Signature using PrK.HCI.ES;

3. the Terminal is allowed

(a) to read the SMC related Data (EF.SMC),

(b) to read the Card Verifiable Authentication Certificates (CVC.SMC.AUT, CVC.SMC.TCE, CVC.CA_SMC.CS),

(c) to read the X.509 certificates (C.HCI.AUT, C.HCI.ENC, C.HCI.ASIG),

(d) to execute the service_SM_Support with secure messaging keys generated by means of the Service_Asym_Mut_Auth_with_SM using PrK.SMC.AUT,

(e) to execute the card-to-card authentication Service_Sym_Mut_Auth_with_SM,

(f) to execute the service_SM_Support with secure messaging keys,

(g) to execute the card-2-card authentication of the Service_Asym_Mut_Auth_w/o_SM to authenticate themselves as corresponding HPC;

4. a related HPC is allowed

(a) to execute the card-2-card authentication of the Service_Asym_Mut_Auth_w/o_SM to authenticate the SMC using the CVC.SMC.AUT and PrK.SMC.AUT to a corresponding eHC

(b) to update CMS related Data (EF.SMC) [50].

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rule:

1. the Card Management System is not allowed

(a) to execute the card-to-card authentication Service_Asym_Mut_Auth_w/o_SM with Pr.SMC.AUT,

(b) to execute the document signing Service_Elec_Signature using PrK.HCI.ES,

(c) to execute the document key decipherment

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

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

Service_Data_Decryption with PrK.HCI.ENC and

(d) to execute the client-server authentication Service_Client_Server_Auth with PrK.HCI.AUT

2. the terminal is not allowed

(a) to execute the card-to-card authentication Service_Asym_Mut_Auth_w/o_SM with PrK.SMC.AUT,

(b) to execute the document key decipherment Service_Data_Decryption with PrK.HCI.ENC,

(c) to execute the client-server authentication Service_Client_Server_Auth with PrK.HCI.AUT,

(d) to execute the document signing Service_Elec_Signature using PrK.HCI.ES,

3. no subject is allowed

(a) to read any private PrK.SMC.AUT, PrK.HCI.ES, PrK.HCI.AUT, and PrK.HCI.ENC,

(b) to update Global Data Object (EF.GDO),

(c) to update the Card Verifiable Authentication Certificates (CVC.SMC.AUT, CVC.SMC.TCE, CVC.CA_SMC.CS)

(d) to update the X.509 certificates (C.HCI.AUT, C.HCI.ENC, C.HCI.ASIG) [52]

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

142 **Application note 27**: The specification [22] describes details of the access control rules in annex A. For the term "related HPC" see application note 3.

143 **Application note 28:** According to [23] the HPC, SMC and eHC should be designed to ensure that only a health professional (i.e. the Card Holder of a HPC) may use the HPC or authorize a SMC to open the eHC for reading protected data. The eHC provides the access to these protected data only after a card-2-card authentication by an entity using a CV certificate with appropriate access rights (i.e. CHA). The SMC have such CV certificate with appropriate CHA CVC.SMC.AUT for the public key PuK.SMC.AUT and may run this authentication protocol by means of Service_Asym_Mut_Auth_w/o_SM with the private key PrK.SMC.AUT (cf. to paragraph 11). The access control of the SMC (cf. FDP_ACF.1.2, clause 2(f) and FDP_ACF.1.4, clause 1(a) and 2(a)) ensures that only the Card Holder can use the card-to-card authentication Service_Asym_Mut_Auth_w/o_SM with PrK.HPC.AUT in security environment #1. The same private key PrK.HPC.AUT and the same certificate CVC.HPC.AUT might be used by everybody (i.e. a terminal without previous authentication to the HPC, cf. FDP_ACF.1.2, clause 3(e)) to establish a trusted channel between HPC and SMC by means the Service_Asym_Mut_Auth_with_SM (cf. to paragraph 12). It is important to ensure that the

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

private key PrK.HPC.AUT, the certificate CVC.HPC.AUT and the Service_Asym_Mut_Auth_with_SM can not be misused for attacks imitating the Service_Asym_Mut_Auth_w/o_SM with private key PrK.HPC.AUT. Such attacks are prevented by design of Service_Asym_Mut_Auth_w/o_SM and Service_Asym_Mut_Auth_with_SM using different algorithm identifier and protocols (cf. to paragraphs 11 and 12). The same security features of the HPC and the additional access control over the CV certificate of the SMC CVC.SMC.AUT ensure that only the Card Holder may use the HPC to authorize the SMC to open the eHC.

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

145 **FDP_RIP.1 Residual Information Protection**

Hierarchical to: No other components.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *[assignment: allocation of the resource to, deallocation of the resource from]* the following objects: *[assignment: list of objects at least including: PINs, secret and private cryptographic keys, data in all files, which are not freely accessible]*[53].

Dependencies: No dependencies.

146 **Application note 29**: The writer of the Security Target may want to use iterations of FDP_RIP.1 in order to distinguish between data, which must be deleted already upon de-allocation and those which can be deleted upon allocation. Note that the SSCD-PP requires to delete secret signature keys upon de-allocation and that this is advisable for all PINs and secret/private cryptographic keys in general. For secret user data deletion upon allocation should be sufficient (depending on the resistance of the concrete TOE against physical attacks).

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

148 **FDP_SDI.2 Stored Data Integrity**

Hierarchical to: FDP_SDI.1.

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

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for integrity errors[54] on all objects, based on the following attributes: *[assignment: user data attributes – the attributes shall be chosen in a way that at least the following data are included:*

- *PINs,*
- *cryptographic keys,*
- *security relevant status variables of the card (e. g. authentication status for the PIN or for mutual authenticate)*
- *input data for electronic signatures*
- *user data in files on the card,*
- *file management information (like access rules for files), and*
- *the card life cycle status]*[55].

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[56].

Dependencies: No dependencies.

149 **Application note 30:** The writer of the Security Target may want to use iterations of FDP_SDI.2, for example in order to distinguish between different types of data (compare the SSCD-PP, where this is done for persistent data on the one hand and other data on the other hand).

#### 6.1.3.3 Inter-TSF-Transfer

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

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

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

Hierarchical to: No other components.

[54] *[assignment: integrity errors]*

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

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

FDP_UCT.1.1 The TSF shall enforce the SMC Access Control SFP [57] to be able to transmit and receive[58] objects in a manner protected from unauthorised disclosure.

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

153 **Application note 31**: The SMC supports secure messaging with TDES encryption (cf. SFR FCS_COP.1/TDES) after card-to-card authentication.

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

155 **FDP_UIT.1 Data exchange integrity**

Hierarchical to: No other components.

FDP_UIT.1.1 The TSF shall enforce the SMC Access Control SFP [59] to be able to transmit and receive [60] user data in a manner protected from modification, deletion, insertion and replay [61] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [62] has occurred.

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

156 **Application note 32**: The SMC supports secure messaging with MAC (cf. FCS_COP.1/MAC) after card-to-card authentication.

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

---

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

58 [selection*: transmit, receive*]

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

60 [selection*: transmit, receive*]

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

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

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

Hierarchical to: No other components.

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

FTP_ITC.1.2 The TSF shall permit the remote trusted IT product [63] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for commands and responses after successful card-to-card authentication with algorithm '1F' [64].

Dependencies: No dependencies.

159 **Application note 33:** The specification [20], Annex C and E, describes the use of secure messaging as trusted channel. The remote trusted IT product (e.g. the secure module of CMS or a HPC) may initiate the trusted channel using Service_Sym_Mut_Auth_with_SM. This does not change the security status of the SMC i.e. the TOE does not enforce the use of the trusted channel. The TOE enforces secure messaging after asymmetric card-to-card authentication with algorithm '1F' (i.e. Service_Asym_Mut_Auth_with_SM). If the external entity sent any command in plain the security status of the HPC reached after this authentication is lost and the secure messaging keys deleted (cf. [20], Annex C.2).

### 6.1.4 Security Management

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

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

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

Hierarchical to: No other components.

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

1. Initialization,

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

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

2. Personalization,
3. Card management,
4. Modification of the PIN [65].

Dependencies: No Dependencies

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

164 **FMT_SMR.1 Security roles**

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles Manufacture, Card Management system, Card Holder, Terminals, HPC [66].

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

Hierarchical to: FIA_UID.1 Timing of identification

165 **Application note 35**: The Certificate Holder authorization (CHA) Role ID are defined in [22], annex A.

166 **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.

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

168 **FMT_LIM.1 Limited capabilities**

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or

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

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

manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks [67].

Dependencies: FMT_LIM.2 Limited availability.

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

170 **FMT_LIM.2 Limited availability**

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks [68].

Dependencies: FMT_LIM.1 Limited capabilities.

171 **Application note 37**: The following four SFR address the protection of the management of the TSF data: Initialization Data, Pre-personalization Data, User Authentication Reference Data (i.e. PIN and PUC), Public Key for CV Certification Verification. Note that the Card Authentication Private Keys, the Client-Server Authentication Keys, the Decipher Private Key and the SMC Electronic Signature Private Key are user data under protection according to SFR FDP_ACF.1.

172 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.

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

Hierarchical to: No other components.

FMT_MTD.1.1/INI The TSF shall restrict the ability to write [69] the Initialization Data and Pre-personalization Data [70] to the Manufacture [71].

---

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

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

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

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/ RAD_WR: The TSF shall restrict the ability to write [72] the
1. User Authentication Reference Data and
2. public keys of the root for CV certificate verification [73]
to the Card Management System [74].

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/ RAD_MOD: The TSF shall restrict the ability to modify [75] the public keys of the root for CV certificate verification [76] to Card Management System [77].

[70] [assignment: *list of TSF data*]
[71] [assignment: *the authorised identified roles*]
[72] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[73] [assignment: *list of TSF data*]
[74] [assignment: *the authorised identified roles*]
[75] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[76] [assignment: *list of TSF data*]
[77] [assignment: *the authorised identified roles*]

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

176 **FMT_MTD.1/PIN Management of TSF data – Management of the Human User Authentication Data**

Hierarchical to: No other components.

FMT_MTD.1.1/PIN The TSF shall restrict the ability to modify and unblock [78] the PIN [79] to the Card Holder [80].

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

177 **Application note 38**: The SFR FMT_MTD.1/RAD_WR address the first writing of the authentication reference data of the Card Holder (i.e. PIN and PUC) and 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 are separated to different roles and addressed by different SFR FMT_MTD.1/RAD_MOD and FMT_MTD.1/PIN. Note, the specification [22] does not describe detailed access conditions for the public keys because their implementation is specific for the operating system. The card holder modifies his or her PIN 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 PUC and the new PIN. He or she unblocks the PIN by means of (i) the command RESET RETRY COUNTER and providing the PUC and the new PIN or (ii) the command RESET RETRY COUNTER and providing the PUC (without a new PIN).

178 **FMT_MTD.1/RAD_CH Management of TSF data – Protection of Human User Authentication Data**

Hierarchical to: No other components.

FMT_MTD.1.1/RAD_CH The TSF shall restrict the ability to read [81] the PIN and PUC [82] to none [83].

---

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

79 [assignment: *list of TSF data*]

80 [assignment: *the authorised identified roles*]

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

82 [assignment: *list of TSF data*]

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

### 6.1.5 SFR for TSF Protection

179 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 SFR "Non-bypassability of the TSP (FPT_RVM.1)" and "TSF domain separation (FPT_SEP.1)" together with "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" and "Resistance to physical attack (FPT_PHP.3)" prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

180 The TOE shall meet the requirement "Subset information flow control (FDP_IFC.1)" as specified below:

**FPT_EMSEC.1 TOE Emanation**

Hierarchical to: No other components.

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

1. PIN and PUC[84]

and

2. Card Authentication Private Keys,
3. Client-Sever Authentication Private Key,
4. Document Cipher Key Decipher Key,
5. Digital Signature Private Key,
6. secure messaging keys [85].

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

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

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

FPT_EMSEC.1.2 The TSF shall ensure any authorized user [86] are unable to use the following interface smart card circuit contacts [87] to gain access to

1. PIN and PUC[88]

and

2. Card Authentication Private Key,
3. Client-Sever Authentication Private Key
4. Document Cipher Key Decipher Key
5. Digital Signature Private Key,
6. secure messaging keys [89].

Dependencies: No other components.

181 **Application note 39**: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The SMC has to provide a smart card interface with contacts according to ISO/IEC 7816-2 [20] 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.

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

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

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

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

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

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

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

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

1. exposure to operating conditions where therefore a malfunction could occur,
2. failure detected by TSF according to FPT_TST.1 [90].

Dependencies: ADV_SPM.1 Informal TOE security policy model

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

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

Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing [91] to the TSF [92] by responding automatically such that the TSP is not violated.

Dependencies: No dependencies.

187 **Application note 40**: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

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

189 **FPT_TST.1 TSF testing**

Hierarchical to: No other components.

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

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

---

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

91 [assignment: *physical tampering scenarios*]

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

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

Dependencies: FPT_AMT.1 Abstract machine testing.

190 **Application note 41**: If SMC chip uses state of the art smart card technology it will run the some self tests at the request of the authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the "authorised user" Manufacture in the Phase 2 Manufactoring. Other self tests may run automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 Operational Use, e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks. The security target writer shall perform the operation claimed by the concrete product under evaluation.

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

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

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

Hierarchical to: No other components.

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

Dependencies: No dependencies.

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

195 **FPT_SEP.1 TSF domain separation**

Hierarchical to: No other components.

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

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

Dependencies: No dependencies.

196 **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 SMC chip Embedded Software. The security enforcing functions and health application data shall be separated in way preventing any inference.

## 6.2 Security Assurance Requirements for the TOE

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

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

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

## 6.3 Security Requirements for the IT environment

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

# 7 Rationale

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

201 The explicitly stated security requirements are taken form the Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001[16]. This PP provides a justification why the SFR 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.

## 7.1 Security Objectives Rationale

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

Table 1: Security Objective Rationale

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

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

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

205 The threat **T.Intercept** “Interception of Communication” is countered by the security objective **OT.Trusted_Channel** “Trusted Channel”. Note that according to the **OSP.SMC_Spec** “Compliance to HPC specifications” and the security objective for the TOE environment **OE.Users** “Adequate usage of TOE and IT-Systems” the external application decides whether

the data the transmitted data are sensitive and require the protection in the confidentiality and integrity. If the application selects the security environment SE #2 (cf. the specification [22]) the TOE will protect transmitted data. If the application selects the security environment SE #1 the TOE is not required to protect the data transmitted after card-to-card authentication because they are not sensitive.

206 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.

207 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.

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

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

210 The organizational security policy **OSP.SMC_Spec** "Compliance to SMC specifications" is implemented by the TOE security objectives **OT.AC_Pers** "Access control for personalization and management", **OT.AC_Serv** "Access Control for TOE Functions", **OT.Data_Confident** "Confidentiality of internal data", **OT.Data_Integrity** "Integrity of internal data" and **OT.Trusted_Channel** "Trusted Channel" and the security objectives for the TOE environment **OD.Material** "Control over Smart Card Material" and **OE.Perso** "Secure personalization and management". The TOE security objectives OT.AC_Pers, OT.AC_Serv and OT.Trusted_Channel implement the protection of the security services of the TOE and their related user data and TSF data as specified in [22] referenced in the OSP.SMC_Spec. OT.Data_Confident and OT.Data_Integrity requires the protection of the confidentiality and the integrity of the user data and the TSF data the specification relay on against any attacks. The security objectives for the environment OD.Material and OE.Perso ensure that the Card Management System will provide genuine TOE initialized and personalized according to specification [22] to the card holder.

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

212 The security objectives for the environment **OE.Perso** "Secure personalization and management" implements the assumption **A.Pers_Agent** "Personalization of the Smart Card" with respect of the concrete user and TSF data described in the specification [20] and [22] (cf. to OSP.SMC_Spec).

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

## 7.2 Security Requirements Rationale

### 7.2.1 Security Requirements Coverage

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

| | OT.AC_Pers | OT.AC_Serv | OT.Data_Confident | OT.Data_Integrity | OT.Trusted_Channel | OT.Prot_Abuse_Func | OT.Prot_Inf_Leak | OT.Malfunction | OT.Prot_Phys_Tamper |
|---|---|---|---|---|---|---|---|---|---|
| FCS_CKM.1/ASYM | | | | | x | | | | |
| FCS_CKM.1/SYM | | | | | x | | | | |
| FCS_CKM.4 | | | | | x | | | | |
| FCS_COP.1/SHA | | x | | | | | | | |
| FCS_COP.1/CCA_SIGN | | x | | | | | | | |
| FCS_COP.1/CCA_VERIF | | x | | | | | | | |
| FCS_COP.1/CSA | | x | | | | | | | |
| FCS_COP.1/RSA_DEC | | x | | | | | | | |
| FCS_COP.1/SIGN_AS | | x | | | | | | | |
| FCS_COP.1/TDES | | x | | | x | | | | |
| FCS_COP.1/MAC | | x | | | x | | | | |
| FCS_RND.1 | | x | | | | | | | |
| FIA_AFL.1 | | x | | | | | | | |
| FIA_ATD.1 | | x | | | | | | | |
| FIA_UID.1 | x | x | | | | | | | |
| FIA_UAU.1 | x | x | | | | | | | |
| FIA_UAU.4 | | x | | | x | | | | |
| FIA_UAU.6 | | x | | | x | | | | |
| FDP_ACC.2 | x | x | x | x | | | | | |
| FDP_ACF.1 | x | x | x | x | | | | | |
| FDP_RIP.1 | | | x | | | | | | |
| FDP_SDI.1 | | | | x | | | | | |
| FDP_UCT.1 | | | | | x | | | | |
| FDP_UIT.1 | | | | | x | | | | |
| FTP_ITC.1 | | | | | x | | | | |

| | OT.AC_Pers | OT.AC_Serv | OT.Data_Confident | OT.Data_Integrity | OT.Trusted_Channel | OT.Prot_Abuse_Func | OT.Prot_Inf_Leak | OT.Malfunction | OT.Prot_Phys_Tamper |
|---|---|---|---|---|---|---|---|---|---|
| FMT_SMF.1 | x | x | | | | | | | |
| FMT_SMR.1 | x | x | | | | | | | |
| FMT_LIM.1 | | x | | | | x | | | |
| FMT_LIM.2 | | x | | | | x | | | |
| FMT_MTD.1/INI | x | | x | | | | | | |
| FMT_MTD.1/PIN | x | x | x | x | | | | | |
| FMT_MTD.1/RAD_CH | | x | x | | | | | | |
| FMT_MTD.1/RAD_WR | x | x | x | x | | | | | |
| FMT_MTD.1/RAD_MOD | x | x | x | x | | | | | |
| FPT_EMSEC.1 | | | x | | | | x | | |
| FPT_FLS.1 | | | x | x | | | x | x | |
| FPT_PHP.3 | | | x | x | | | x | x | x |
| FPT_RVM.1 | x | x | x | x | | x | x | x | |
| FPT_SEP.1 | | | x | x | | x | | x | |
| FPT_TST.1 | | | | | | | x | x | |

Table 5: Security functional requirements rationale

### 7.2.2 Security Requirements Sufficiency

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

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

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

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

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

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

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

(i) the TOE security service Service_Asym_Mut_Auth_w/o_SM is implemented by the SFR **FCS_COP.1/CCA_SIGN**, **FCS_COP.1/CCA_VERIF**, **FCS_RND.1** and **FIA_UAU.4**.

(ii) the TOE security service Service_Asym_Mut_Auth_with_SM is implemented by the SFR **FCS_COP.1/SHA, FCS_CKM.1**, **FCS_CKM.4**, **FCS_COP.1/CCA_SIGN**, **FCS_COP.1/CCA_VERIF**, **FCS_RND.1**, **FCS_COP.1/TDES**, **FCS_COP.1/MAC** and **FIA_UAU.4**.

(iii) the TOE security service Service_Client_Server_Auth is implemented by the SFR **FCS_COP.1/CSA**,

(iv) the TOE security service Service_Key_Decryption is implemented by the SFR **FCS_COP.1/RSA_DEC,**

(v) the TOE security service Service_SM_Support is implemented by the SFR **FCS_COP.1/TDES** and **FCS_COP.1/MAC,**

(vi) the TOE security service Service_Elec_Signature is implemented by the SFR **FCS_COP.1/SHA** and **FCS_COP.1/SIGN_AS**.

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

(i) the **SFR FMT_SMR.1** define the Card holder as known role of the TOE and **FIA_ATD.1** binds his identity and role for the authentication,

(ii) the SFR **FMT_MTD.1/PIN**, **FMT_MTD.1/RAD_CH**, and **FIA_AFL.1/PIN** protect and limit the management of the authentication reference data to the Card holder,

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

(iv) the **SFR FDP_ACC.1** and **FDP_ACF.1** limit the use of the security services except Service_Asym_Mut_Auth_with_SM to the Card holder only.

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

(i) The SFR **FMT_MTD.1/RAD_CH** protects the confidentiality of the PIN and PUC as card holder authentication reference data against reading,

(ii) the SFR **FDP_ACC.1** and **FDP_ACF.1** (cf. FDP_ACF.1.4, rule 3b) protects the confidentiality of the private keys against reading,

(iii) the SFR **FDP_RIP.1** protects the misuse of residual user data,

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

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

(i) The SFR **FMT_MTD.1/PIN** and **FMT_MTD.1/RAD_CH** protects the intergity of the PIN and PUC as card holder authentication reference data against reading,

(ii) the SFR **FDP_ACC.1** and **FDP_ACF.1** (cf. FDP_ACF.1.4, rule 3a) protects the integrity of the data under the TSC,

(iii) the SFR **FDP_SDI.1** protects the internal stored user data against alteration,

(iv) the SFR **FPT_FLS.1**, **FPT_PHP.3**, **FPT_RVM.1** and **FPT_SEP.1** protect the confidential user data and TSF data against general smart card attacks.

219 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 are implemented by following SFR:

(i) the SFR **FCS_CKM.1/ASYM, FCS_CKM.1/SYM** and **FCS_RND.1** establish and **FCS_CKM.4** destructs the secure messaging keys,

(ii) the SFR **FCS_COP.1/TDES** and **FCS_COP.1/MAC** providing encryption, decryption, MAC calculation and MAC verification,

(iii) the SFR **FDP_UCT.1, FDP_UIT.1** and **FTP_ITC.1** provides the protection of the confidentiality and integrity of the transmitted data

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### 7.2.3 Dependency Rationale

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| FCS_CKM.1/ASYM | [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction,<br>FMT_MSA.2 Secure security attributes | FCS_CKM.4, FCS_COP.1, justification 1 for non-satisfied dependencies |

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| FCS_CKM.1/SYM | [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction,<br>FMT_MSA.2 Secure security attributes | FCS_CKM.4, FCS_COP.1, justification 1 for non-satisfied dependencies |
| FCS_CKM.4 | [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation],<br>FMT_MSA.2 Secure security attributes | FCS_CKM.1, justification 1 for non-satisfied dependencies |
| 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]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | justification 2 for non-satisfied dependencies |
| 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]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | justification 3 for non-satisfied dependencies |
| FCS_COP.1/CCA_VERIF | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | justification 3 for non-satisfied dependencies |
| FCS_COP.1/CSA | [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]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | justification 3 for non-satisfied dependencies |
| FCS_COP.1/RSA_DEC | [FDP_ITC.1 Import of user data without | justification 3 for non- |

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| | security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | satisfied dependencies |
| FCS_COP.1/SIGN_AS | [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]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | FCS_CKM.1, FCS_CKM.4, justification 3 for non-satisfied dependencies |
| FCS_COP.1/TDES | [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]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | FCS_CKM.1, FCS_CKM.4, justification 1 for non-satisfied dependencies |
| FCS_COP.1/MAC | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction<br>FMT_MSA.2 Secure security attributes | FCS_CKM.1, FCS_CKM.4, justification 1 for non-satisfied dependencies |
| FCS_RND.1 | No dependencies | n.a. |
| FIA_AFL.1 | FIA_UAU.1 Timing of authentication | fulfilled |
| 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.6 | No dependencies | n.a. |
| FDP_ACC.2 | FDP_ACF.1 Security attribute based access control | fulfilled |

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| FDP_ACF.1 | FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization | FDP_ACC.2, justification 4 for non-satisfied dependencies |
| FDP_RIP.1 | No dependencies | n.a. |
| FDP_SDI.1 | No dependencies | n.a. |
| FDP_UCT.1 | [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] | Fulfilled by FTP_ITC.1 and FDP_ACC.2 hierarchical to FDP_ACC.1 |
| FDP_UIT.1 | [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] | Fulfilled by FTP_ITC.1 and FDP_ACC.2 hierarchical to FDP_ACC.1 |
| FTP_ITC.1 | No dependencies | n.a. |
| FMT_SMF.1 | No dependencies | n.a. |
| FMT_SMR.1 | FIA_UID.1 Timing of identification | fulfilled |
| FMT_LIM.1 | FMT_LIM.2 | fulfilled |
| FMT_LIM.2 | FMT_LIM.1 | fulfilled |
| FMT_MTD.1/INI | 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 |
| FMT_MTD.1/RAD_CH | FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles | fulfilled |
| FMT_MTD.1/RAD_WR | FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles | fulfilled |
| FMT_MTD.1/RAD_MOD | FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles | fulfilled |
| FPT_EMSEC.1 | No dependencies | n.a. |
| FPT_FLS.1 | ADV_SPM.1 | fulfilled by EAL4 |
| FPT_PHP.3 | No dependencies | n.a. |
| FPT_RVM.1 | No dependencies | n.a. |

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| FPT_SEP.1 | No dependencies | n.a. |
| FPT_TST.1 | FPT_AMT.1 Abstract machine testing | See justification 5 for non-satisfied dependencies |

Table 2: Dependency rationale overview

224 Justification for non-satisfied dependencies:

No. 1: The TSF according to SFR FCS_CKM.1 and FCS_CKM.4 generate and destroy automatically the secure messaging keys used for FCS_COP.1/TDES and FCS_COP.1/MAC. If the TOE does not support the optional management of logical channels it will be no need for security attributes of these keys. If the TOE support the management of logical channels the security target will describe the management security attributes of theses keys (cf. Application note 33).

No. 2: The cryptographic algorithm SHA-1 does not use any cryptographic key. Therefore none of the listed SFR are needed to be defined for this specific instantiation of FCS_COP.1.

No. 3: The SFR FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/CSA, FCS_COP.1/SIGN_AS and FCS_COP.1/RSA_DEC use keys which are loaded or generated during the personalisation and are not updated or deleted over the life time of the TOE. Therefore none of the listed SFR are needed to be defined for this specific instantiations of FCS_COP.1.

No. 4: The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.2) is necessary here.

No. 5: The TOE consist of the software and its underlying hardware on which it is running. Thus there is no abstract machine to be tested.

### 7.2.4 Rationale for the Assurance Requirements

225 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.

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

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

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

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

230 The component ADV_IMP.2 has the following dependencies:

- ADV_LLD.1 Descriptive low-level design
- ADV_RCR.1 Informal correspondence demonstration
- ALC_TAT.1 Well-defined development tools

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

231 The component AVA_MSU.3 has the following dependencies:

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

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

232 The component AVA_VLA.4 has the following dependencies:

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

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

### 7.2.5 Security Requirements – Mutual Support and Internal Consistency

233 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.

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

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

The dependency analysis in section 7.2.3 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

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

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

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

# 8 PP Application Notes

## 8.1 Glossary and Acronyms

| Term | Definition |
|---|---|
| *Application note* | Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7). |

| Term | Definition |
|---|---|
| *Health Employee Card* | Special case of a HPC with |
| *Health Professional Data* | Personal data identifying the Health Professional holding the HPC as natural person |
| *IC Dedicated Support Software* | That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases. |
| *IC Dedicated Test Software* | That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter. |
| *Initialisation Data* | Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification (IC identification data). |
| *Integrated circuit (IC)* | Electronic component(s) designed to perform processing and/or memory functions. The eHC's chip is a integrated circuit. |
| *Personalization* | The process by which personal data are brought into the TOE before it is handed to the card holder |
| *secure messaging in encrypted mode* | Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 |
| *Secure Module Card* | Smart card providing security services in the health care environment. |
| *TSF data* | Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [1]). |
| *User data* | Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [1]). |

**Acronyms**

| Acronyms | Term |
|---|---|
| *CVC.SMC.AUT* | Certificate of the public key corresponding to |
| *CA* | Certification authority |
| *CC* | Common Criteria |

| Acronyms | Term |
|---|---|
| *CSP* | Certification service provider |
| *eHC* | Electronic health card |
| *HEC* | Health employee card |
| *HPC* | Health professional card |
| *PIN.SMC.ASS* | Global PIN of human user authentication for all HPC security services except the application for qualified signature |
| *PrK.HCI.AUT* | Private key for client-server authentication |
| *PrK.HCI.ENC* | Private key to decipher document encryption keys |
| *PrK.SMC.AUT* | Private key for card-to-card authentication between TOE and external SMC |
| *PuK.CA_SMC.CS* | Public key of certification service provider used for verification of card verifiable certificates |
| *SAR* | Security assurance requirements |
| *SFR* | Security functional requirement |
| *SMC* | Secure module card |
| *TOE* | Target of Evaluation |
| *TSF* | TOE security functions |

## 8.2 Literature

**Common Criteria**

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.1, August 1999

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.1, August 1999

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.1, August 1999

[4] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999

[5] Anwendungshinweise und Interpretationen zum Schema, AIS32: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, Version 1, 02.07.2001, Bundesamt für Sicherheit in der Informationstechnik

**Cryptography**

[6] Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, Bonn, 10.8.2004 (Zieldatum der Veröffentlichung ist Januar 2005)

[7] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

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

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

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

[11] Certicom Research: SEC 1: Elliptic Curve Cryptography, September 20, 2000, Version 1.0

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

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

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

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

**Protection Profiles**

[16] Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

[17] Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002

**Sonstige**

[18] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform, gematik, Version 0.99, Standardentwurf, 31.Oktober 2005

[19] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Anwendungen und anwendungsspezifische Strukturen, gematik, Version 0.99, Standardentwurf, 06.November 2005

[20] Specification German Health Professional Card and Security Module Card - Pharmacist & Physician – Part 1: Commands, Algorithms and Functions of the COS Platform, Version 2.1, 07.11.2005, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychoterapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Deutsche Krankenhaus-Gesellschaft

[21] German Health Professional Card and Security Module Card Specification - Pharmacist & Physician – Part 2: HPC Applications and Functions, Version 2.1 draft, 19.11.2005, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychoterapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Deutsche Krankenhaus-Gesellschaft

[22] German Health Professional Card and Security Module Card Specification - Pharmacist & Physician - Part 3: SMC Applications and Functions, Version 2.1 draft, 19.11.2005, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychoterapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Deutsche Krankenhaus-Gesellschaft

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