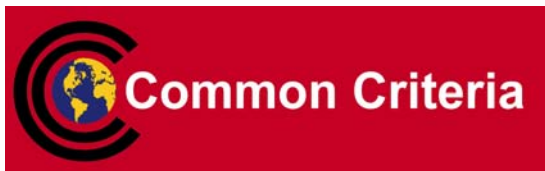Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Protection Profile
Health Professional Card (HPC)
Heilberufsausweis (HPA)

Common Criteria

BSI-PP-0018

Approved by the
Federal Ministry of Health

—— this page was intentionally left blank ——

Foreword

This 'Protection Profile — Professional Health Card (PP-HPC)' 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 — Professional Health Card (PP-HPC) 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

Variables

Name	Value	Display
File name and sizes	Set automatically	Protection Profile_HPC_v1_0.doc (1242112 Byte)
Last Version	1.0	1.0
Date	12th December 2005	12th December 2005
Classification	unclassified	unclassified
Authors	Wolfgang Killmann	Wolfgang Killmann

Table of Content

1   PP Introduction

1.1   PP reference

1   Title: Protection Profile — Health Professional Card (PP-HPC)

    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-0018

    Keywords: electronic health card, health professional card

1.2   PP Overview

2   The protection profile defines the security objectives and requirements for the electronic **Health Professional Card** (HPC, German: "Heilberufsausweis") 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 HPC and a electronic Health Card (eHC) or the HPC and a Security Module Card (SMC),

- Document key decipherment for an external application,

- Client-server authentication for a client.

    This Protection profile <u>does not</u> address the use of the HPC as secure-signature creation device for qualified electronic signature (cf. chapter 9 Informative Annex: HPC as SSCD for details).

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 Health Professional Card (HPC, German "Heilberufsausweis"). HPC is a contact based smart card which is conformant to the specification documents [15] and [16].

5   The **TOE** comprises of

   TOE_IC, consisting of:
   -    the circuitry of the HPC's chip (the integrated circuit, IC) and
   -    the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
   TOE_ES
   -    the IC Embedded Software (operating system)
   TOE_APP
   -    the HPC applications (data structures and their content)
   and
   TOE_GD
   -    the guidance documentation delivered together with the TOE.

6   The **TOE** is used by an individual acting as accredited health profession

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

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

   (3) to decrypt keys of encrypted application data.

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 (7) listed below,

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

   (4)   Asymmetric card-to-card authentication between the HPC and the SMC with 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) Document key decipherment,

(7) Client-server authentication,

2.2 TOE usage and security features for operational use

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

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

This service is meant as a protection of the other services, which require user authentication. In addition it provides privacy protection because certain data in the card (or secured by the card) can only be accessed after user authentication ([16], section 7.4).

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 **Service_Asym_Mut_Auth_w/o_SM[1]**: Mutual Authentication using asymmetric techniques between the HPC and a eHC without establishment of a trusted channel ([16], section 7.5).

This service is meant for situations, where the eHC requires authentication by a HPC or SMC and the SMC requires authentication by HPC to provide access to protected data. 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 [15], Annex E.2). The algorithmic identifier '1E' used for the commands EXTERNAL AUTHENTICATE and INTERNAL AUTHENTICATE enforces the answer expected by the command EXTERNAL AUTHENTICATE and the answer provided by the command INTERNAL AUTHENTICATE are signed by private key of the entity which authenticates themselves (cf. for details to [15], Annex E.2).

11 **Service_Asym_Mut_Auth_with_SM**: Mutual Authentication using asymmetric techniques between the HPC and a SMC or the CMS 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 (cf. for details to [15], Annex C).

This service is meant for situations, where the HPC and a SMC or the CMS, 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 run a protocol in two linked together 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

---

[1] The Abbreviation SM here stands for Secure Messaging, which is the card security protocol implementing a trusted channel (cf. e.g. [15], Annex A).

[15], 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 are signed by private key of the entity which authenticates themselves (cf. for details to [15], Annex E.3) and encrypted with the public key of the entity verifying the authentication attempt.

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

This service is meant for situations, where the HPC communicates with an external entity, which shares symmetric keys agreed with the HPC by means of Service_Sym_Mut_Auth_with_SM and stored in the HPC for future use. The HPC uses of the protocol 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 [15], 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.

13 **Service_Client_Server_Auth**: The HPC 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, [16], section 9.6). 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.

14 **Service_Key_Decryption**: The HPC 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 ([16], section 9.7). 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.

15 In detail the functionality of the HPC 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 draft, 07.11.2005, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychotherapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Deutsche Krankenhaus-Gesellschaft

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

16 **Application note 1**: The HPC also supports the creation of qualified electronic signatures [16], chapter 8. The security requirements for the HPC as secure-signature creation device is not described in this protection profile. The security target writer will include the security objectives and relevant security requirements in the security target if they are subject of the product evaluation.

2.3   TOE life cycle

17 The following description is a short summary of the HPC life cycle model based on a common model normally used for smart cards. The TOE life cycle is described in terms of the seven life cycle phases as usually defined for smart cards, see for example the SSVG-PP [12]. They are summarized in the following table.

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

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

Table 1: Smart Card Life Cycle Overview

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

19   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.

20   For the evaluation of the HPC 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:

21 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.

22 The data structures and the access rights to the health application data as defined in the HPC specification [16] are covered by the evaluation.

23 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.

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

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

        o 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 [16].

        o 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 [16], but isn't embedded in a plastic card yet.

        o 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 [16] (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]:

        o 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.

---

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

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

o 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.

o 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

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

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

- **subjects**, who are users (human or system) of the TOE or who might be threat agents (i. e. attack the security of the assets)

- **operational security policies** , which describe overall security requirements defined by the organisation in charge of the overall system including the TOE. In particular this may include legal regulations, standards and technical specifications.

- **threats** against the assets, which shall be averted by the TOE together with its environment

- **assumptions** on security relevant properties and behaviour of the TOE's environment

3.1   Introduction

Assets

26 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.CAMS_HPC.AUT)	The Card Verifiable Authentication Certificate of the Card Management System CVC.CAMS_HPC.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.RCA.CS (cf. to [16], chapter 12, for details).
Root Public Key of the Certificate Service Provider (PuK.RCA.CS)	The public key PuK.RCA.CS of the Health Care Root CA for verification of the card verifiable certificate of the certificate service provide for card verifiable certificates in the health care environment (cf. to [16], sec. 5.3, for details). It is part of the TSF data which integrity shall be protected.
Certificate of the Certificate Service Provider (CVC.CA_NN_HPC.CS)	The certificate of the Certificate Service Provider for card verifiable certificates in the health care environment CVC.CA_NN_HPC.CS containing the public key PuK.CA_NN_HPC.CS for verification of the card verifiable certificates like CVC.HPC.AUT. It is part of the 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.CA_NN_HPC.CS.
Public Key of the Certificate Service Provider (PuK.CA_NN_HPC.CS)	The public key of the Certificate Service Provider for card verifiable certificates in the health care environment PuK.CA_NN_HPC.CS used for verification of the card verifiable certificate CVC.SMC.AUT and CVC.eHC.AUT. It is part of the TSF data which integrity shall be protected.
Card Authentication Private Keys (PrK.HPC.AUT)	The Card Authentication Private Key PrK.HPC.AUT is an asymmetric cryptographic key used for the authentication of a HPC to a SMC or a eHC on behalf of the card holder. PrK.HPC.AUT is part of the user data.
Card Verifiable Authentication Certificate (CVC.HPC.AUT)	Card verifiable certificate CVC.HPC.AUT for the Card Authentication Public Key PuK.HPC.AUT as authentication reference data corresponding to the Authentication Private Key PrK.HPC.AUT and used for the card-to-card authentication of the HPC to the eHC and to the SMC **without** establishing a trusted channel by means of secure messaging. It contains encoded access rights (Role ID) and is signed by the HPC card issuer. It is part of the user data provided for use by external

---

3   Note the names of the keys and certificates are not consolidated between [15], [16] and [18] yet.

Name of asset[3]	Description
	entities as authentication reference data of the HPC. It is stored in the file EF.CVC.HPC.AUT which integrity shall be protected.
Card Verifiable Authentication Certificate (CVC.HPC.TCE)	Card verifiable certificate CVC.HPC.TCE for the Card Authentication Public Key PuK.HPC.AUT as authentication reference data corresponding to the Authentication Private Key PrK.HPC.AUT and used for the card-to-card authentication of the HPC to the eHC and to the SMC **with** establishing a trusted channel by means of secure messaging. It contains encoded access rights (Role ID) and is signed by the HPC 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.HPC.TCE which integrity shall be protected.
Client-Server Authentication Private Key (PrK.HP.AUT)	The Client-Server Authentication Private Key PrK.HP.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.HP.AUT)	X.509 Certificate C.HP.AUT for the Client-Server Authentication Public Key PuK.HP.AUT corresponding to the Client-Server Authentication Private Key PrK.HP.AUT. It is part of the user data provided for use by external entities as authentication reference data of the HPC (cf. to [16], sec. 9.6, for details).
Decipher Private Key (PrK.HP.ENC)	The Document Cipher Key Decipher Key PrK.HP.ENC is asymmetric private key used for document decryption on behalf of the card holder. It is part of the user data.
Encryption Certificate (C.HP.ENC)	X.509 Certificate C.HP.ENC for the Document Cipher Key Encipher Public Key PuK.HP.ENC corresponding to the Document Cipher Key Decipher Key PrK.HP.ENC (cf. to [16], sec. 9.7, for details). It is part of the user data provided for use by external entities.
Health Professional Data (HPD)	Personal data of the smart card holder (stored in the file EF.HPD). It is part of the user data. The integrity of this data shall be protected.
Display message (DM)	Display message contained in the DF.ESIGN which a terminal is allowed to read if secure messaging is established.
TOE initialization data	Data stored in the TOE during the initialization process. It may contain user data and TSF data.
TOE pre-personalization data	Data stored in the TOE during pre-personalization process. It may contain user data and TSF data.
User Authentication Reference Data	The User Authentication Reference Data are used to verify the card holder attempt to activate certain functions of the TOE. This

Name of asset[3]	Description
(PIN.CH, PUC.CH)	data include PIN.CH and PUC.CH. They are in particular not used for qualified electronic signatures. They are part of the TSF data.

Table 2: Assets of the HPC

27 **Application note 3:** The PKI under the HP Sector Root CA and the CA HP-ADMIN are introduced in [16]. The User Authentication Reference Data (PIN.CH and PUC.CH) and the public keys for CV certificate verification (PuK.CA-HP-ADMIN.CS, PuK.CA_NN_HPC.CS, PuK.CA_NN_HPC.CS) are used as authentication reference by TSF for human user and card authentication. The Card Authentication Private Keys (PrK.HPC.AUT), the Client-Server Authentication Private Key (PrK.HP.AUT) and the Document Cipher Key Decipher Key (PrK.HP.ENC) are used as cryptographic keys by the TOE security services provided to the user. Therefore they are assessed as user data.

Subjects

28 This protection profile considers the following subjects:

Name of subject	Description
Card Management System	Person(s) responsible for the personalization of the card for the Card Holder and for the Card Application Management System (CAMS).
Card Holder	Person for whom the HPC is personalized and which controls the use of the HPC. He or she knows rightfully the user authentication data (PIN and PUC).
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.
Secure Module Card	Smart card possessing the private key corresponding to the public key in a card verifiable certificate with a corresponding card holder authorization as Secure Module Card according to [16], Annex F.
Unauthorized subject	All subjects who is trying to interact with the TOE as Card Management System, Card Holder or SMC without being authenticated for this role.

Table 3: Subjects

29 **Application note 4:** 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 [16], 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

30   OSPs will be defined in the following form:

OSP.name   Short Title

Description.

31   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).

32   **OSP.HPC_Spec   Compliance to HPC specifications**

The HPC shall be implemented according to the specifications:

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

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

33   **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

34   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.

35   Threats will be defined in the following form:

T.name   Short Title

Description.

3.3.1 Threats mainly addressing TOE_ES and TOE_APP

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

37 **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).

38 **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.

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

40 **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 SMC to read, to forge, to delete or to add other data to the transmitted sensitive data.

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

3.3.2 Threats mainly addressing TOE_IC and TOE_ES

41 **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.

42 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).

43 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.

44 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

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

46 The assumptions will be defined in the following form:

   A.name   Short Title

   Description.

47 **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 [16] and ensures the correctness, the quality and - if necessary - the confidentiality of all data structures and data on the card.

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

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

4 Security Objectives

49 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 Security Objectives for the TOE

50 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.

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

   OT.name   short title

   Description of the objective.

52 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).

53 **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 the Card Management System only except the card holder authentication reference data managed by the card holder.

54 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 against attacks with high attack potential. The TOE allows to read the display message only an authenticated corresponding SMC after establishing secure messaging.

55 OT.Data_Integrity   Integrity of internal data

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

56 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 (selecting the security environment SE #2 [4]).

57 OT.AC_Serv   Access Control for TOE Security Services

The TOE provides the 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 TOE must ensure that the TOE security Service_Asym_Mut_Auth_w/o_SM, Service_Client_Server_Auth and Service_Key_Decryption can be used by the card holder only.

58 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.

59 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

---

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

- 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.

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

61 **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.

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

63 **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.

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

4.2 Security Objectives for the Development and Manufacturing Environment

65   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).

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

OD.name   short title

Description of the objective.

67   **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.

68   **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.

4.3 Security Objectives for the Operational Environment

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

OE.name   short title

Description of the objective.

70   The following objectives for the operational environment correspond directly to the assumptions in section 3.4 Assumptions:

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

All data structures and data on the card produced during personalisation or additional administration or management steps during the end-usage phase must be performed correctly according to the specifications [16] and are handled correctly regarding integrity and confidentiality of these data. The Card management system ensure (i) the correctness of the personal data of smart card holder (Health Professional Data), (ii) the generation of the card-to-card authentication keys stored on smart card and the distribution of the corresponding public key in form of CV certificates including the access rights of the card holder, (iii) writing the public key for verification of CV certificates for card-to-card authentication, (iv) the generation of the client-server authentication keys stored on smart card and the distribution of the corresponding public key in form of X.509 certificates by an public key infrastructure, (v) the generation of the decipher key stored on the smart card and the distribution of the corresponding public key in form

of X.509 certificates by an public key infrastructure. This includes in particular sufficient cryptographic quality of cryptographic keys (in accordance with the cryptographic algorithms specified for the HCP) and their confidential handling.

72 OE.Users   Adequate usage of TOE and IT-Systems

The card holder of the TOE needs to use the TOE adequately. In particular he mustn't tell the PIN (or PINs) of the HCP to others and mustn't 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 in particular by selection of appropriate smart card security environment (i.e. SE#1 or SE#2 for the HPC).

5   Extended Components Definition

73 This protection profile uses components defined as extensions to CC part 2. Some of these components are defined in [12] and [14], other components are defined in this protection profile.

5.1   Definition of the Family FCS_RND

74 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.

75 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 Generation of random numbers        │─────│ 1 │
└──────────────────────────────────────────────┘     └───┘
```
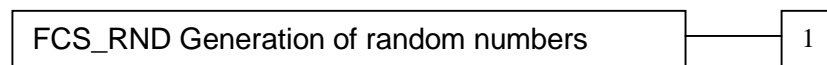
FCS_RND.1   Generation of random numbers requires that random numbers meet a defined quality metric.

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

76 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.

77 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:
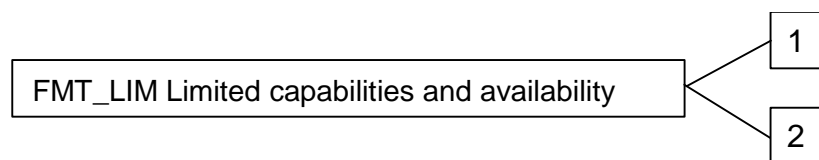
FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

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.

78   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.

79   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.

80   Application note 8: 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.

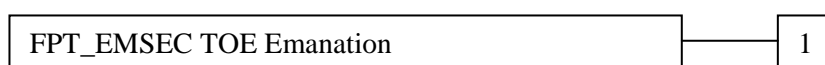The combination of both requirements shall enforce the policy.

5.3   Definition of the Family FPT_EMSEC

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

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC TOE Emanation	1

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

82   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.

83   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.

84   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*.

85   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*.

86 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

87 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].

88 **Application note 9:** The following table provides an overview how the security services (listed in paragraph 7) match to the SFR.

Security Service	SFR	Comment
Human user authentication	FIA_AFL.1, FIA_ATD.1, FIA_UID.1, FIA_UAU.1, FMT_MTD.1/PIN, FMT_MTD.1/RAD_WR, FMT_MTD.1/RAD_CH	Human user authentication is performed by means of the 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 [15], Annex E, 1. verification of digital signatures of certificates according to ISO 9796-2 (without random numbers) 2. RSA with private key for INTERNAL AUTHEN-TICATE and RSA with public key for EXTERNAL AUTHENTICATE with DSI according [15], Annex E
Client-server authentication	FCS_COP.1/CSA	Client-server authentication by means of digital signature-creation according to PKCS#1, EMSA-PKCS1-v1_5 [11]
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 [15], Annex E and secure messaging encryption and MAC is described in [15], 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. [16], 9.7 and Annex E for details

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

6.1.1 Cryptographic support (FCS)

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

90 **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 <u>asymmetric card-to-card authentication with key agreement</u> [5] and specified cryptographic key sizes <u>112 bit</u> [6] that meet the following: <u>[15], Annex E.3</u> [7].

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

91 **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 <u>symmetric card-to-card authentication with key agreement</u> [8] and specified cryptographic key sizes <u>112 bit</u> [9] that meet the following: <u>[15], Annex E.4</u> [10].

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

92 **Application note 10:** The [15], Annex E, describes 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 [15], Annex D. The **asymmetric** card-to-card authentication with key agreement [15], Annex E.3, 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**

---

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

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

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

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

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

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

card-to-card authentication with key agreement [15], Annex E.4, 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.

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

94   **FCS_CKM.4 Cryptographic key destruction**

Hierarchical to: No other components.

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

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

95   **Application note 11:** 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.

96   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.

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

Hierarchical to: No other components.

FCS_COP.1.1/   The TSF shall perform hashing [11] in accordance with a specified
SHA   cryptographic algorithm SHA-1 and SHA-2 (256 bit) [12] and
                      cryptographic key sizes none [13] that meet the following: FIPS 180-2 [14].

---

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

[12]   [assignment: *cryptographic algorithm*]

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

[14]   [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

98 **Application note 12:** This SFR requires the TOE to implement the hash function SHA-1 (160 bit hash value) and SHA-2 (256 bit hash value) for the cryptographic primitive of the authentication mechanism according to [15], chapter 4, Table 6a, and chapter 11.

99 **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 <u>digital signature-creation</u> [15] in accordance with a specified cryptographic algorithm <u>RSA</u> [16] and cryptographic key sizes <u>1024 bit module length</u>[17] that meet the following: <u>[16], Annex E</u> [18].

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

100 **Application note 13:** 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 [15], 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 [15], 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.

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

Hierarchical to: No other components.

---

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

[16]   [assignment: *cryptographic algorithm*]

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

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

FCS_COP.1.1/ CCA_VERIF	The TSF shall perform digital signature-verification [19] in accordance with a specified cryptographic algorithm RSA [20] and cryptographic key sizes 1024 bit module length[21] that meet the following: [16], Annex E [22].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

102 **Application note 14:** 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. EXTERNAL AUTHENTICATE, algorithm identifier '1E' and '1F') according to [15], 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 [15], 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.

103 **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 [23] in accordance with a specified cryptographic algorithm RSA [24] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: PKCS#1, EMSA-PKCS1-v1_5 [11] [25].
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 15:** 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 [16], sec. 9.6. The [15], chp. 11, does not specify the RSA module length for the

---

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

[20] [assignment: *cryptographic algorithm*]

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

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

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

[24] [assignment: *cryptographic algorithm*]

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

digital signature-creation for the client-server authentication mechanism. Therefore the ST writer shall perform the missing operation in FCS_COP.1/CSA.

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

Hierarchical to: No other components.

FCS_COP.1.1/ RSA_DEC
The TSF shall perform <u>decryption</u> [26] in accordance with a specified cryptographic algorithm <u>RSA</u> [27] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [16], Annex E [28].

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 16:** This SFR requires the TOE to implement the RSA for the cryptographic primitive of the RSA decryption to [16], sec. 9.7. The [15], chp. 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/RSA_DEC.

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

Hierarchical to: No other components.

FCS_COP.1.1/ TDES
The TSF shall perform <u>encryption and decryption</u> [29] in accordance with a specified cryptographic algorithm <u>Triple-DES in CBC mode</u> [30] and cryptographic key sizes <u>112 bit</u> [31] that meet the following: <u>FIPS 46-3 [8] and [15], Annex C</u> [32].

---

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

[27] [assignment: *cryptographic algorithm*]

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

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

[30] [assignment: *cryptographic algorithm*]

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

[32] [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 17:** 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.

109 FCS_COP.1/MAC Cryptographic operation – Retail MAC

Hierarchical to: No other components.

FCS_COP.1.1/   The TSF shall perform generation and verification of message authentication
MAC   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 [15], Annex C [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

110 **Application note 18:** 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.

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

112 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*].

---

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

[34]   [assignment: *cryptographic algorithm*]

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

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

Dependencies: No dependencies.

113 **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

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

115 **FIA_AFL.1 Authentication failure handling – HPC-PIN**

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 for the health care application [37].

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 [38].

Dependencies: FIA_UAU.1 Timing of authentication.

116 **Application note 20:** The component FIA_AFL.1 address the human user authentication by means of the PIN.CH for the health care application. The reference data for the PIN is stored EF.PIN under MF [16], sec. 7.2. 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 [15], 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.

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

118 **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 [39].

---

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

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

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

Dependencies: No dependencies.

119 **Application note 21:** The component FIA_ATD.1 applies to (i) the human user authentication, i.e. the card holder which identity is given in the Health Professional Data (EF.HPD), and to (ii) the card-to-card authentication where the identity (i.e. the ICCSN.ICC) and the role (i.e. Role ID) are encoded in the CV certificate (cf. [15] Annex B, for details).

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

121 **FIA_UID.1 Timing of identification**

Hierarchical to: No other components.

FIA_UID.1.1   The TSF shall allow

(1) reading the ATR

(2) reading data with access condition ALWAYS,

(3) [assignment: *list of TSF mediated actions*] [40]

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.

122 **Application note 22:** The ST writer shall perform the missing operation in FIA_UID.1.1. According to the specification [16], Annex B, the list of data objects with read access condition includes but is not limited to the Health Professional related Data, the Card Verifiable Authentication Certificates and the X.509 Certificates. The card management system may create DF and EF in MF and DF ,and define their access conditions.

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

124 **FIA_UAU.1 Timing of authentication**

Hierarchical to: No other components.

---

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

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.HPC.AUT, algorithm '1F' in SE#2,

(5) [assignment: *list of TSF mediated actions*] [41]

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

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

Dependencies: FIA_UID.1 Timing of identification.

125 **Application note 23:** The ST writer shall perform the missing operation in FIA_UAU.1.1. According to the specification [16] 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.

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

127 **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 Card-to-Card Authentication Mechanism

(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 [42].

Dependencies: No dependencies.

128 **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

---

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

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

FCS_RND.1) as challenge to prevent reuse of a response generated in a successful authentication attempt.

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

130 **FIA_UAU.6 Re-authenticating**

Hierarchical to: No other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions <u>successful established secure messaging</u> [43].

Dependencies: No dependencies.

131 **Application note 25:** The specification [15] 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

132 The following Security Function Policy (SFP) HCP 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 (except trusted channel by means of Service_Asym_Mut_Auth_with_SM and Service_Sym_Mut_Auth_with_SM). The TOE protects the communication with the outside world in confidentiality and integrity for reading the display message or on demand of the IT environment."

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

134 **FDP_ACC.2 Complete Access Control**

Hierarchical to: Subset access control

---

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

FDP_ACC.2.1   The TSF shall enforce the <u>HCP Access Control SFP</u> [44] on

     1. <u>the subjects</u>

        (a)   <u>the Card Management System,</u>

        (b)   <u>the Card Holder,</u>

        (c)   <u>a Terminal,</u>

        (d)   <u>a Secure Module Card and</u>

     2. <u>the objects</u>

        •   <u>Master File (MF), Dedicated Files (DF) and Elementary Files (EF),</u>

        •   <u>Health Professional related Data (EF.HPD),</u>

        •   <u>Global Data Object (EF.GDO),</u>

        •   <u>Card Authentication Private Keys (PrK.HPC.AUT)</u>

        •   <u>Client-Server Authentication Private Key (PrK.HP.AUT),</u>

        •   <u>Decipher Private Key (PrK.HP.ENC),</u>

        •   <u>Card Verifiable Certificates (CVC.HPC.AUT, CVC.HPC.TCE, CVC.CA_HPC.CS),</u>

        •   <u>X.509 certificates (C.HP.AUT, C.HP.ENC)</u>

        •   <u>display message in DF.ESIGN</u> [45]

     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

135 **Application note 26:** The subjects and objects are described in section 3.1 Introduction. The User Authentication Reference Data (PIN.CH and PUC.CH) and the public key for CV certificate verification (PuK.CA_NN_HPC.CS, PuK.CA_NN_HPC.CS) are TSF data. The private keys, the certificates and the display message for creation of qualified signature (contained in the DF.QES) are out of scope of this protection profile for HPC.

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

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

Hierarchical to: No other components.

FDP_ACF.1.1   The TSF shall enforce the <u>HPC Access Control SFP</u> [46] to objects based on the following: <u>authentication status of user</u> [47].

---

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

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

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

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) using the Service_Asym_Mut_Auth_with_SM and PrK.HPC.AUT,

    (b) to create the Health Professional related Data (EF.HPD),

    (c) to create and to write the Global Data Object (EF.GDO),

    (d) to create and to write Card Authentication Private Key (PrK.HPC.AUT)

    (e) to create and to write Client-Server Authentication Private Key (Pr.HP.AUT),

    (f) to create and to write Decipher Private Key (PrK.HP.ENC),

    (g) to create, to write and to read Card Verifiable Certificates (CVC.HPC.AUT, CVC.HPC.TCE, CVC.CA_HPC.CS),

    (h) to create, to write and to read X.509 certificates (C.HP.AUT, C.HP.ENC),

    (i) to create the display message in DF.ESIGN;

2. the Card Holder is allowed

    (a) to read and to update the Health Professional related Data (EF.HPA),

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

    (c) to read the Card Verifiable Certificates (CVC.HPC.AUT, CVC.HPC.TCE, CVC.CA-HPC.CS),

    (d) to read the X.509 certificates (C.HP.AUT, C.HP.ENC),

    (e) to update the display message (DM) in DF.ESIGN,

    (f) to execute the card-to-card authentication Service_Asym_Mut_Auth_w/o_SM using PrK.HPC.AUT in security environment #1,

    (g) to execute the card-to-card authentication Service_Asym_Mut_Auth_with_SM using PrK.HPC.AUT in security environment #2,

    (h) to execute the document key decipherment Service_Data_Decryption using PrK.HP.ENC,

    (i) to execute the client-server authentication Service_Client_Server_Auth using PrK.HP.AUT,

    (j) to write the display message (DM) in DF.ESIGN;

---

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

   3.   a Terminal is allowed

      (a)   to read the Health Professional related Data (EF.HPD),

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

      (c)   to read the Card Verifiable Certificates (CVC.HPC.AUT, CVC.HPC.TCE, CVC.CA_HPC.CS),

      (d)   to read the X.509 certificates (C.HP.AUT, C.HP.ENC),

      (e)   to execute the card-to-card authentication Service_Asym_Mut_Auth_with_SM using PrK.HPC.AUT in security environment #2,

      (f)   to execute the card-to-card authentication Service_Sym_Mut_Auth_with_SM

      (g)   to read the display message (DM) after establishing secure messaging [48].

FDP_ACF.1.3   The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[49].

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 PrK.HPC.AUT,

      (b)   to execute the document key decipherment Service_Data_Decryption with PrK.HP.ENC and

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

      (d)   to read the display message (DM) in DF.ESIGN;

   2.   the Terminal is not allowed

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

      (b)   to execute the document key decipherment Service_Data_Decryption with PrK.HP.ENC and

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

      (d)   to read the display message (DM) in DF.ESIGN;

   3.   no subject is allowed

      (a)   to read any private key PrK.HPC.AUT, PrK.HP.AUT, and PrK.HP.ENC

      (b)   to update the Card Verifiable Certificates (CVC.HPC.AUT,

---

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

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

> CVC.HPC.TCE, CVC.CA_HPC.CS),
>
> (c)   to update the X.509 certificates (C.HP.AUT, C.HP.ENC),
>
> (d)   to update the Global Data Object (EF.GDO) [50].

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

138 **Application note 27:** The specification [16] describes details of the access control rules in annex B. The element FDP_ACF.1.2, access control rule 3g, is drawn form the [16], Annex B, tables B.7 and B.8, which does not require any specific key to be used to establish secure messaging.

139 **Application note 28:** According to [20] 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 HPC have such CV certificate with appropriate CHA CVC.HPC.AUT for the public key PuK.HPC.AUT and may run this authentication protocol by means of Service_Asym_Mut_Auth_w/o_SM with the private key PrK.HPC.AUT (cf. to paragraph 10). The access control of the HPC (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 11). It is important to ensure that the private key PrK.HPC.AUT, the certificate CVC.HPC.AUT and the Service_Asym_Mut_Auth_with_SM can not be misused for attacks on the authentication to eHC or SMC for gaining access to the eHC user data. On the one hand the HPC fulfils the necessary condition to prevent such attacks by the design of Service_Asym_Mut_Auth_w/o_SM and Service_Asym_Mut_Auth_with_SM of the HPC using different algorithm identifier and protocols (cf. to paragraphs 10 and 11) and the access control to these services with PrK.HPC.AUT. On the other hand the eHC and the SMC provide the related authentication (i.e. only Service_Asym_Mut_Auth_w/o_SM with CVC.HPC.AUT respective CVC.SMC.AUT as reference data) and the access control to their data as well (i.e. the user data of the eHC and the CVC.SMC.AUT with the relevant CHA).

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

141 **FDP_RIP.1 Residual Information Protection**

Hierarchical to: No other components.

---

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

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]*[51].

Dependencies: No dependencies.

142 **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 deallocation and those which can be deleted upon allocation. Note that the SSCD-PP requires to delete secret signature keys upon deallocation 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).

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

144 **FDP_SDI.2 Stored Data Integrity**

Hierarchical to: FDP_SDI.1.

FDP_SDI.2.1   The TSF shall monitor user data stored within the TSC for integrity errors [52] 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]* [53].

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[54].

Dependencies: No dependencies.

145 **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).

---

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

[52]   [assignment*: integrity errors*]

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

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

6.1.4 Inter-TSF-Transfer

146 **Application note 31**: FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1 require the TOE to protect User Data transmitted between the TOE and a remote device by secure messaging with encryption and message authentication codes after successful mutual authentication. The services Service_Sym_Mut_Auth_with_SM and Service_Sym_Mut_Auth_with_SM include authentication mechanisms with key agreement (cf. FCS_CMK.1/ASYM and FCS_CKM.1/SYM), the TDES encryption (cf. SFR FCS_COP.1/TDES) and the Retail-MAC (cf. SFR FCS_COP.1/MAC). The rules for the data transfer are defined in the security policy HCP Access Control SFP defined in the preceding section.

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

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

Hierarchical to: No other components.

FDP_UCT.1.1   The TSF shall enforce the <u>HPC Access Control SFP</u> [55] to be able to <u>transmit and receive</u>[56] 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]

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

150 **FDP_UIT.1 Data exchange integrity**

Hierarchical to: No other components.

FDP_UIT.1.1   The TSF shall enforce the <u>HPC Access Control SFP</u> [57] to be able to <u>transmit and receive</u> [58] user data in a manner protected from <u>modification, deletion, insertion and replay</u> [59] errors.

FDP_UIT.1.2   The TSF shall be able to determine on receipt of user data, whether <u>modification, deletion, insertion and replay</u> [60] has occurred.

---

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

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

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

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

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

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

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]

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

152 **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 <u>the remote trusted IT product</u> [61] to initiate communication via the trusted channel.

FTP_ITC.1.3   The TSF shall initiate communication via the trusted channel for <u>commands and responses after successful card-to-card authentication with algorithm '1F'</u> [62].

Dependencies: No dependencies.

153 **Application note 32:** The specification [15], 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 SMC) may initiate the trusted channel using Service_Sym_Mut_Auth_with_SM. This does not change the security status of the HPC 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). The TOE allows the SMC to read the display message only through such trusted channel. 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. [15], Annex C.2).

6.1.5   Security Management

154 **Application note 33**: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

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

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

Hierarchical to: No other components.

---

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

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

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

    1.   Initialization,

    2.   Personalization,

    3.   Card Management,

    4.   Modification of the PIN [63].

Hierarchical to: No other components

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

158 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, SMC [64].

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

Hierarchical to: FIA_UID.1 Timing of identification.

159 **Application note 34**: The Certificate Holder Authorization (CHA) Role ID are defined in [15], annex H.

160 **Application note 35**: 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.

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

162 FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1   The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks [65].

Dependencies: FMT_LIM.2 Limited availability.

---

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

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

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

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

164 **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 [66].

Dependencies: FMT_LIM.1 Limited capabilities.

165 **Application note 36**: 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.

166 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.

167 **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 [67] the Initialization Data and Pre-personalization Data [68] to the Manufacture [69].

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

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

Hierarchical to: No other components.

---

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

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

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

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

FMT_MTD.1.1/   The TSF shall restrict the ability to write [70] the
RAD_WR
> 1. User Authentication Reference Data, and
>
> 2. public keys of the root for CV certificate verification [71]
>
> to the Card Management System [72].

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/   The TSF shall restrict the ability to modify [73] the public keys of the root
RAD_MOD   for CV certificate verification [74] to Card Management System [75].

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/   The TSF shall restrict the ability to modify and unblock [76] the PIN [77] to the
PIN   Card Holder [78].

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

171 **Application note 37**: 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 [16] does not describe detailed access conditions for the public keys because their

---

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

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

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

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

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

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

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

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

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

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).

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

Hierarchical to: No other components.

FMT_MTD.1.1/   The TSF shall restrict the ability to <u>read</u> [79] the <u>PIN and PUC</u> [80] to <u>none</u> [81].
RAD_CH

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

6.1.6   SFR for TSF Protection

173 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.

174 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. <u>PIN and PUC</u>[82]

and

2. <u>Card Authentication Private Keys</u>,

---

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

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

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

3. Client-Sever Authentication Private Key,

4. Document Cipher Key Decipher Key,

5. secure messaging keys [83].

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

1. PIN and PUC[86]

and

2. Card Authentication Private Key,

3. Client-Sever Authentication Private Key,

4. Document Cipher Key Decipher Key,

5. secure messaging keys [87].

Dependencies: No other components.

175 **Application note 38**: 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 HPC / SMC has to provide a smart card interface with contacts according to ISO/IEC 7816-2 [15] but the integrated circuit may have additional contacts or a contactless interface as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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

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

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

Hierarchical to: No other components.

FPT_FLS.1.1   The TSF shall preserve a secure state when the following types of failures occur:
1. exposure to operating conditions where therefore a malfunction could occur,

---

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

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

84   [assignment: *type of users*]

85   [assignment: *type of connection*]

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

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

2. failure detected by TSF according to FPT_TST.1 [88].

Dependencies: ADV_SPM.1 Informal TOE security policy model

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

180 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

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

Dependencies: No dependencies.

181 **Application note 39**: 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.

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

183 FPT_TST.1 TSF testing

Hierarchical to: No other components.

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

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

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

Dependencies: FPT_AMT.1 Abstract machine testing.

184 **Application note 40**: If HPC chip uses state of the art smart card technology it will run the some self tests at the request of the authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the "authorised user" Manufacture in the Phase 2 Manufacturing. Other self tests may run automatically to detect failure and to preserve of secure

---

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

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

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

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.

185 The following security functional requirements support the separation and the non-bypassability of TSF.

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

187 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.

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

189 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.

190 **Application note 41**: Those parts of the TOE which support the security functional requirements "TSF testing (FPT_TST.1)" and "Failure with preservation of secure state (FPT_FLS.1)" shall be protected from interference of the other security enforcing parts of the HPC chip Embedded Software. The security enforcing functions and health application data shall be separated in a way preventing any interference.

6.2   Security Assurance Requirements for the TOE

191 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.

192 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

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

7 Rationale

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-	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.HPC_Spec	x	x	x	x	x						x	x	
OSP.Manufact										x	x		
A.Pers_Agent												x	
A.Users													x

Table 1: Security Objective Rationale

194 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.

195 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.

196 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 administration" 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.

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

"Compliance to HPC specifications" and the security objective for the TOE environment **OE.Users** "Adequate usage of TOE and IT-Systems" the external application decides whether the 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 [15]) 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.

198 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.

199 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.

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

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

202 The organizational security policy **OSP.HPC_Spec** "Compliance to HPC specifications" is implemented by the TOE security objectives **OT.AC_Pers** "Access control for personalization and administration", **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". 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 [15] referenced in the OSP.HPC_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 [15] to the card holder.

203 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 security policy **OSP.Manufact** "Manufacturing of the Smart Card" in the development and manufacturing of the TOE.

204 The security objectives for the environment **OE.Perso** "Secure personalization and management" implements the assumption **A.Pers_Agent** "Personalization and management of the Smart Card" with respect of the concrete user and TSF data described in the specification [15] (cf. to OSP.HPC_Spec).

205 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

206 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.

207 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[12]. 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.

7.2.1 Security Functional Requirements Coverage

208 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/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.2				x					
FDP_UCT.1					x				
FDP_UIT.1					x				
FTP_ITC.1					x				
FMT_SMF.1	x	x							
FMT_SMR.1	x	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_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 Functional Requirements Sufficiency

209 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 personalization 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.

210 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_CKM.1/ASYM**, **FCS_CKM.4**, **FCS_COP.1/CCA_SIGN**, **FCS_COP.1/CCA_VERIF**, **FCS_RND.1**, **FCS_COP.1/TDES**, **FCS_COP.1/MAC, FIA_UAU.4** and **FIA_UAU.6**.

(iii) the TOE security service Service_Sym_Mut_Auth_with_SM is implemented by the SFR **FCS_CKM.1/SYM**, **FCS_CKM.4**, **FCS_RND.1**, **FCS_COP.1/TDES**, **FCS_COP.1/MAC, FIA_UAU.4** and **FIA_UAU.6**.

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

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

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** 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),

(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.

211 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 **FMT_MTD.1/INI, FMT_MTD.1/PIN, FMT_MTD.1/RAD_WR** and **FMT_MTD.1/RAD_MOD** protect the integrity of TSF data and therefore support the TSF to protect the confidentiality of the user data,

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

(iv)   the SFR **FDP_ACC.1** and **FDP_ACF.1** (cf. FDP_ACF.1.2, rule 4a, and FDP_ACF.1.4, role 1d and 2d) ensure that only corresponding SMC may read the DM in DF.ESIGN,

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

(vi)   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.

212 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.2** 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.

213 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 for secure messaging,

(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.

214 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.

215 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.

216 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.

217 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], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, FCS_COP.1, justification 1 for non-satisfied dependencies
FCS_CKM.1/SYM	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, FCS_COP.1, justification 1 for non-satisfied dependencies
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes	FCS_CKM.1, justification 1 for non-satisfied dependencies
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	justification 2 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
	FMT_MSA.2 Secure security attributes	
FCS_COP.1/CCA_SIGN	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes	justification 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] FCS_CKM.4 Cryptographic key destruction 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] FCS_CKM.4 Cryptographic key destruction 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 security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes	justification 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] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 1 for non-satisfied dependencies
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key	FCS_CKM.1, FCS_CKM.4, justification 1 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
	destruction FMT_MSA.2 Secure security attributes	
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
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

SFR	Dependencies	Support of the Dependencies
FMT_MTD.1/RAD_WR	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/RAD_MOD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	ADV_SPM.1	fulfilled by EAL4
FPT_PHP.3	No dependencies	n.a.
FPT_RVM.1	No dependencies	n.a.
FPT_SEP.1	No dependencies	n.a.
FPT_TST.1	FPT_AMT.1 Abstract machine testing	See justification 5 for non-satisfied dependencies

Table 6: Dependency rationale overview

218 Justification for non-satisfied dependencies:

No. 1: The TSF according to SFR FCS_CKM.1/ASYM, FCS_CKM.1/SYM 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 32).

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 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

219 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.

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

221 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.

222 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 Security Objectives for the TOE, especially OT.Data_Confident and OT.Prot_Phys-Tamper). Therefore the component AVA_VLA.4 was included to meet the security objectives.

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

224 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.

225 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.

226 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

227 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.

228 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.

229 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 HPC 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.

230 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).
Health Employee	Special case of a HPC with

Term	Definition
Card	
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
CA	Certification authority
CC	Common Criteria
CSP	Certification service provider
CVC.CA_NN_HPC.CS	Certificate of the Certificate Service Provider for card verifiable certificates in the health care environment
CVC.HPC.AUT	Certificate of the public key PuK.HPC.AUT corresponding to the private

Acronyms	Term
	key PrK.HPC.AUT of the HPC
eHC	Electronic health card
HPC	Health professional card
PIN.CH	Global PIN of human user authentication for all HPC security services except the application for qualified signature
PrK.HP.AUT	Private key for client-server authentication
PrK.HP.ENC	Private key to decipher document encryption keys
PrK.HPC.AUT	Private key for card-to-card authentication between TOE and external SMC or eHC
PuK.CA_NN_HPC.CS	Public Key of the Certificate Service Provider for card verifiable certificates in the health care environment
PUC.CH	Reset code for PIN.CH
PuK.RCA.CS	Root public key for verification of the card verifiable certificate of the certificate service provide for card verifiable certificates in the health care environment
SAR	Security assurance requirements
SE#1	Security environment #1 communicating without secure messing
SE#2	Security environment #2 communicating with secure messing
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, 2.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]   ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004

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

Protection Profiles

[12]   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

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

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

Other

[15]   Specification German Health Professional Card and Security Module Card - Pharmacist & Physician – Part 1: Commands, Algorithms and Functions of the COS Platform, Version 2.1

draft, 07.11.2005, Bundesärztekammer, Kassenärztliche Bundesvereinigung, Bundeszahnärztekammer, Bundespsychotherapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Deutsche Krankenhaus-Gesellschaft

[16] 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, Bundespsychotherapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Deutsche Krankenhaus-Gesellschaft

[17] 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, Bundespsychotherapeutenkammer, Kassenzahnärztliche Bundesvereinigung, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Deutsche Krankenhaus-Gesellschaft

[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] 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)

[21] Verordnung zur elektronischen Signatur, 16. November 2001, BGBl I 2001, 3074

[22] Gesetz über Rahmenbedingungen für elektronische Signaturen, 16. Mai 2001,: BGBl I 2001, 876

[23] Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, EAL 4+, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference PP-BSI-0005-2002

[24] Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.04, EAL 4+, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference PP-BSI-0006-2002

[25] COMMISSION DECISION of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council (notified under document number C(2003) 2439)
http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf

[26] CEN CWA14890-1 Application Interface for SmartCards used as Secure Signature Creation Devices Part 1 – Basic Requirements, March 8th 2004

9   Informative Annex: HPC as SSCD

9.1   Requirements

The HPC will be used as secure signature-creation device (SSCD) for qualified signatures according to the German signature law (SigG) [22]. Therefore the HPC specification [15] defines a electronic signature application. The German signature ordinance (SigV) [21] requires to certify a secure signature-creation device according to ITSEC on level E3 high or Common Criteria on EAL4 where "evaluations shall be conducted against a high attack potential and a full misuse analysis shall be carried out". The evaluation of a HPC as secure signature-creation device may be performed in different ways:

Case 1:   A smart card already assessed as secure signature-creation device may be evaluated and certified against a security target conform to the current protection profile HPC (PP HPC) where the both the HPC application and the signature application shall fulfill the specification [15]. The evaluation as SSCD may be performed according to ITSEC or Common Criteria.

Case 2:   A smart card may be certified based on a security target (ST) which is conform to the PP HPC and includes additional security functional requirements to get the security assessment as secure signature-creation device. Note that the PP HPC already include the security assurance requirements as defined by the SigV (i.e. EAL4 augmented with AVA_MSU.3 and AVA_VLA.4).

Case 3:   As special sub-case of the case 2 the ST may claim the compliance to the PP HPC and one (or both) of the PP, the BSI-PP-0005-2002 (for SSCD Type 2) [**Fehler! Textmarke nicht definiert.**] or BSI-PP-0006-2002 (for SSCD Type 3) [**Fehler! Textmarke nicht definiert.**]. The conformance to one of the later protection profile provides some certainty based on [25] that the certificate will meet the requirements to get the assessment as secure signature-creation device.

This informative annex guides the security target writer to combine the PP HPC with one or both PP for the SSCD.

9.2   ST conformant to PP HPC and SSCD

9.2.1   PP conformance

The Common Criteria parts 1 [1] and 2 [3] describe how a security target may claim conformance to one or more protection profiles. The rules for a compliance claim may be summarized as follows (for details refer to [1], sections 5.1.3 and A.2.8, and [3], section 5.5, assurance component ASE_PPC.1):

(1)   The developer shall provide any PP claims as part of the ST (cf. ASE_PPC.1.1D) and each PP claim shall identify the PP for which compliance is being claimed, including qualifications needed for that claim (cf. ASE_PPC.1.1C).

(2)   The ST includes all security objectives for the TOE contained in the PP for which compliance is being claimed.

(3) The ST includes all security functional requirements for the TOE (or their hierarchical components) contained in the PP for which compliance is being claimed where all operations shall be performed or completed.

(4) The ST includes all security assurance requirements or their hierarchical components. The ST may require additional security assurance requirements.

(5) The ST may include additional security functional and assurance requirements which must not weaken or contradict the security requirements of the PP.

The developer shall provide the PP claims rationale for each provided PP claim (cf. ASE_PPC.1.2D).

The following section discuss how a ST may be written claiming compliance to the PP HPC and one (or both) of the PP SSCD, the BSI-PP-0005-2002 or BSI-PP-0006-2002. The security writer should pay intention to the technology independence of the BSI-PP-0005-2002 and BSI-PP-0006-2002 (cf. chapter 2 of [**Fehler! Textmarke nicht definiert.**] and [**Fehler! Textmarke nicht definiert.**]) and smart card specific descriptions of the current PP HPC. These approaches result in different text of similar security objectives or security requirements.

9.2.2   Security Objectives

The ST claiming compliance to the PP HPC and one (or both) of the PP SSCD (i.e. the BSI-PP-0005-2002 or BSI-PP-0006-2002) shall include all security objectives of the respective PPs. Note, these PP contain similar security objectives which should be stated in parallel because the address different assets. Some of them may be combined if appropriate rationale is given.

The security objectives OT.AC_Pers in the PP HPC and the security objectives OT.Lifecycle and OT.Init in the PP SSCD address the security of the initialization and personalization of the TOE. The OT.AC_Pers, OT.Lifecycle and OT.Init limit personalization to authorized users but relates to different data. The HPC specification does not allow any modification of the card holders personal data. The PP SSCD allows for safe destruction of the signature-creation data (SCD) which end the SSCD life cycle. The SCD may be re-generated starting a new life cycle.

The security objectives OT.Data_Confident in the PP HPC and OT.SCD_Secrecy in the PP SSCD address the confidentiality of TOE secrets. OT.Data_Confident cover all confidential user and TSF data including the listed authentication data and keys where OT.SCD_Secrecy is specific for the signature application (focusing on SCD).

The security objectives OT.Trusted_Channel, OT.DTBS_Integrity_TOE and OT.SVD_Auth_TOE address the protection of user data different in respect of (i) the security features (OT.Trusted_Channel: confidentiality and integrity, OT.DTBS_Integrity_TOE: integrity only, OT.SVD_Auth_TOE: authenticity), (ii) the protected objects (OT.Trusted_Channel: controlled by the external application, OT.DTBS_Integrity_TOE: DTBS imported by the TOE, OT.SVD_Auth_TOE: exported SVD), (iii) rigour of usage (OT.Trusted_Channel: on demand of the external application, OT.DTBS_Integrity_TOE: mandatory for DTBS, OT.SVD_Auth_TOE: mandatory for the SVD).

The security objectives OT.AC_Serv in the PP HPC, OT_Access_rights and OT.Services in the PP eHC and OT.Sigy_SigF in the PP SSCD require access control on the function respective objects provided by the application for the card holder. They are very similar and result in different access control SFP implemented by FDP_ACC and FDP_ACF components.

The security objectives OT.Prot_Inf_Leak and OT.EMSEC_Design are more specific in the attacks (i.e. information leakage through side channels) and extend the protection to any secret data. The security objective OT.Data_Integrity of the PP HPC has not direct equivalent in the PP SSCD. The security objectives OT.Prot_Phys_Tamper in the PP HPC and OT.Tamper_Resistance in the PP SSCD require resistance against physical tampering. The security objective OT.Tamper_ID for the SSCD describe an other aspect of physical protection – the detection of physical manipulation by a user (e.g. by specific ATR indicating permanent blocking state due to physical manipulation). The security objectives OT.Prot_Abuse_Func and OT.Prot_Malfunction address in more details obvious vulnerabilities of smart cards which are also relevant for SSCD if implemented in form of a smart card. Note that the PP SSCD was written in a technology independent

The security objectives OT.SCD_SVD_Corresp, OT.Sig_Secure and OT.SCD_Unique are specific security features of the signature-creation and key generation function of the SSCD. These security objectives of the PP SSCD has not direct equivalent in the PP HPC or PP eHC.

9.2.3   Security Functional Requirements

The ST shall include all security functional requirements (SFR) of all PP for which compliance is being claimed. The protection profiles HPC, eHC and SSCD define almost all SFR with performed operation. The ST writer shall perform all operation which are not performed already in these PP. The instantiations of the SFR components either address different security features of the TOE or describe the same security features in a consistent way.

The ST writer should be aware of the different roles and identities handled by the TOE (cf. FMT_SMR.1 of the respective PP):

- The PP SSCD maintain roles Administrator and Signatory.

- The PP HPC maintain the roles Manufacture, Card Management System, Card Holder and Terminals.

Note that the roles Card Holder and Signatory will be assigned to the same person but in different context:

- The user authenticated for the role Card Holder may use the health application but the can not use the signature-creation data (SCD) in the signature application.

- The user authenticated for the role Signatory may use the SCD in the signature application but the can not use the health application.

- The ST shall define different authentication reference data for both roles. The values of these authentication reference data may be chosen independent on each other. This is a result of the German signature ordinance and their technical interpretation given by Bundesnetzagentur.

The instantiations of components of the families FDP_ACC, FDP_ACF, FDP_UCT and FDP_UIT of the PP HPC, eHC and SSCD enforce different security functional policies defined for different subjects, objects and operations:

- the Personalisation SFP, the Signature-creation SFP and SVD Export SFP for SSCD Type 2 and 3, where the SCD Import SFP is enforced in case of SSCD Type 2 and the Initialisation SFP is enforced in case of SSCD Type 3 only,

- the PP HPC enforces the HPC Access Control SFP,

- the PP eHC enforces the SFP access rules defined in the security objective OT.Access_Rigths.

Note that the PP SSCD, HPC and eHC require the TOE to provide trusted channel to remote trusted products. The smart card specific PP HPC and eHC assume to use secure messaging as mechanism to establish the trusted channel. The PP SSCD as being technology independent does not require the TOE to use mechanisms secure messaging.

The instantiations SFR components of the class FCS address different cryptographic mechanisms. Note that the PP HPC and eHC use the digital signature-creation for card-to-card authentication and the client-server-authentication where the PP SSCD address the digital signature-creation for electronic signature of the data to be signed (DTBS). These digital signature use specific cryptographic algorithms and keys.

The PP SSCD, HPC and eHC use slightly different approach to describe the TSF protection.

The instantiation of the SFR FPT_EMSEC.1 TOE emanation are very similar in the PP SSCD, PP HPC and PP eHC:

- they are not operated in respect of the types and limits of emanation,

- they list specific sets of user data and TSF data to protect, and

- only the PP HPC and eHC specify the smart card circuit interface as the interface of the connection which the ST should use for a smart card as SSCD as well.

The FPT_FLS.1 Failure with preservation of secure state is common to the PP SSCD, the PP HPC and the PP eHC where the PP SSCD does not perform the operation but the PP HPC and eHC assign the exposure of operating condition and the failure detected by self tests. Thus the ST writer may use the list of failure defined in the PP HPC and eHC or may add other failure in which the TOE preserve a secure state.

The SFR FPT_AMT.1 Abstract machine testing is used in PP SSCD only and is missing in the PP HPC and eHC. The PP SSCD include the component FPT_AMT.1 because the TOE may be hardware or software implementing the SCD. E.g. the TOE may include the hardware cave implementing the SFR FPT_PHP.3 for physical protection but may not include all computer hardware inside this cave. In case of a smart card the ST will

- on the one hand define the TOE as smart card i.e. consisting of all the hardware, the software and the health application and the signature-creation application and

- on the other hand require abstract machine testing i.e. the TSF to perform testing to demonstrate the security assumptions made about the underlying abstract machine upon which the TSF relies.

In case of a smart card a test of the arithmetic coprocessor may be seen form the software part of the TOE view as test of the "underlying abstract machine" and form the hardware part of the TOE as self test (normally described by means of the SFR FPT_TST.1). Thus the ST writer should explain that the self tests of the hardware platform on which the software is running fulfil the SFR FPT_AMT.1 even if the "underlying abstract machine" is part of the TOE.

9.2.4   Security Assurance Requirements

The ST compliant with the PP SSCD and one of the PP HPC or eHC will include at least

- the assurance package EAL4 and as augmentations

- the assurance components ADV_IMP.2 contained in the PP HPC and eHC,

- the assurance components AVA_MSU.3 and AVA_VLA.4 contained in all three PP.

10   Informative Annex: Key Usage Counter for C2C-Authentication Keys

The HPC specification [15], sec. Annex F, and [16], sec. 5.3, defines a usage counter for C2C-authentication keys which is not mandatory currently for all HPC but may be mandatory in the future. Therefore this security feature is not described as mandatory in the protection profile. This informal annex advice the security target writer how to supplement the security target if the usage counter is supported by the TOE.

The security target writer should

- introduce the key usage counter as security attribute of the asset Card Authentication Private Keys PrK.HPC.AUT,

- introduce the subject card management system

- add the threat OSP.Limit_Usage,

- the security objective OT.Limited_Key_Usage, and

- the security functional requirements.

PrK.HPC.AUT has the security attribute "key usage counter" which counts the number of left allowed usage of this key and is managed by card management system. The security attribute "key usage counter" has a default value to which it is reset after successful authentication of the card management system. The card management system as user of the TOE is allowed to reset the usage counter of PrK.HPC.AUT only.

The card management system is allowed to reset the key usage counter of PrK.HPC.AUT. This user authenticates themselves using PrK.HPC.AUT_ADMIN and the HPC uses the CVC.CAMS_HPC.AUTto verify the authentication attempt.

The ST writer should define an organisational security policy like this:

OSP.Limit_Usage   Limitation of HPC usage

The HPC card management system controls the usage of the HPC for access to the eHC. The card management system authorizes a valid HPC after mutual authentication to perform only a limited number of authentication sessions with eHC and SMC.

Application note 42: The access to some specific eHC user data requires of a health professional. The health professional authenticates themselves to the HPC by knowledge of a PIN for access to an C2C authentication function with the eHC. The HPC performs the card-to-card authentication with the key PrK.HPC.AUT (to) open directly the eHC for access to the specific user data, or (ii) to authorize a SMC to open the eHC for access to the specific user data.

The ST writer should define an organisational security policy like this:

OT.Limited_Key_Usage   **Limitation of the C2C-Authentication Key**

The TOE shall control the number of Card-to-card authentication attempts to an eHC or a SMC for authorization to an eHC. The TOE shall allow only a pre-defined number of key usage between successful authentication of the card management system.

The ST writer should define security functional requirements like listed below.

FIA_AFL.1/C2C Authentication failure handling – C2C authentication

Hierarchical to: No other components.

FIA_AFL.1.1/C2C   The TSF shall detect when [selection*: [assignment: positive integer number], "an administrator configurable positive integer within [assignment: range of acceptable values]"*] successful or [91] unsuccessful authentication attempts occur related to key usage of the PrK.HPC.AUT [92].

FIA_AFL.1.2/C2C   When the defined number of successful or [93] unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions, which at least includes: block the PrK.HPC.AUT*][94].

Dependencies: FIA_UAU.1 Timing of authentication

Application note 43: The component FIA_AFL.1/C2C addresses the usage of the private key PrK.HPC_AUT for mutual card-2-card authentication (cf. FIA_UAU.4) by means of Service_Asym_Mut_Auth_w/o_SM in SE#1. The number of successful or unsuccessful authentication attempts occur related to usage of the PrK.HPC.AUT are stored in the security attribute "key usage counter" of PrK.HPC.AUT. The private key PrK.HPC.AUT is used to authenticate the TOE to the eHC or SMC. The reference data used by the eHC or SMC is the card verifiable certificate CVC.HPC.AUT which contain the HPC relevant access rights. The ST writer shall perform the missing operation in the components FIA_AFL.1.1/C2C and FIA_AFL.1.2/C2C.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

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

1. Initialization,

2. Personalization,

---

[91]   refinement: not only unsuccessful but also successful attempts shall be counted here – obviously this refinement is valid, because the original requirement is still fulfilled

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

[93]   refinement: not only unsuccessful but also successful attempts shall be counted here – obviously this refinement is valid, because the original requirement is still fulfilled

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

3. <u>Modification of the PIN</u>

4. <u>unblocking the PrK.HPC.AUT</u> [95].

Dependencies: No Dependencies

Application note 44: Clause 4 in the component FMT_SMF.1.1 is an extension to the component defined in paragraph 156 this protection profile.

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1   The TSF shall maintain the roles <u>Manufacture, Card Management System, Card Holder, Terminals and card management system</u> [96].

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

Hierarchical to: FIA_UID.1 Timing of identification

Application note 45: The text "and card management system" in the component FMT_SMR.1.1 is an extension to the component defined in paragraph 158 this protection profile.

FMT_MTD.1/C2C   Management of TSF data – Protection of Human User

Authentication Data

Hierarchical to: No other components.

FMT_MTD.1.1/   The TSF shall restrict the ability to <u>reset to</u> *[assignment: default value]* [97]
C2C   the <u>key usage counter of PrK.HPC.AUT</u> [98] to <u>card management system</u> [99].

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

Application note 46: The key usage counter of PrK.HPC.AUT addressed in the component FMT_MTD.1.1/CVC is defined in . The ST writer shall perform the missing operation to define the number of C2C-Authentication after reset of the key usage counter of PrK.HPC.AUT in the component FMT_MTD.1.1/CVC.

The ST writer using the security organisational policy OSP.Limit_Usage, the security policy OT.Limited_Key_Usage and the SFR FIA_AFL.1/C2C, FMT_SMF.1, FMT_SMR.1 and FMT_MTD.1/C2C as shown above may provide easily the appropriate rationale for

---

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

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

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

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

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

- OT.Limited_Key_Usage covering OSP.Limit_Usage, and

- FIA_AFL.1/C2C, FMT_SMF.1, FMT_SMR.1 and FMT_MTD.1/C2C implementing OT.Limited_Key_Usage.

The dependencies of the new components introduced above are obviously fulfilled.