Security Target Lite
STARCOS 3.2 eGK V1.0

Version 1.1 / Stand 20.11.2007

F&E

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

© Copyright 2007
Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München

This document as well as the information or material contained is copyrighted. Any use not explicitly permitted by copyright law requires prior consent of Giesecke & Devrient GmbH. This applies to any reproduction, revision, translation, storage on microfilm as well as its import and processing in electronical systems, in particular.

The information or material contained in this document is property of Giesecke & Devrient GmbH and any recipient of this document shall not disclose or divulge, directly or indirectly, this document or the information or material contained herein without the prior written consent of Giesecke & Devrient GmbH. All copyrights, trademarks, patents and other rights in connection herewith are expressly reserved to the Giesecke & Devrient group of companies and no license is created hereby.

Subject to technical changes.
All brand or product names mentioned are trademarks or registered trademarks of their respective holders.

Inhalt

1 Introduction 5
1.1 ST Identification 5
1.2 ST Overview 5
1.3 CC Conformance 6
1.4 Overview 6
1.5 Application Notes of the PP 7
1.6 Editorial refinements 7

2 TOE Description 9
2.1 Product Type 9
2.1.1 TOE definition 9
2.1.2 TOE usage and security features for operational use 11
2.1.3 TOE life cycle 14

3 TOE Security Environment 18
3.1 Introduction 18
3.1.1 Assets 18
3.1.2 Subjects 20
3.2 Organizational Security Policies 21
3.3 Threats 24
3.3.1 Threats mainly addressing TOE_ES and TOE_APP 24
3.3.2 Threats mainly addressing TOE_ES and TOE_IC 25
3.4 Assumptions 27

4 Security Objectives 28
4.1 Security Objectives for the TOE 28
4.1.1 Security objectives, which are mainly TOE_App oriented 28
4.1.2 Security Objectives, which are mainly TOE_ES oriented 31
4.1.3 Security Objectives, which are mainly TOE_IC oriented 32
4.2 Security Objectives for the Development and Manufacturing Environment 34
4.3 Security Objectives for the Operational Environment 35

5 Extended Components Definition 38
5.1 Definition of the Family FCS_RND 38
5.2 Definition of the Family FMT_LIM 38
5.3 Definition of the Family FPT_EMSEC 40

6 Security Requirements 42
6.1 TOE Security Functional Requirements 43
6.1.1 Cryptographic support (FCS) 43
6.1.2 Identification and Authentication 49
6.1.3 Access Control 55
6.1.4 Security Management 61
6.1.5 General Security Functions 66
6.2 Security Assurance Requirements for the TOE 70
6.3 Security Requirements for the IT environment 70

7 TOE Summary Specification 71

7.1 TOE Security Functions 71
7.1.1 SF.ACCESS Access Control 71
7.1.2 SF.ADMIN Administration of the TOE 77
7.1.3 SF.AUTH Authentication of the Cardholder 77
7.1.4 SF.CRYPTO Cryptographic Support 78
7.1.5 SF.TRUST Authentication and Trusted Communication 79
7.1.6 SF.PROTECTION Protection of TSC 79
7.1.7 SF.IC_SF Security Functions of the IC 80
7.2 Assurance Measures 81
8 PP Claims 82
8.1 PP Reference 82
9 Rationale 83
9.1 Security Objectives Rationale 83
9.2 Security Requirements Rationale 87
9.2.1 Security Functional Requirements Coverage 87
9.2.2 Functional Requirements Sufficiency 88
9.2.3 Dependency Rationale 93
9.2.4 Rationale for the Assurance Requirements 96
9.2.5 Security Requirements – Mutual Support and Internal Consistency 98
9.3 Rationale for TOE Summary Specification 99
9.3.1 Rationale for TOE Security Functions 99
9.3.2 Rationale for Assurance Measures 107
9.3.3 Rationale for Strength of Function High 107
10 Conventions and Terminology 109
10.1 Glossary 109
10.2 Acronyms 110
11 References 112

1 Introduction

1.1 ST Identification

Title: Security Target Lite of STARCOS 3.2 eGK V.1.0

Version Number/Date: Version 1.1 /Status 20.11.2007

Origin: Giesecke & Devrient GmbH

Compliant to:

- Common Criteria Protection Profile, electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK), BSI-PP-0020-V2-2007, version 2.00, 29th January 2007, Bundesamt für Sicherheit in der Informationstechnik.

TOE name: STARCOS 3.2 eGK

TOE version: 1.0

TOE documentation:

- Administrator Guidance,
- User Guidance,
- Generic Application – Security Relevant Sections,
- Installation, generation and start-up.

HW-Part of TOE: Infineon SLE66CX680PE certified according to Common Criteria (Cert ID: BSI-DSZ-CC-0322-2005-MA-04).

1.2 ST Overview

The aim of this document is to describe the Security Target for the electronic health card (eHC) / elektronische Gesundheitskarte (eGK) based on the OS STARCOS 3.2. The eHC is a contact based smart card with applications for the German health system according to “Gesetz zur Modernisierung der Gesetzlichen Krankenversicherung” (GKV-Modernisierungsgesetz – GMG), the “Sozialgesetzbuch” (SGB) and the privacy legislation (“Datenschutzgesetze des Bundes und der Länder”). The eHC is based on the Integrated Circuit (IC) from Infineon (SLE66CX680PE). The eHC is based on the specification of the eGK [7], [8]. This ST does not cover the requirements of the qualified electronic signature (QES) application as this is part of a separate Common Criteria evaluation.

The eHC will be used by the cardholder, who might be a patient or the insured person or both.

STARCOS 3.2 is a fully interoperable ISO 7816 compliant multiapplication Smart Card OS, including a cryptographic library.

This document describes

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

The assurance level for the TOE is CC **EAL4** augmented with **ADV_IMP.2, AVA_MSU.3** and **AVA_VLA.4**

The minimum strength level for the TOE security functions is **high** (SOF high).

1.3 CC Conformance

This ST claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, August 2005, version 2.3, CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Introduction and general model, August 2005, version 2.3, CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, August 2005, version 2.3, CCMB-2005-08-003

as follows

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

The minimum strength level for the TOE security functions is **SOF high**.

1.4 Overview

Chapter 1 provides the introductory material for the Security Target.

Chapter 2 provides general purpose and TOE description.

Chapter 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Chapter 4 defines the security objectives for both the TOE and the TOE environment.

Chapter 5 defines components defined as extensions to the CC part 2 [2].

Chapter 6 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [2] and Part 3 [3], that must be satisfied.

Chapter 7 contains the TOE Summary Specification.

Chapter 8 provides the compliance claims to Protection Profiles .

Chapter 9 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective.

Chapter 10 provides information on applied conventions and used terminology as well as acronyms.

Chapter 11 identifies background material (reference section).

1.5 Application Notes of the PP

All application notes of the PP are discussed in ‘Note of the ST-author’ in this document.

There are different types of application notes in the PP. Some application notes in the PP are specifying actions to be taken by the ST-author. In such cases the ‘Note of the ST-author’ describes, how this has been applied in the ST. In other cases the application notes in the PP give additional information to better understand the PP. In this cases the note of the ST-author cover this information, so it is available to the ST reader to better understand the ST.

1.6 Editorial refinements

Editorial changes according to the PP will be described in the table below, if not otherwise marked in the ST itself:

chapter / item eGK-PP	mistake	chapter / item eGK-ST	corrected version
5.1.3 SFR FDP_ACC.2	FDP_ACC.2.1 has been used twice instead of FDP_ACC.2.1 and FDP_ACC.2.2.	6.1.3 SFR FDP_ACC.2	FDP_ACC.2.1 changed to FDP_ACC.2.2.

2 TOE Description

2.1 Product Type

The TOE is compliant to the requirements of the Protection Profile of the electronic Health Card [28].

2.1.1 TOE definition

The Target of Evaluation (TOE) is a smart card, the electronic Health Card (eHC), which is based on the specification documents [7] and [8].

The size of the card is type ID-1 according to ISO 7810 (the usual credit-card-size).

The card is a card with contacts according to ISO 7816-1 to –3. If it has an additional contact less interface, none of the eHC functions shall be accessible via this interface.

The overall system including the TOE and its environment are intended to comply to the relevant German legal regulations, in particular the “Gesetz zur Modernisierung der Gesetzlichen Krankenversicherung” (GKV-Modernisierungsgesetz – GMG), the “Sozialgesetzbuch” (SGB) and the privacy legislation (“Datenschutzgesetze des Bundes und der Länder”).

The TOE comprises the following parts

TOE_IC, consisting of :

- the circuitry of the eHC’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 eHC applications (data structures and their content)

and

guidance documentation (see ‘TOE documentation’ in § 1.1) delivered together with the TOE.

The **TOE_IC** is the TOE from the chip evaluation of the SLE66CX680PE (Cert ID: BSI-DSZ-CC-0322-2005-MA-04) performed by the IC manufacturer Infineon. In this evaluation, which is a ‘composite evaluation’, the TOE_IC evaluation results from Infineon will be used. The TOE_IC is well described in the Security Target of the chip evaluation [HW ST SLE66]. It comprises of chip HW and firmware. The chip HW of TOE_IC includes: Security logic, Microcontroller type ECO 2000 (CPU) with the

subcomponents memory encryption and decryption unit, memory management unit and 256 bytes of internal RAM, Memory Control Unit, external memory (comprising XRAM, ROM, including the routines for chip management, test ROM containing the test routines, and a total of 68 kBytes non-volatile memory (EEPROM) with error detection and error correction). In addition the TOE_IC HW comprises of a true random number generator, Checksum module, Interrupt module, Input Logic, Timer, address and data bus, SFR bus, Memory bus, Advanced Crypto Engine, DES accelerator and extended SFR registers.

The TOE_IC firmware consists of RMS routines for EEPROM programming, security functions test, and random number online testing and the Self Test Software consisting of test and initialization routines. In addition the TOE_IC firmware consists of a RSA crypto library, which will not be used in this evaluation project.

The **TOE_ES** is the operating system STARCOS 3.2 from Giesecke & Devrient and is implemented in the ROM area of the chip hardware.

The **TOE_APP** is implemented as a file system containing the Applications according to the security relevant parameters defined in [7] and [8] and is installed in the EEPROM of the IC and the underlying IC itself (see Figure 1). Parts of the operating system may also reside in the EEPROM.

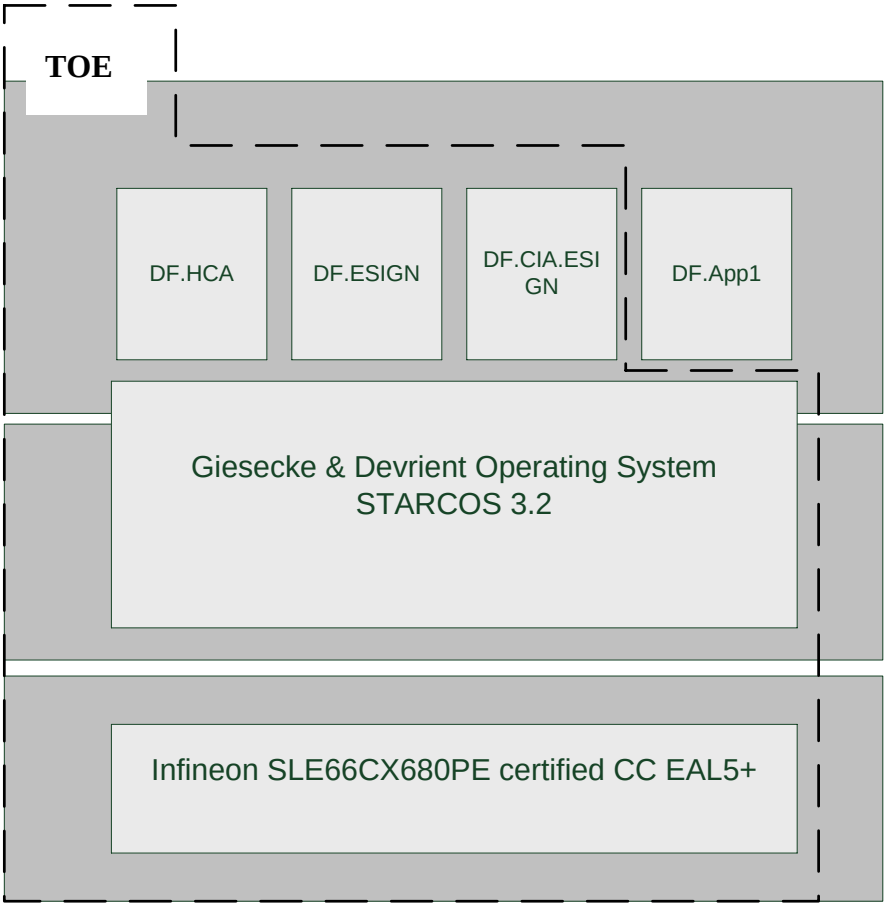

Figure 1 TOE description

Note: The short terms TOE_IC, TOE_ES and TOE_APP will be used were appropriate in the rest of this document in order to refer to these parts of the TOE.

2.1.2 TOE usage and security features for operational use

German health insurance companies issue electronic Health Cards to patients insured by them. The card is used by the cardholders, when they use health care services, which are covered by the insurance. A picture of the patient is printed on the card in order to support identification. The eHC contains data for

- cardholder identification,
- contractual and financial information to be exchanged between cardholder and health care provider and/or the health insurance company and
- medical data, including electronic prescriptions.

(For a more detailed definition of the assets see section 3.1.1.)

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

[7] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform, Version 1.1.0, 07.02.2006,gematik

[8] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Anwendungen und anwendugngsspezifische Strukturen, Version 1.2.1, 07.09.2006,gematik

The following list gives an overview of the main security services provided by the electronic Health Card during the usage phase. In order to refer to these services later on, short identifiers are defined:

Service_Asym_Mut_Auth_w/o_SM[1]: Mutual Authentication using asymmetric techniques between the eHC and a Health Professional Card (HPC) or a Security Module Card (SMC) without establishment of a Secure Channel ([8], section 3.5).

This service is meant for situations, where the eHC requires authentication by a HPC or SMC, but where the following data exchange is done without help of a security module.

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

Service_Asym_Mut_Auth_with_SM: Mutual Authentication using asymmetric techniques between the eHC and a Security Module Card (SMC) or another security module with establishment of a Secure Channel. ([8], section 3.6).

This service is meant for situations, where the eHC requires authentication by a SMC or another security module, which provides similar functionality, and where the following data exchange is done with the help of this security module and can therefore be encrypted and/or secured by a MAC.

Service_Sym_Mut_Auth_with_SM: Mutual Authentication using symmetric techniques between the eHC and a security module with establishment of a Secure Channel ([8] section 3.7).

This service is meant for situations, where the eHC communicates with a central security module, which shares symmetric keys with the card. This may be a security module of the health insurance organisation, when managing the patient contractual data, or a module of the Download Service Provider, which may add new applications to the eHC (or manage the existing ones).

Service_User_Auth_PIN: The cardholder authenticates himself with one of his PINs, either PIN.CH or PIN.home.

This service is meant as a support service for some of the other services, which may require user authentication. In addition it provides privacy protection because certain data in the card (or secured by the card) can only be accessed after user authentication. In particular this applies to sensitive medical data. See the specification [8], section 3.3 for PIN management.

Functions to change the PIN or to unblock the PIN, 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**.

Service_Privacy: The cardholder may deactivate sensitive medical data in the eHC. In order to use this service he authenticates himself with his PIN.home.

This service allows the cardholder to prevent health care providers from accessing data, which the cardholder doesn’t want them to know. Note, that that the name Service_Privacy doesn’t mean that this is the only privacy related service. In fact all other services also support privacy. See the specification [8], sections 4.5.2.7 and 8 for this service.

Service_Client_Server_Auth: The eHC implements a PKI application, which in particular allows using the TOE as an authentication token for an authentication of a client to a server (by means of an asymmetric method using X.509 certificates). The eHC contains two different keys and corresponding certificates for this service. For one of these keys the

cardholder authenticates himself with his PIN.home in order to access this service. The other key can be used without authentication by the cardholder but requires authentication by a HPC or SMC. See the specification [8] section 5.5 ff for this service.

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

Note, that a potential authentication of the server to the client is not supported by the eHC.

Service_Data_Decryption: The eHC implements a PKI application, which in particular allows using the TOE as a data decryption token. Symmetric document encipherment keys, which are themselves encrypted with the cards public key can only be decrypted with the help of the card. There are two sets of asymmetric key pairs in the eHC to allow the following two possibilities of authentication for this service:

- One of the key pairs require that, the cardholder authenticates himself with his PIN.home in order to access this service.
- The other key pair requires that a HPC or SMC is authenticated using Card-To-Card authentication to access this service.

This service is meant for situations, where confidential data are stored on a server, but shall only be accessible with the cardholders permission or with the authentication of a health professional . So it can also be seen as a privacy feature. See the specification [8], section 5.6 resp. 5.7. for this service.

Service_Card_Management: The eHC allows creation of new applications and management of existing applications to the card management system. This is secured by the service Service_Sym_Mut_Auth_with_SM. See the specification [8], sections 7 and 9 for this service.

Service_Logging: The eHC provides a file, which allows to store information about the fifty last accesses to medical data in the card. The card itself doesn’t control the content of these data, it is up to the authorised persons, who have write access to these data, to write them correctly. See the specification [8], section 4.1.7 and 4.9 for this service.

Note:The eHC may implement a PKI application, which in particular makes it possible to use the TOE as an electronic signature creation device for qualified signatures. The specification of requirements for this service is **not** covered by this evaluation.

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

[7] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform, Version 1.1.0, 07.02.2006,gematik

[8] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Anwendungen und anwendugngsspezifische Strukturen, Version 1.2.1, 07.09.2006,gematik

2.1.3 TOE life cycle

The following description is a short summary of the eHC 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 [26] chapter 8.

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

Phase		Description
		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 (shorter also "Card Manufacturer")** is responsible for • the initialisation of the TOE (in form of the initialisation of the modules of phase 4) and • its testing. The smartcard product finishing process comprises the embedding of the initialised modules for the TOE and the card production what may be done alternatively by the Smartcard Product Manufacturer or by his customer (e. g. Personaliser or Card Issuer)**.**
6	**Smartcard Personalisation**	The **Personaliser** is responsible for • the smartcard personalisation and • final tests. The personalization of the smart card includes the printing of the (cardholder specific) visual readable data onto the physical smart card, and the writing of (cardholder specific) TOE User Data and TSF Data into the smart card.

Phase		Description
7	**Smartcard End-usage**	The **Smartcard Issuer** is responsible for • the smartcard product delivery to the smartcard end-user (the cardholder), and the end of life process. • The authorized personalization agents (card management systems) might be allowed to add data for a new application, modify or delete an eHC application, but not to load additional executable code. Functions used for this are specifically secured functions for this usage phase (for example the require card-to-card authentication and secure messaging). This functionality doesn't imply that the card can be switched back to an earlier life cycle stage. • The TOE is used as eHC by the smart cardholder in the End-usage phase

Table 1: Smart Card Life Cycle Overview

The life-cycle phases are summarized in the table above.

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

In this ST the initialisation phase (phase 5) completely belongs to the operational use. The TOE will be delivered as hardware and as initialisation data. No modifications by a third party (e.g. the party loading the initialisation data into the hardware) is possible.

a)

Note, that this fulfils the requirements from application note 1 part a of the eHC-PP [28].

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

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

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

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

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

- TOE operational use

If the Card Management System or the card issuer load data onto the smartcard in the phase 7 Smartcard End-usage these data could only be non-executable code. There is no way to load executable code onto the TOE.

Note by the ST-author 1:

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

Both alternatives meet the following eHC-PP [28] requirements:

- All executable software in the TOE has to be covered by the evaluation. This is one of the reasons to include the assurance component ADV_IMP.2.
- The data structures and the access rights to these data as defined in the eHC specification [7], [8] are covered by the evaluation.

3 TOE Security Environment

3.1 Introduction

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

3.1.1 Assets

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

Name of asset	Description	Acronym used in eHC Specification
Personal and health insurance data (open)	Identity data or contractual data, which can be read without authentication	EF.PD, EF.VD, EF.StatusVD
Personal and health insurance data (protected)	Identity data or contractual data, which can be read only with authentication	EF.GVD
electronic prescription	A document containing one or more referrals (“Überweisungen”) or medications (“Verordnungen”). Note: The eHC itself cannot control, if an electronic prescription is valid. The eHC only serves as a trusted transport medium for prescriptions. In particular this has the consequence, that the right to write prescriptions into the eGK is not equivalent with the right to sign a prescription. Signing a prescription is an additional process done by a different card, for example the HPC.	EF.eRezept-Tickets, EF.eRezept_Container, EF.StatusRezept
VAD (eHC)	“Verification Authentication Data”: PIN codes or a resetting code entered by a cardholder to activate certain functions of the TOE. Note: These PINs are in particular not the same PIN as a PIN used for qualified electronic signatures. The electronic signature PIN is not listed as an asset in this ST (as it is not listed in the PP [28], since it is defined in a suitable Protection Profile for electronic signatures). For the same reason signing keys (PrK.CH.ES) are not listed here. Additional note by the ST-author: The eHC-PIN includes the PIN.CH and the PIN.home as described in 3.2.7 in [8].	--
RAD (eHC)	“Reference Authentication Data”: The eHC PIN and corresponding resetting code values stored in the TOE and used for comparison with the VAD entered by the cardholder. Note: Again this is not identical to similar values for an electronic signature provided by the eHC.	EF.PIN (containing PIN.CH, PIN.home and resetting code)
initialisation data	All data stored in the TOE during the initialisation process.	--
personalisation data	All data stored in the TOE during personalisation process.	--
logging data	Data stored in the TOE in order to document the last fifty accesses to medical data by care providers.	EF.Logging
Card Authentication Private Key	The Card Authentication Private Key is a asymmetric cryptographic key used for the authentication of an eHC to a HPC, to a SMC or to a service provider.	PrK.eGK.AUT

Name of asset	Description	Acronym used in eHC Specification
Card Verifiable Authentication Certificate	These data include Card verifiable certificates of the Card Authentication Public Key as authentication reference data corresponding to the Card Authentication Private Key and used for the card-to-card authentication. They contain encoded access rights (Role ID[2]) and are signed by a certificate provider on behalf of the card issuer. In addition these data contain a certificate for the CA used in the case of the two-step certificate verification. These data are part of the user data provided for use by external entities as authentication reference data of the eHC.	EF.CVC
Client-Server Authentication Private Keys	The Client-Server Authentication Private Keys are asymmetric cryptographic keys used for the authentication of a client application acting on behalf of the cardholder to a server.	PrK.CH.AUT, PrK.CH.AUTN
Decipher Private Keys	The Document Cipher Key Decipher Keys are asymmetric private keys used for document decryption on behalf of the cardholder.	PrK.CH.ENC, PrK.CH.ENCV
Display Message	A display message is used as a means for the Cardholder to check, if a secure channel is established. Note: Technically there are two Display messages, one is stored under DF.HCA and another one under DF.ESIGN. The latter is used in the context of the services Service_Client_Server_Auth and Service_Data_Decryption	EF.DM
X.509 Certificates	The certificates for the keys used in the context of the services Service_Client_Server_Auth and Service_Data_Decryption. These certificates are provided by the card to other entities, which wants to verify the validity of the card's keys used for these services.	EF.C.CH
Public Keys for CV Certificate Verification	Public keys of the Certification Authorities used for verification of the card verifiable certificates.	EF.PuK
Secret Keys for interaction with the "Health Insurance Agency Service Provider"	Two Triple-DES keys for MAC-Calculation and encryption purposes during interaction with the "Health Insurance Agency Service Provider" (The German term for this service is "Versichertenstammdaten-Dienst" (VSDD).)	SK.VSDD
Secret Keys for interaction with the "Download Service Provider"	Two Triple-DES keys for MAC-Calculation and encryption purposes during interaction with the "Download Service Provider" (Also called card application management system, CAMS.)	SK.CAMS
Secret Keys for interaction with the "combined service provider"	Two Triple-DES keys for MAC-Calculation and encryption purposes during interaction with the "combined service provider".	SK.VSDDCAMS
permission data	These data contain information about the permissions given by the cardholderto use specific "freiwillige Anwendungen" (these are applications in the card which may only be used if a patient has allowed this explicitly before the first use)	EF.Einwilligung
reference data (voluntary application)	Data of a so called "freiwillige Anwendung" (this is applications which may only be used if a patient has allowed this explicitly before the first use). Note: In fact the files listed in the next column only contain "pointers" to services, which are handeled outside of the TOE.	EF.Verweis
emergency data	Emergency data ("Notfalldaten") are a specific part of "medical data (voluntary application)".	EF.eNotfalldaten, EF.StatusNotfalldaten

Table 2 Assets to be protected by the TOE and its environment

[2] The definition of role IDs could be found in [11] in table F.2.

3.1.2 Subjects

This Security Target considers the following subjects, who can interact with the TOE:

Name of subject	Description
Cardholder	The cardholder of the TOE is the legitimate user of the card, who is authenticated by use of the PIN.CH or the PIN.home. Note: The following terms are related to the cardholder: The patient is the person who uses the eGK in order to receive e. g. treatment by a doctor. Normally the patient is identical to the cardholder. However, the patient may be incapable of using the card himself (e. g. children) and the cardholder may be a different person acting on behalf of the patient. The insured person ("Versicherter") is the person, who has the insurance relation to the health insurance company. Usually this person is again identical to the cardholder, however the latter may be for example a child of the former. However, since the TOE cannot distinguish these roles, only the cardholder is defined as a subject in the PP [28].
Health Professional	Person acting as health professionals providing medical care to a patient (e.g. physician, dentist, pharmacist, psychotherapist, but also other health professionals yet to be formally defined, like midwives). These health professionals hold a HPC with a Card Verifiable Certificate of the Card Authentication Key with Role ID '2A', '3A','4A', '5A' or '7A'. Note: As a help for the reader of the PP these Role Ids can be interpreted as follows, where access rights for an electronic prescription can be taken as example: Role Id 2A allows to write an electronic prescription to the eHC or to change it and allows comparable rights for other medical data. So typically physicians and dentists may have this Role Id. Role Id 3A also allows to read and modify/delete an (existing) electronic prescription. Typically pharmacists may have this Role ID. Role Id 4A allows no specific rights for an electronic prescription, but may allow read and write access for certain other medical information. Typically psychotherapists may have this Role Id. Role Id 5A also allows to read and modify/delete an (existing)electronic prescription and may be the Role Id for professionals not belonging to one of the preceding groups. Role Id 7A allows to read non –medical data and the emergency data and may be the Role Id for emergency personnel. The preceding examples are not necessary for the correct and secure implementation of Roles in the eGK itself, because the eGK technically only distinguishes the Role Ids and does not "know" the profession of its users.
Medical Assistant	Persons supporting a Health Professional. These health employees hold a HPC with a Card Verifiable Certificate of the Card Authentication Key with a Role ID corresponding with that of the Health Professional, whom they support, i.e. '2A', '3A', '4A', '5A' or '7A'. Note that in medical institutions (e. g. hospitals) some or all of these Role Ids will also be needed for certain administrative personnel.
Security Module Card (health care) (SMC)	This Security Module Card is used in a health care environment in order to allow interaction with the eHC in situations, where employees without a personal card provide services. The SMC has a Card Verifiable Certificate of the Card Authentication Key with a Role ID usually corresponding to that of the Health Professional, who is responsible for its operation,, i. e. '2A', '3A', '4A', '5A' or '7A'. However, a special type of SMC for hospitals exists, which has Role Id 2A, but can be activated by HPCs with other Role Ids. In addition there is a specific additional Role Id '6A' for online transactions of pharmacies ("Mail-Order-Pharmacies").
Self Service Terminal	A Self Service Terminal allows a cardholder of an eHC to perform certain services. The Self Service Terminal has an SMC with a Card Verifiable Certificate of the Card Authentication Key with Role ID '1A', which is distinct from the Role Ids of the preceding subjects.
Health Insurance Agency Service Provider	The "Health Insurance Agency Service Provider" interacts with the TOE on behalf of the health insurance agency. The German term for this is "Versichertenstammdaten-Dienst" (VSDD). The service provider uses a security module (e. g. in form of a SMC), which is authenticated by use of the key SK.VSDD.
TOE Manufacturer	Person(s) responsible for development and production of the TOE. Note: According to the life cycle description in section 2.1.3, the initialisation of the card is either done by the TOE Manufacturer or by the personalisation service provider.

Name of subject	Description
Personalisation Service Provider	person(s) responsible for personalisation of the card This subject authenticates with an authentication mechanism that guarantees that only personalisation data authorised by this subject will be accepted and loaded into the TOE. This subject has only access in life-cycle phase 6 but not in life-cycle phase 7.
Download Service Provider	person(s) responsible for Downloading additional applications (consisting of file structures, their access rights and data) into the card in phase 7 of the TOE's lifecycle. (Also called card application management system, CAMS.) The service provider uses a security module (e. g. in form of a SMC), which is authenticated by use of the key SK.CAMS.
Combined Services Provider	Name for the combination of the Health Insurance Agency Service Provider and the download service provider (in case a descision is made to combine these services or at least to allow the use of a shared key for these services).
Other Person	All persons who interact with the TOE without being authorised (as one of the preceding roles).

Table 3 Subjects of the eHC

Note, that the list of subjects in this Security Target is identical to the list of subjects defined in the eHC-PP [28] section 3.1.2. There are no additional roles known to the TOE.

3.2 Organizational Security Policies

On the one hand the overall security objectives for the eHC-System can be derived mainly from the legal requirements. On the other hand the concrete security services to be provided by the TOE are defined by the specifications. For this reason the organisational security policies define the greater part of the security needs for the eHC compared to lists of individual threats.

OSPs will be defined in the following form:

OSP.name Short Title

Description.

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).

OSP.eHC_Spec Compliance to eHC specifications

The eHC shall be implemented according to the security relevant requirements of the specifications:

[7] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform, Version 1.1.0, 07.02.2006,gematik

[8] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Anwendungen und anwendugngsspezifische Strukturen, Version 1.2.1, 07.09.2006,gematik

Note by the ST-author 2:

No newer versions of the specifications as the one listed in the eHC-PP [28] have been used.

OSP.Additional_Applications Protection of additional Applications

- The TOE shall provide the possibility to authorised parties to load data for additional applications to the card. Loading of additional executable code shall not be possible.
- The TOE shall separate existing applications from additional applications. This means that data structures, access rights and data contents of such additional applications can not modify the security properties, in particular access control, for the existing applications.
- By defining access rights to the files belonging to additional applications suitably it shall be possible to provide access control to such files using the mutual authentication services or the PIN authentication services as defined in section 2.1.2.

Note by the ST-author 3:

This OSP is designed to provide the functionality to add such applications in a secure way and to provide support for their future security needs. For example, access to further medical data not covered by the current specifications of the eHC may require some kind of authentication either by a health professional or by the cardholder.

OSP.Electronic_Prescriptions Access to electronic prescriptions

Access to electronic prescriptions in the eHC must only be possible after authentication.

Creation or modification of these data in the eHC must only be possible in connection with a HPC.

The Cardholder in combination with a Self Service Terminal has the following rights: He can read, deactivate or activate and also delete an electronic prescription.

Access to data on an eHC for personnel without HPC may be authorized by the holder of a HPC. Such access must be logged securely.

Unauthorized access or modification of these data during transport and storage must be prevented.

OSP.User_Information Information about secure usage

The Cardholder of the eHC needs to be informed clearly about secure usage of the product.

Note: In order to use the eHC securely the user needs this information. This is also required by privacy legislation.

OSP.Legal_Decisions Legal responsibility of authorised persons

The decision, which data are legally feasible for storage on the eHC has to be made by the persons authorised to deal with the data. The same holds for the decision, when data need to be deleted.

Note: The eHC itself cannot decide about the legal relevance and medical correctness of data stored in it.

OSP.services Services provided by the card

The eHC shall provide the following services:

- Service_Asym_Mut_Auth_w/o_SM,
- Service_Asym_Mut_Auth_with_SM,
- Service_Sym_Mut_Auth_with_SM,
- Service_User_Auth_PIN and Service_User_Auth_PUC,
- Service_Privacy,
- Service_Client_Server_Auth,
- Service_Data_Decryption,
- Service_Card_Management and
- Service_Logging

as described in section 2.1.2.

Note: The eHC also provides electronic signature services, however this is to be evaluated according to security requirements for electronic signatures, e. g. from another PP. Annex 7.1 gives guidance how to combine such PP with the eHC-PP [28].

OSP.logging Logging of access to medical data

All access to medical data (except reading access by the Cardholder himself) must be logged. Access to the log file must be protected.

OSP.Manufact Manufacturing of the Smart Card

The TOE Manufacturer shall ensure the quality and integrity of the manufacturing process and control the smart card material during development and production of the TOE.

3.3 Threats

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

Threats will be defined in the following form:

T.name Short Title

Description, for example starting “An attacker tries to...”.

3.3.1 Threats mainly addressing TOE_ES and TOE_APP

The TOE shall avert the threats, which are application and operating system oriented, as specified below. As potential attackers all kinds of subjects as listed in the Table in section 3.1.1 are considered, as far as they

- try to perform actions, which they are not allowed by their access rights as defined in the PP [28] and
- may have expertise, resources and motivation as expected from an attacker with high attack potential

T.Compromise_Internal_Data Compromise of confidential User or TSF data

An attacker with high attack potential tries to compromise confidential user data or TSF data through the communication interface of the TOE by sending commands or by listening to the communication between a terminal and the TOE.

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

T.Forge_Internal_Data Forge of User or TSF data

An attacker with high attack potential tries to forge internal user data or TSF data.

This threat comprises several attack scenarios of smart card forgery. The attacker may try to alter the user data e.g. to add keys for decipherment of documents. The attacker may misuse the TSF management functions to change the user authentication data to a known value.

T.Misuse Misuse of TOE functions

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

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

T.Intercept Interception of Communication

An attacker with high attack potential tries to intercept the communication between the TOE and an SMC, HPC, Download Service Provider or Health Insurance Agency Service Provider in order to read, to forge, to delete or to add other data to transmitted data classified as assets.

This threat comprises several attack scenarios. A health professional reads from and writes onto eHC patient's data like medication or medical data which an attacker may read or forge during transmission. Attacker may try to read the document keys output by the TOE as DECIPHER command response. Attackers may try to manipulate card management processes.

3.3.2 Threats mainly addressing TOE_ES and TOE_IC

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

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.

T.Information_Leakage Information Leakage from TOE's chip

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 contact less interface (emanation) or direct measurements (by contact to the chip still available even for a contact less 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).

T.Malfunction Malfunction due to Environmental Stress

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

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

T.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.

3.4 Assumptions

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

The format for assumptions will be as follows:

A.name short title

Description.

The following assumptions hold for the usage environment:

A.Users Adequate usage of TOE and IT-Systems in the environment.

The cardholder of the TOE uses the TOE adequately. In particular he doesn't tell the PIN (or PINs) of the eHC to others and doesn't hand the card to unauthorised persons. Other actors (see subjects defined in section 3.1.2) use their data systems according to the overall system security requirements.

A.Perso Secure handling of data during personalisation and additional personalisation

All data structures and data on the card produced during personalisation or additional personalisation steps during the end-usage phase are correct according to the specifications and are handled correctly regarding integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys (in accordance with the cryptographic algorithms specified for the eHC) and their confidential handling. The Personalisation Service Provider controls all materials, equipment and information, which he uses to personalize authentic smart cards, in order to prevent counterfeit of the TOE.

The same requirements hold for all activities belonging to Phase 5 "Initialisation", if they are executed after TOE delivery. This holds for example if the Personalisation Service Provider also sends the initialisation data to the TOE or if the TOE is delivered by the TOE Manufacturer in form of smart card modules, which are then inserted into the plastic cards at a later stage.

In addition to these assumptions the threats and assumptions made in [29] for the certification of the IC have to be considered.

4 Security Objectives

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

Note by the ST-author 4:

The separation of the security objectives for the TOE environment follows the approach of CC version 2.4 and does not violate the CC version 2.3. The CC version 2.3 address the operational environment only.

4.1 Security Objectives for the TOE

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

Objectives for the TOE will be defined in the following form

OT.name short title

Description of the objective.

In order to support developers, who want to reuse results of a IC (hardware) evaluation or an evaluation of the card operating system, the security objectives are grouped according to the parts of the TOE.

Note by the ST-author 5:

The structuring of the PP has been transferred without changes for the ST.

4.1.1 Security objectives, which are mainly TOE_App oriented

OT.Access_rights Access control policy for data in the TOE

In the End Usage Phase the TOE shall implement the access control policy **SFP_access_rules**, which is defined in the following table.

SFP_access_rules
The following subjects may interact with the TOE (see also section 3.1.2, Table 2): Cardholder, Health Professional, Medical Assistant, Security Module Card (health care), Self Service Terminal, Health Insurance Agency Service Provider, TOE Manufacturer, Personalisation Service Provider, Download Service Provider, Combined Services Provider, Other Person

SFP_access_rules

The following objects are covered by the policy (see also section 3.1.1, Table 3):

Personal and health insurance data (open), Personal and health insurance data (protected), , electronic prescription, VAD (eHC), RAD (eHC), logging data, Card Authentication Private Key, Card Verifiable Authentication Certificates, Client-Server Authentication Private Keys, Decipher Private Keys, Display Message, X.509 Certificates, Public Keys for CV Certificate Verification, SK.VSDD, SK.CAMS, permission data, medical data (voluntary application), emergency data.

Note: initialisation data and personalisation data are terms used for data written during the corresponding life cycle phases. For the End Usage Phase all assets are covered by the data already listed above.

The following authentication methods are covered by the policy:

The services Service_Asym_Mut_Auth_w/o_SM, Service_Asym_Mut_Auth_with_SM, Service_Sym_Mut_Auth_with_SM, Service_User_Auth_PIN, Service_User_Auth_PUC as defined in chapter 2 “TOE description”.

The following security attributes for subjects are maintained by the TOE:

For every authentication method the TOE maintains the status of successful authentication (successful PIN verification, successful mutual authentication). (These are security attributes for the connected subject, because the TOE derives the access rights from these attributes).

The following access methods are maintained by the TOE:

Access is allowed only using the defined command interface of the TOE. In other words: A subject sends a command APDU as defined in the eHC specification to the TOE and the TOE processes it. Access to eHC data is not allowed via a contact-less interface.

Requirements for encryption or MAC-protection (Using Secure Messaging) will be included in addition for access to some of the data.

The following types of access are used in the rules below:

“Read”, “write”, “delete”, “deactivate” (this means making data invisible for other subjects, but without deleting them), “activate” (making deactivated data visible again), “use” (a command is called, which uses data internally, this is relevant for cryptographic keys).

As specific variants of the write access the following terms are used: “Modify” means to change existing data. “Append” means to add data at the end of existing data. “Create” means to create new data structures.

The following access rules are defined for the TOE’s objects:

For all files and other security relevant data (PINs, keys) the TOE maintains the following access rules as defined in the eHC specification, Part 2. Note, that these rules hold for the End Usage Phase of the TOE.

Rule_1:

Personal and health insurance data (open) may be read by all subjects and written only by the Health Insurance Agency Service Provider or Combined Services Provider. Writing of these data requires secure messaging with encryption and MAC.

Rule_2:

Personal and health insurance data (protected) can be read by:Cardholder, Health Professional, Medical Assistant, Security Module Card (health care), Combined Services Provider and Health Insurance Agency Service Provider. They can be written by the Health Insurance Agency Service Provider and Combined Services Provider. Writing of these data requires secure messaging with encryption and MAC. Reading data also requires secure messaging with encryption and MAC in the case of Health Insurance Agency Service Provider, Combined Services Provider and Role Id ‘6A’ (online access by a pharmacy).

Rule_3:

Data of type electronic prescription can be read or deleted by Health Professional with Role ID 2A, 3A or 5A, Medical Assistant with one of the same Role IDs, Security Module Card (health care) with one of the same Role IDs. An entity with Role Id 6A (online pharmacy) can also read and
delete an electronic prescription, but only with secure messaging with encryption and MAC.

The cardholder can read the data and in combination with a Self Service Terminal he has the following rights: He can deactivate or activate and also delete an electronic prescription. Only Health Professional with Role ID 2A, Medical Assistant with Role ID 2A and Security
Module Card (health care) with Role ID 2A can write these data.

Note: Technically the ability to delete an electronic prescription is realised by the right to modify EF.eRezept_Tickets. The confidentiality of the contents of the electronic prescription is ensured by encryption of the EF.eRezept_Container with a key stored in EF.eRezept_Tickets.

Rule_4:

Data of type RAD (eHC): The PIN.CH and PIN.home may be modified by the Cardholder, the resetting code (PUC) cannot be modified. Both data can not be read by anyone. The retry counter for the PIN can be reset by the Cardholder after authentication with the PUC.

Note: VAD (eHC) stands for PIN or resetting code values, which are entered by the Cardholder in clear text and therefore require no specific rules by this policy.

Rule_5:

The logging data can be written by Health Professional , Medical Assistant, Security Module Card (health care) and by the Self Service Terminal. Only new entries can be appended, existing entries can not be modified (however, when fifty entries are full, the oldest entry is deleted, when adding a new one). Appending data also requires
secure messaging with encryption and MAC in the case of Role Id ‘6A’ (online access by a pharmacy). The data can be read by the Cardholder.

SFP_access_rules
Rule_6: The Card Authentication Private Key can never be read or written. It can be used in the services Service_Asym_Mut_Auth_w/o_SM and Service_Asym_Mut_Auth_with_SM. These services include the verification of a CV certificate for the card or security module, with which the TOE interacts during the service.
Rule_7: The Card Verifiable Authentication Certificates can always be read and never written.
Rule_8: The Client-Server Authentication Private Keys and the Decipher Private Keys cannot be read or written, they can only be used in the corresponding services Service_Client_Server_Auth and Service_Data_Decryption. For the keys PrK.CH.AUT and PrK.CH.ENC respectively both services are possible only after authentication by the cardholder. For the second authentication key PrK.CH.AUTN the service Service_Client_Server_Auth is allowed after authentication by Health Professional, Medical Assistant, Security Module Card (health care) all of these with Role ID 1A, 2A, 3A, 4A or 5A. For the second decryption key PrK.CH.ENCV the service Service_Data_Decryption is allowed after authentication by Health Professional, Medical Assistant, Security Module Card (health care) all of these with Role ID 3A (pharmacy) or 6A (online pharmacy). This requires secure messaging with encryption and MAC in case of Role Id 6A.
Rule_9: The Public Keys for CV Certificate Verification can never be written. It can be used for verification of certificates. Note: Additional Public keys may be stored temporarily in case of cross-certification. The above rule holds for the “root” key of the eHC.
Rule_10: The symmetric keys SK.VSDD, SKVSDDCAMS and SK.CAMScannot be read or written. They can be used for establishment of trusted channels by the service Service_Sym_Mut_Auth_with_SM.
Rule_11: Files and other data structures necessary for additional applications can be created by the Download Service Provider or Combined Services Provider. The commands used for this require protection by secure messaging with encryption and MAC.
Rule_12: The Health Insurance Agency Service Provider, the Download Service Provider and the Combined Services Provider have the right to deactivate the complete health care application, which means that the card isn’t usable as an eHC any more. They can also re-activate the application. The commands used for this require protection by secure messaging with encryption and MAC (and therefore authentication by the service Service_Sym_Mut_Auth_with_SM).
Rule_13: The Display Message can be written only by the cardholder. It can be read only by use of secure messaging, which requires authentication using the service Service_Asym_Mut_Auth_with_SM or Service_Sym_Mut_Auth_with_SM. Note: This allows to demonstrate the establishment of a secure channel to the cardholder.
Rule_14: The X.509 Certificates of the card except EF.C.CH.AUTN can be read by everybody and all of them can be written by the Download Service Provider and the Combined Services Provider. Writing requires protection by secure messaging with encryption and MAC. Reading EF.C.CH.AUTN is allowed only for entities authenticated as Role Id ‘2A’ or ‘3A’.
Rule_15: The permission data can be read by the cardholder and by those Health Professional, Medical Assistant, Security Module Card (health care) who have Role Id ‘2A’ or ‘3A’. Reading these data is also possible but requires secure messaging with encryption and MAC in the case of Role Id ‘6A’ (online access by a pharmacy). They can be written by Health Professional with Role ID 2A or 3A, by Medical Assistant with Role ID 2A or 3A and by Security Module Card (health care) with Role ID 2A or 3A. Writing requires additional authentication using PIN.CH.
Rule_16: The reference data (voluntary application) can be read by all subjects. They can be written by the Combined Services Provider and the Download Service Provider using secure messaging wih encryption and MAC and by Health Professional, Medical Assistant and by Security Module Card (health care) with specific Role Ids 2A or 3A together with the cardholder (using PIN.CH).
Rule_17: The emergency data can be written by Health Professional with Role ID 2A, Medical Assistant with Role ID 2A and Security Module Card (health care) with Role ID 2A but only together with the cardholder (PIN.CH). They can be read by all Health Professional, Medical Assistant, Security Module Card (health care) with one of the Role-IDs 2A, 7A. They can be deactivated or activated by the cardholder in combination with a Self Service Terminal.

Table 4: Access Control Policy for Usage Phase

Note by the ST-author 6:

No newer version than listed in the eHC-PP [28] are known and therefore no other rules have been defined.

4.1.2 Security Objectives, which are mainly TOE_ES oriented

The TOE security objectives in this section are those, which will probably be addressed by the TOE operating system.

The following objectives all refer to the specifications of the eHC:

[7] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform, Version 1.1.0, 07.02.2006,gematik

[8] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Anwendungen und anwendugngsspezifische Strukturen, Version 1.2.1, 07.09.2006,gematik

The following objectives shall be upheld by the TOE:

OT.AC_Pers Access control for personalization

The TOE must ensure that the personalisation data can be written by authorized Personalisation Service Provider only.

OT.Additional_Applications Protection of additional Applications

- The TOE shall provide the possibility to authorised parties to load data for additional applications to the card. Loading of additional executable code shall not be possible.
- The TOE shall separate existing applications from additional applications. This means that data structures, access rights and data contents of such additional applications can not modify the security properties, in particular access control, for the existing applications.
- By defining access rights to the files belonging to additional applications suitably it shall be possible to provide access control to such files using the mutual authentication services or the PIN authentication services as defined in section 2.1.2.

Note by the ST-author 7:

This objective is designed to provide the functionality to add additional applications in a secure way and to provide support for their future security needs.

OT.Services Services provided by the Card

The eHC shall provide the following services:

- Service_Asym_Mut_Auth_w/o_SM,
- Service_Asym_Mut_Auth_with_SM,

- Service_Sym_Mut_Auth_with_SM,
- Service_User_Auth_PIN and Service_User_Auth_PUC,
- Service_Privacy,
- Service_Client_Server_Auth,
- Service_Data_Decryption,
- Service_Card_Management and
- Service_Logging

as described in section 2.1.2.

Note: The eHC also provides electronic signature services, however this is to be evaluated according to security requirements for electronic signatures, e. g. from another PP. Annex 7.1 gives guidance how to combine such PP with the eHC-PP [28].

OT.Cryptography Implementation of cryptographic algorithms

The cryptographic algorithms required by the eHC specifications, Part 1, (see [7], section 12) are implemented according to their definition.

These algorithms are:

- RSA for Card-To-Card authentication (asymmetric authentication procedures with and without trusted channel establishment, which includes signature and verification operations) and for X.509 based data decryption and signatures. Supported RSA digital signature input formats are:
  - PKCS #1 V1.5 (for signatures related to keys with x.509 certificates)
  - ISO 9796-2 (with random numbers. for signatures related to keys with x.509 certificates and without random numbers for CV certificate processing)
- SHA-1, DES-3.

4.1.3 Security Objectives, which are mainly TOE_IC oriented

The following TOE security objectives are drawn from BSI-PP-0002 [26] and address the protection provided mainly by TOE_IC (however it may use support by the other components of the TOE) and independent off the TOE environment.

Note by the ST-author 8:

This should allow a developer to use the method of composite evaluation with a hardware already evaluated according to BSI-PP-0002.

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's chip

- 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 and
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

Note by the ST-author 9:

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 specified in the eHC-PP in more detail. This analysis is part of AVA_VLA.4 of this evaluation.

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 chip 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.

Note by the ST-author 10:

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.

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. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

Note by the ST-author 11:

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.Prot_Phys_Tamper) provided that detailed knowledge about the TOE´s internal construction is required and the attack is performed in a controlled manner.

OT.Prot_Abuse_Func Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order (i) to disclose critical User Data, (ii) to manipulate critical User Data of the Smartcard Embedded Software, (iii) to manipulate Soft-coded Smartcard 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.

4.2 Security Objectives for the Development and Manufacturing Environment

OD.Assurance Assurance Security Measures in Development and Manufacturing Environment

The developer and manufacturer 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.

OD.Material Control over Smart Card Material

The TOE Manufacturer must control all materials, equipment and information, which he uses in order to produce, to initialise, to pre-personalize genuine smart card materials in order to prevent counterfeit of the TOE.

4.3 Security Objectives for the Operational Environment

OE.Users Adequate usage of TOE and IT-Systems in the environment.

The Cardholder of the TOE needs to use the TOE adequately. In particular he mustn't tell the PIN (or PINs) of the eHC to others and mustn't hand the card to unauthorised persons.

OE.Legal_Decisions Legal responsibility of authorised persons

The decision, which data are legally feasible for storage on the eHC has to be made by the persons authorised to deal with the data. The same holds for the decision, when data need to be deleted. These persons must use their IT systems according to the legal requirements.

This objective holds for all subjects (or the persons controlling them, if the subjects themselves are technical devices) listed in section 3.1.2, Table 3 except the Cardholder (who's behaviour is covered by other objectives) and the category "Other Person", which includes attackers.

OE.Data_Protection Protection of sensitive data outside of the eHC

The persons responsible for the handling of sensitive data outside of the eHC (this includes medical data, PINs, cryptographic keys and sensitive personal data, see the definition of assets in Table 1.) use adequate protection for confidentiality and integrity of these data.

OE.User_Information Information about secure usage

The Cardholder of the TOE must be informed clearly about secure usage of the product.

OE.Perso Secure handling of data during personalisation and additional personalisation

All data structures and data on the card produced during personalisation or additional personalisation steps during the end-usage phase must be correct according to the specifications and must be handled correctly regarding integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys (in accordance with the cryptographic algorithms specified for the eHC) and their confidential handling. The Personalisation Service Provider must control all materials, equipment and information needed to personalize authentic smart cards in order to prevent counterfeit of the TOE.

The same requirements hold for all activities belonging to Phase 5 "Initialisation", if they are executed after TOE delivery. This holds for example if the Personalisation Service Provider also sends the initialisation data to the TOE or if the TOE is delivered

by the TOE Manufacturer in form of smart card modules, which are then inserted into the plastic cards at a later stage.

Note by the ST-author 12

The security objectives for the environment are very important for the security of the system, in which the eHC is used. According to the requirements defined in the assurance class AGD the user guidance of the TOE will therefore contain more detailed information about measures to support these objectives. The following considerations may be helpful for this:

- If communication between the TOE and another device is done across insecure networks, only services secured by secure messaging must be used. A typical example would be an internet apothecary. The end user must be informed about his possibilities to check this (e. g. how to use the Display Message in order to see that a secure channel was established).

- The concept of the two PINs PIN.CH and PIN.home have to be made clear to the cardholder, in particular he needs to be informed, that the PIN.home must only be used in his private environment or at a Self Service Terminal. In any other IT system of a medical practice or apothecary only PIN.CH must be used. If the cardholder wants to make real use of the privacy features like activation or deactivation of certain data, he needs to make sure that PIN.CH and PIN.home have distinct values.

- The procedures used by the card issuer in order to deliver the eHC as well as PINs and PUCs to the Cardholder must be suitable to prevent attackers from successfully intercepting and using the eHC and the PIN and/or PUC. The requirements defined by gematik in the document [9] (in the version valid at the time of evaluation) will have to be fulfilled and the guidance documentation (e. g. for the Personalisation Service Provider) will have to describe the procedures adequately.

- The environment, where the cardholder enters his PIN, must make sure that the PIN is not intercepted on the line between the device, where the PIN is entered and the TOE.
- Similarly, all environments, where authentication (e. g. of a HPC) without secure messaging is used, must ensure that interception or modification of the sensitive data is not possible on the line between the TOE and other devices. They must also prevent unauthorised persons from sending card commands to the TOE after such type of authentication.

- If the Service_Data_Decryption is used the environment must ensure that the deciphered data (usually document encipherment keys) are not intercepted during transport outside of the TOE.
- If medical data are stored outside of the eGK, for example on a Server, then appropriate access control needs to be in place to prevent unauthorised read or write access to these data.
- Of course all parties, which have management access to the TOE (Health Insurance Agency Service Provider, Personalisation Service Provider, Download Service Provider) must ensure that their activities maintain the security of the TOE and its data.

5 Extended Components Definition

This security target uses components defined as extensions to CC part 2, as defined in the protection profile [28]. Some of these components are defined originally in the protection profile [26].

5.1 Definition of the Family FCS_RND

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.

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

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:

Fehler! Es ist nicht möglich, durch die Bearbeitung von Feldfunktionen Objekte zu erstellen.

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.

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

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

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

Dependencies: FMT_LIM.2 Limited availability.

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

FMT_LIM.2	Limited availability
Hierarchical to:	No other components.
FMT_LIm.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: *Limited capability and availability policy*].
Dependencies:	FMT_LIM.1 Limited capabilities.

Note by the ST-author 13

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

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	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 other components.

6 Security Requirements

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

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of part 2 of the CC. Each of these operations is used in the eHC PP [28] and respectively also in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements made in the eHC PP [28] is either

- denoted by the word “refinement” in bold text and the added/changed words are in bold text or
- 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. Additional refinements in the ST will be underlined and put in brackets “(…)” and marked by a footnote that states that this refinement is made by the ST-author.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors of the eHC PP [28] are denoted as <u>underlined text</u> and the original text of the component is given by a footnote. Any uncompleted selection that have been completed by the ST author appear *italicized* and <u>underlined</u> and the original text of the eHC PP [28] is given by a footnote.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors of the eHC PP [28] are denoted by showing as <u>underlined but not italicized text</u> and the original text of the component from [2] is given by a footnote. Any uncompleted assignments that have been completed by the ST author appear *italicized* and <u>underlined</u> and the original text of the eHC PP [28] is given by a footnote.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier. Iterations in the ST, which do not appear in the PP appear in addition *italicized* in the header and the full text.

If the *italicized* format for iteration leads to an non unambiguous tracing of PP changes according to italicized forms used also for selections, assignments and refinements additional information will be given in the footnotes for an unambiguous definition.

6.1 TOE Security Functional Requirements

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

6.1.1 Cryptographic support (FCS)

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

FCS_CKM.1/SM Cryptographic key generation – Secure Messaging Keys

Hierarchical to: No other components.

FCS_CKM.1.1/SM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm card-to-card authentication with secure messaging [3] and specified cryptographic key sizes 112 bit[4] that meet the following: [8], Sections 3.6, 3.7 [5].

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

Note by the ST-author 14:

The Key Generation is done during a mutual authentication with trusted channel establishment according to section 3.6 or 3.7 of the eHC specification, part 2 ([8]). The Authentication Protocol produces agreed parameters to generate the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging. The algorithm uses random numbers generated by the TSF as required by FCS_RND.1.

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

---

3 [*assignment: cryptographic key generation algorithm*]

4 [*assignment: cryptographic key sizes*]

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 *physical deletion of key values*[6] that meets the following: *none*[7].

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

Note by the ST-author 15:

As recommended in the eHC-PP [28], the TOE destroys the Triple-DES encryption session key and the Retail-MAC message authentication session keys for secure messaging after reset or termination of secure messaging session or reaching fail secure state according to FPT_FLS.1.

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

FCS_COP.1/SHA Cryptographic operation – Hash Algorithm

Hierarchical to: No other components.

FCS_COP.1.1/SHA The TSF shall perform hashing [8] in accordance with a specified cryptographic algorithm SHA-1 [9](and RIPEMD-160, SHA-2 (224 bit), SHA-2 (256 bit), SHA-2 (384 bit), SHA-2 (512 bit))[10] and cryptographic key sizes none [11] that meet the following: FIPS 180-2 [12].

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or

5 [assignment: *list of standards*]
6 [*assignment: cryptographic key destruction method*]
7 [*assignment: list of standards*]
8 [assignment: *list of cryptographic operations*]
9 [assignment: *cryptographic algorithm*]
10 The extension of RIPEMD-160 and SHA-2 is a refinement of FCS_COP.1/SHA as defined in the PP.
11 [assignment: *cryptographic key sizes*]
12 [assignment: *list of standards*]

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Note by the ST-author 16:

This SFR requires the TOE to implement the hash function SHA-1. In addition other hash functions have been attached as explicitly allowed by the corresponding application note in the eHC-PP [28]. Note, that as required by the PP all added hash functions are compliant to the requirements of the RegTP for electronic signatures [19].

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

Hierarchical to: No other components.

FCS_COP.1.1/ CCA_SIGN	The TSF shall perform digital signature-creation [13] in accordance with a specified cryptographic algorithm RSA [14] and cryptographic key sizes *from 1024 bit to 2048 bit module length*[15] that meet the following: ISO/IEC9796-2 (DS scheme 1) [16].

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

Note by the ST-author 17:

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 according the eHC specification, part 2 ([8]).

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

Hierarchical to: No other components.

---

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

FCS_COP.1.1/ CCA_VERIF	The TSF shall perform digital signature-verification [17] in accordance with a specified cryptographic algorithm RSA [18] and cryptographic key sizes *from 1024 bit to 2048 bit module length*[19] that meet the following: ISO/IEC9796-2 (DS scheme 1) [20].

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

Note by the ST-author 18:

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 according to eHC specification, part 2 ([8]).

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 [21] in accordance with a specified cryptographic algorithm RSA [22] and cryptographic key sizes *from 1024 bit to 2048 bit module length*[23] that meet the following: PKCS#1 [24] [24].

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

Note by the ST-author 19:

---

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

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 eHC specification, Part 2 [8].

FCS_COP.1/RSA_DEC Cryptographic operation – RSA Decryption

Hierarchical to: No other components.

FCS_COP.1.1/ RSA_DEC	The TSF shall perform decryption [25] in accordance with a specified cryptographic algorithm RSA [26] and cryptographic key sizes *from 1024 bit to 2048 bit module length*[27] that meet the following: PKCS#1, [24] [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

Note by the ST-author 20:

This SFR requires the TOE to implement the RSA for the cryptographic primitive of the RSA decryption.

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

Hierarchical to: No other components.

FCS_COP.1.1/ TDES	The TSF shall perform encryption and decryption [29] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode [30] and cryptographic key sizes 112 bit [31] that meet the following: FIPS 46-3 [21] [32].

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

---

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

FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Note by the ST-author 21:

This SFR requires the TOE to implement the cryptographic primitive for secure messaging and for possible other uses of TDES.

FCS_COP.1/MAC Cryptographic operation – Retail MAC

Hierarchical to: No other components.

FCS_COP.1.1/ MAC	The TSF shall perform generation and verification of message authentication code [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[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

Note by the ST-author 22:

This SFR requires the TOE to implement the cryptographic primitive for secure messaging.

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

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 *functionality class K3 with SOF-high of AIS20 [5] and functionality class P2 with SOF-high of AIS31[6]*[37].

Dependencies: No dependencies.

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

Note by the ST-author 23:

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/SM for secure messaging. The quality metric that have been chosen is the AIS 20 [5] for deterministic random number generators which allows SOF-high evaluation.

6.1.2 Identification and Authentication

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

The eHC-PIN are two PINs that will be handled separately. Therefore authentication attempts of the user will be handled separately for each of the PINs: PIN.CH and PIN.home. This has been covered by an iteration and refinement of FIA_AFL.1/PIN and FIA_AFL.1/PUC.

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

Hierarchical to: No other components.

FIA_AFL.1.1/PIN.CH	*The TSF shall detect when three [38] unsuccessful authentication attempts occur related to consecutive failed human user authentication (with the PIN.CH[39]) for the health care application [40].*
FIA_AFL.1.2/PIN.CH	*When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall block the PIN (PIN.CH[41]) for authentication until successful unblock with resetting code [42].*

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1/PIN.home Authentication failure handling – eHC-PIN.home

Hierarchical to: No other components.

[38] Fulfilled selection; Version of the PP: [selection: [assignment: *positive integer number*], "*an administrator configurable positive integer within* [assignment*: range of acceptable values*]

[39] refinement by the ST-author – obviously this refinement is valid, because the original requirement is still fulfilled

[40] Copied assignment of the PP; version from CC part 2: [*assignment: list of authentication events*]

[41] Refinement by the ST-author – obviously this refinement is valid, because the original requirement is still fulfilled

[42] Copied assignment of the PP; version form CC part 2: [assignment: *list of actions*]

FIA_AFL.1.1/PIN .home	*The TSF shall detect when three [43] unsuccessful authentication attempts occur related to consecutive failed human user authentication (with the PIN.home[44]) for the health care application [45].*
FIA_AFL.1.2/PIN .home	*When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall block the PIN (PIN.home[46]) for authentication until successful unblock with resetting code [47].*

Dependencies: FIA_UAU.1 Timing of authentication.

Note by the ST-author 24:

The component FIA_AFL.1/PIN of the eHC-PP [28] addresses the human user authentication by means of the PIN (PIN.CH and PIN.home) for the health care application. In the ST this component has been iterated to handle PIN.CH and PIN.home separately. For PIN.CH and for PIN.home a retry counter of 3 with a PIN-length of at least 6 has been chosen to fulfil the requirements of SOF-high.

Note by the ST-author 25:

The PIN for the qualified electronic signatures is not part of this evaluation.

FIA_AFL.1/PUC.CH Authentication Failure Handling – eHC-PIN.CH-unblocking code

Hierarchical to: No other components.

---

43 Fulfilled selection of the PP; Version from the PP: [selection: [assignment: *positive integer number*], "*an administrator configurable positive integer within* [assignment*: range of acceptable values*]

44 refinement by the ST-author – obviously this refinement is valid, because the original requirement is still fulfilled

45 Copied assignment of the PP; version from CC part 2: [*assignment: list of authentication events*]

46 Refinement by the ST-author – obviously this refinement is valid, because the original requirement is still fulfilled

47 Copied assignment of the PP; version from CC part 2: [assignment: *list of actions*]

FIA_AFL.1.1/PUC.CH	*The TSF shall detect when ten [48] successful or[49] unsuccessful authentication attempts occur related to usage of the eHC-PIN (PIN.CH[50]) unblocking code[51].*
FIA_AFL.1.2/PUC.CH	*When the defined number of successful or unsuccessful authentication attempts has been met or surpassed, the TSF shall block the PIN unblocking code for the [52] (PIN.CH[53]).*

Dependencies: *FIA_UAU.1 Timing of authentication*

FIA_AFL.1/PUC.home Authentication Failure Handling – eHC-PIN.home-unblocking code

Hierarchical to: No other components.

FIA_AFL.1.1/PUC.home	*The TSF shall detect when ten [54] successful or[55] unsuccessful authentication attempts occur related to usage of the eHC-PIN (PIN.home[56]) unblocking code[57].*
FIA_AFL.1.2/PUC.home	*When the defined number of successful or unsuccessful authentication attempts has been met or surpassed, the TSF shall block the PIN unblocking code for the [58] (PIN.home[59]).*

Dependencies: *FIA_UAU.1 Timing of authentication*

Note by the ST-author 26:

---

[48] Fulfilled selection of the PP; Version from the PP: [assignment*: positive integer number], from CC part 2: [selection: [assignment: positive integer number], "an administrator configurable positive integer within [assignment: range of acceptable values]"]*

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

[50] Refinement of the ST-author – obviously this refinement is valid, because the original requirement is still fulfilled

[51] Copied assignment from the PP; Version of CC part 2: [assignment: *list of authentication events*]

[52] Fulfilled assignment of the PP; Version of the PP:[assignment: *list of actions, which at least includes: block the PIN unblocking code*]; version of CC part 2: [*assignments: list of actions*]

[53] Refinement by the ST-author – obviously this refinement is valid, because the original requirement is still fulfilled

[54] Fulfilled selection of the PP; Version from the PP: [assignment*: positive integer number], from CC part 2: [selection: [assignment: positive integer number], "an administrator configurable positive integer within [assignment: range of acceptable values]"]*

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

[56] Refinement of the ST-author – obviously this refinement is valid, because the original requirement is still fulfilled

[57] Copied assignment from the PP; Version of CC part 2: [assignment: *list of authentication events*]

[58] version PP: [assignment: *list of actions, which at least includes: block the PIN unblocking code*]; version CC part 2: [assignment: *list of actions*]

[59] Refinement by the ST-author – obviously this refinement is valid, because the original requirement is still fulfilled

The component FIA_AFL.1/PUC from the eHC-PP [28] address the human user authentication by means of the PIN unblocking code for the PIN used for the health care application. To handle the PUC for the PIN.home separately from the PUC of the PIN.CH the component of the eHC-PP [28] has been iterated in this ST. The PUC of the PIN.CH as well as the PUC of the PIN.home has a length of 8 and a usage counter of 10. This fulfills the requirements of SOF-high for the PUC mechanism, which will be discussed in the appropriate evaluation documents.

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

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

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

Dependencies: No dependencies.

Note by the ST-author 27:

The component FIA_ATD.1 applies to (i) the human user authentication, i.e. the cardholder, whose identity is given in the Personal and health insurance data (open), 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.

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 the Card Verifiable Authentication Certificate,

(3) reading the Certificate Service Provider Certificate,

(4) reading data with access condition ALWAYS

(5) *generating random numbers*

(6) *generating a hash*[60]

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

	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.

Note by the ST-author 28:

The list has been completed by reading data with access condition ALWAYS, generating random numbers and setting security environments which are all TSF-mediated actions. The sublementary does not contradict the policy SFP_access_rules. Note that there are actions which could be done without identification but are not TSF-mediated actions and are therefore not part of this SFR, for example selecting files.

Note also that this SFR is meant to support the access control policy SFP_access_rules. Access rules for the initialisation and personalisation phases are defined by the management SFRs (FMT_MTD.1).

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

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow

(1) *reading the ATR*

(2) *reading the Card Verifiable Authentication Certificate,*

(3) *reading the Certificate Service Provider self-signed Certificate,*

(4) *reading data with access condition ALWAYS*

(5) *generating random numbers*

(6) *generating a hash*

(7) *execution of INTERNAL AUTHENTICATE with PrK.eGK.AUT*

(8) *Identification by providing the users eHC-PIN*

(9) *identification by providing the users certificate*[61]

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.

Note by the ST-author 29:

The list has been completed by reading data with access condition ALWAYS, generating random numbers and setting security environments which does not contradicts the policy SFP_access_rules. Note that there are actions which could be done without identification and authentication but are not TSF-mediated actions and are therefore not part of this SFR, for example selecting files.

[61] version PP: [assignment: *list of TSF-mediated actions, including*

(1) reading the ATR

(2) reading the Card Verifiable Authentication Certificate,

(3) reading the Certificate Service Provider self-signed Certificate,

(4) Identification by providing the users eHC-PIN

(5) identification by providing the users certificate]; version CC part 2: [assignment: *list of TSF-mediated actions*]

Note also that this SFR is meant to support the access control policy SFP_access_rules. Access rules for the initialisation and personalisation phases are defined by the management SFRs (FMT_MTD.1).

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

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to Card-to-Card Authentication Mechanism [62].

Dependencies: No dependencies.

Note by the ST-author 30:

The Card-to-Card Authentication Mechanism required in this protection profile is based on asymmetric cryptographic primitives as required by FCS_COP.1/CCA_SIGN and FCS_COP.1/CCA_VERIF or on symmetric cryptography using FCS_COP.1/TDES and uses the freshness generated by the TOE random data (see FCS_RND.1) as challenge to prevent reuse of a response generated in a successful authentication attempt.

6.1.3 Access Control

The Security Function Policy (SFP) **SFP_access_rules,** which as defined in the security objective OT.Access_Rights (section 4.1.1), is used in 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 access control policy **SFP_access_rules** is only defined for the End Usage phase of the TOE. Note, that access rules for initialisation and personalisation phases are defined by management SFRs (FMT_MTD.1, see section 6.1.4), not by an explicit policy.

The following SFRs require the TOE to enforce the security policy SFP_access_rules. Note that all subjects, objects, security attributes, access methods and access rules are defined already in this policy. Therefore all of the following SFRs simply refer to this policy in all assignments.

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

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

FDP_ACC.2 Complete Access Control

Hierarchical to: FDP_ACC.1.

FDP_ACC.2.1 The TSF shall enforce the SFP_access_rules[63] on all subjects and objects defined by SFP_access_rules[64] 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

Note by the ST-author 31:

Keys and other data for creation of qualified signatures are out of scope of this Security Target.

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

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the SFP_access_rules[65] to objects based on the following: all subjects and objects together with their respective security attributes as defined in SFP_access_rules[66].

---

63 *[assignment: access control SFP]*

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

65 [assignment: *access control SFP*]

66 [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*]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: rules for all access methods and the access rules defined in SFP_access_rules[67].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[68].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rule: rules for all access methods and the access rules defined in SFP_access_rules[69].

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

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

FDP_RIP.1/RES_DESAL Residual Information Protection (dealocation)

Hierarchical to: No other components.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[70] the following objects:

- *PIN (either PIN.home or PIN.CH)*
- *secret and private cryptographic keys[71].*

Dependencies: No dependencies.

FDP_RIP.1/RES_AL Residual Information Protection (alocation)

Hierarchical to: No other components.

---

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

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

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

[70] Fulfilled selection of the PP; version of the PP: *[selection: allocation of the resource to, deallocation of the resource from]*

[71] Fulfilled selection of the PP; version of the PP: *[selection: list of objects at least including: PINs, secret and private cryptographic keys, data in all files, which are not freely accessible], version CC part 2: [assignment: list of objects]*

FDP_RIP.1.1 *The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource from*[72] *the following objects:*

- *all new created files*[73].

Dependencies: *No dependencies.*

Note by the ST-author 32:

One iteration has been used. This ST distinguish between the PIN and keys, which will be deleted upon dealocation and other data which will be at least deleted, when the memory space is allocated again.

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

The following data have the user data attribute "integrity checked data":

- RADs and VADs of all PINs (either PIN.home or PIN.CH)
- all cryptographic keys
- security relevant status variables of the card: authentication status for the PINs, authentication status for mutual authenticate
- input data for electronic signatures
- user data in files on the card
- access rules for files
- card life cycle status

FDP_SDI.2 Stored Data Integrity

Hierarchical to: FDP_SDI.1.

[72] Fulfilled assignment of the PP; version of the PP: *[assignment: allocation of the resource to, deallocation of the resource from]*

[73] Fulfilled assignment of the PP; version of the PP: *[assignment: list of objects at least including: PINs, secret and private cryptographic keys, data in all files, which are not freely accessible], version CC part 2: [assignment: list of objects]*

FDP_SDI.2.1

- The TSF shall monitor user data stored within the TSC for integrity errors[74] on all objects, based on the following attributes: *integrity checked data*[75].

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[76].

Dependencies: No dependencies.

Note by the ST-author 33:

No iteration has been used for FDP_SDI.2. Distinguishing between different types of data seems not be necessary for the ST.

6.1.3.1 Inter-TSF-Transfer

Note by the ST-author 34:

FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1 require the TOE to protect User Data transmitted between the TOE and a connected device by secure messaging with encryption and message authentication codes after successful authentication of the remote device. The authentication mechanisms as part of the Card-to-Card Authentication Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging. The rules for the data transfer are defined in the security policy **SFP_access_rules** defined in objective OT.Access_Rights (section 4.1.1).

---

[74] *[assignment: integrity errors]*

[75] Version of the PP: *[assignment: user data attributes – the attributes shall be chosen in a way that at least the following data are included:*
• PINs,
• cryptographic keys,
• security relevant status variables of the card (e. g. authentication status for the PIN or for mutual authenticate)
• input data for electronic signatures
• user data in files on the card,
• file management information (like access rules for files), and
• the card life cycle status
]; version of CC part 2: *[assignment: user data attributes]*

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

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

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

FDP_UCT.1.1 The TSF shall enforce the SFP_access_rules [77] to be able to transmit and receive[78] 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]

Note by the ST-author 35:

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

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

FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

FDP_UIT.1.1 The TSF shall enforce the SFP_access_rules [79] to be able to transmit and receive [80] user data in a manner protected from modification, deletion, insertion and replay [81] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [82] has occurred.

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

---

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

78 [selection*: transmit, receive*]

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

80 [selection*: transmit, receive*]

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

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

Note by the ST-author 36::

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

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

FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other components.

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit the remote trusted IT product[83] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for all functions requiring a trusted channel as defined by SFP_access_rules[84].

Dependencies: No dependencies.

6.1.4 Security Management

Note by the ST-author 37:

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

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1	The TSF shall be capable of performing the following

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

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

security management functions:

1. Initialization
2. Personalization
3. the “Service_Card_Management”
4. Modification of the PIN [85].

Dependencies: No Dependencies

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

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1	The TSF shall maintain the roles Health Professional, Medical Assistant, Security Module Card (health care), Self Service Terminal, Health Insurance Agency Service Provider, Combined Services Provider, Cardholder, Download Service Provider, Personalisation Service Provider, TOE Manufacturer [86].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1.

Note by the ST-author 38:

The Cardholder, Health Professional, Medical Assistant, Security Module Card (health care), Self Service Terminal, Health Insurance Agency Service Provider, Combined Services Provider and Download Service Provider are authenticated by services defined in this ST coming from the eHC-PP [28]. The method, how the TOE authenticates the Personalisation Service Provider and TOE Manufacturer is part of the TSFs of this ST and of other evaluation documents. Note, that the PP explicitly allows, that these roles are identical.

Note by the ST-author 39:

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.

---

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

86 [assignment: *the authorised identified roles*]

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.[87]

Dependencies: FMT_LIM.2 Limited availability.

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.[88]

Dependencies: FMT_LIM.1 Limited capabilities.

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

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

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

FMT_MTD.1/Ini Management of TSF data - Initialisation

Hierarchical to: No other components.

FMT_MTD.1.1/Ini	The TSF shall restrict the ability to write [89] the initialisation data [90] to the TOE Manufacturer [91].

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

Note by the ST-author 40:

As discussed in section 2.1.3 “TOE life cycle“ the delivery of the TOE might be organised in a way, that hardware and initialisation data are two separate parts of the TOE during delivery. When hardware and initialisation data have been delivered as separate parts of the TOE the process guarantees that the initialisation data could not be modified by the party, which stores them into the hardware.The method used to guarantee the authenticity of the data implicitly also authenticates the TOE Manufacturer as the source of the data. So the SFR FMT_MTD.1/Ini is fulfilled even if the command(s) to write the initialisation data is sent technically by a party different from the TOE Manufacturer.

FMT_MTD.1/Pers Management of TSF data - Personalisation

Hierarchical to: No other components.

FMT_MTD.1.1/ Pers	The TSF shall restrict the ability to write [92] the personalisation data [93] to thePersonalisation Service Provider [94].

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

---

[89] [selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]
[90] [assignment: *list of TSF data*]
[91] [assignment: *the authorised identified roles*]
[92] [selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]
[93] [assignment: *list of TSF data*]
[94] [assignment: *the authorised identified roles*]

Note by the ST-author 41:

Note, that the management of applications during the end usage phase is not a task for the "Personalisation Service Provider" but for the "Download Service Provider".

FMT_MTD.1/CMS Management of TSF data – Card Management

Hierarchical to: No other components.

FMT_MTD.1.1/ CMS

The TSF shall restrict the ability to write [95] the

1. File structures for additional Applications,
2. Cryptographic Keys for additional applications,
3. PINs and other user authentication reference data for additional applications and
4. Access Rights for additional applications [96]

to the Download Service Provider. [97].

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

FMT_MTD.1/PIN Management of TSF data – Human User Authentication data

Hierarchical to: No other components.

FMT_MTD.1.1/ PIN

The TSF shall restrict the ability to modify and unblock [98] the PIN [99] to the Cardholder [100].

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

Note by the ST-author 42:

The cardholder 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)

---

95 [selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]

96 [assignment: *list of TSF data*]

97 [assignment: *the authorised identified roles*]

98 [selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]

99 [assignment: *list of TSF data*]

100 [assignment: *the authorised identified roles*]

the command RESET RETRY COUNTER and providing the PUC (without a new PIN). The PIN.home and the PIN.CH will be handled separately in this context.

Note by the ST-author 43:

The following SFR addresses the protection of the keys as part of the TSF data. Note that other keys are user data under protection according to SFR FDP_ACF.1.

FMT_MTD.1/KEY_MOD Management of TSF data – Key Management

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_MOD	The TSF shall restrict the ability to modify [101] the Public Key for CV Certification Verification [102] to none [103].

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

6.1.5 General Security Functions

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.

The TOE shall meet the requirement “TOE Emanation (FPT_EMSEC.1)” as specified below (Common Criteria Part 2 extended):

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

---

[101] [selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]

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

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

FPT_EMSEC.1.1 The TOE shall not emit *information about IC power consumtion and command execution time*[104] in excess of *non useful information*[105] enabling access to

1. PIN and PUC[106]

and

2. Card Authentication Private Keys,
3. Client-Sever Authentication Private Key
4. Document Cipher Key Decipher Key
5. secure messaging keys [107].

FPT_EMSEC.1.2 The TSF shall ensure any user [108] are unable to use the following interface smart card circuit contacts [109] to gain access to

1. PIN and PUC[110]

and

2. Card Authentication Private Key,
3. Client-Sever Authentication Private Key
4. Document Cipher Key Decipher Key
5. secure messaging keys [111].

Dependencies: No other components.

Note by the ST-author 44:

The TOE is preventing attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. As the underlying chip hardware is contact based power consumption and timing of signals are ways to gain secret information of the TOE and have therefore be considered in this SFR.

---

104 [*assignment: types of emissions*]
105 [assignment: *specified limits*]
106 [assignment: *list of types of TSF data*]
107 [assignment: *list of types of user data*]
108 [assignment: *type of users*]
109 [assignment: *type of connection*]
110 [assignment: *list of types of TSF data*]
111 [assignment: *list of types of user data*]

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

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

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

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

1. exposure to operating conditions where therefore a malfunction could occur,
2. failure detected by TSF according to FPT_TST.1 [112]

Dependencies: ADV_SPM.1 Informal TOE security policy model

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

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing [113] to the TSF [114] by responding automatically such that the TSP is not violated.

Dependencies: No dependencies.

Note by the ST-author 45:

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

---

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

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

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

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

FPT_TST.1.1 The TSF shall run a suite of self tests *at the request of the authorised user*[115] to demonstrate the correct operation of *the TSF*[116].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity *of TSF data*[117].

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.

Note by the ST-author 46:

The TOE will run some self tests at the request of the authorised user and some self tests automatically as described in FPT_TST.1.

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

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

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.

[115] [*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*]]

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

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

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

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.

Note by the ST-author 47:

Those parts of the TOE which support the security functional requirements “TSF testing (FPT_TST.1)” and “Failure with preservation of secure state (FPT_FLS.1)” are protected from interference of the other security enforcing parts of the chip Embedded Software. The security enforcing functions and application data shall be separated in way preventing any inference.

6.2 Security Assurance Requirements for the TOE

The assurance components 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.

The minimum strength of function is SOF-high. This ST contains with FCS_RND a security functional requirement, which explicitly claims a strength of function.

6.3 Security Requirements for the IT environment

This security target does not describe security functional requirements for the IT environment as the PP [28] does not describe security functional requirements for the IT environment.

7 TOE Summary Specification

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

7.1 TOE Security Functions

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

In the following table all TOE Security Functions are listed and if appropriate a SOF claim is stated. The assessment of cryptographic algorithms is not part of this CC evaluation.

Table 5 SOF claims for TOE Security Functions

TOE Security Function	SOF claim	Description
SF.ACCESS	not appropriate	This TOE Security Function is not realised by a probabilistic or permutational noncryptographic mechanism.
SF.ADMIN	not appropriate	This TOE Security Function is not realised by a probabilistic or permutational noncryptographic mechanism.
SF.AUTH	high	There is a probabilistic password mechanism for the authentication of the cardholder and a related probabilistic reseting code for a blocked password.
SF.CRYPTO	high	The random number generators and hash functions are probabilistic mechanisms.
SF.TRUST	not appropriate	This TOE Security Function is not realised by a probabilistic or permutational noncryptographic mechanism.
SF.PROTECTION	not appropriate	This TOE Security Function is not realised by a probabilistic or permutational noncryptographic mechanism.
SF.IC_SF	high	Several Security Functions of the IC are realised by probabilistic or permutational noncryptographic mechanisms as stated in the IC-evaluation.

7.1.1 SF.ACCESS Access Control

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

This Security Function is composed of:

1. Maintenance of the user security attributes „identity“ and „role“.
2. Maintenance of the roles: Cardholder, Download Service Provider, Personalisation Service Provider, TOE Manufacturer, Health Professional, Medical Assistant,

Security Module Card (health care), Self Service Terminal, Health Insurance Agency Service Provider, Combined Services Provider.

3. Access rules for data in life-cycle phase 7:

   All allowed read-,write-,delete-,activate-,deactivate-,create-access rules for assets are described in table 7. If an access to an asset is not explicitly allowed by this table it is not possible. In table 8 additional access rules for other data are described.

   Note that the identifiers from table 6 will be used in the further description of this TSF. The role IDs in table 6 are part of the certificates provided by a health professional card or a Security Module Card.

   In chapter 3.1.2 more information on the relationchip of subjects and role IDs could be found.

table 6 Description of identifiers used in this TSF

Subject	identifier	Role IDs of the CVCs
Health Insurance Agency Service Provider	h_ins	
Download Service Provider	dsp	
Combined Services Provider	csp	
Cardholder authenticating with PIN.CH	c_holder _pinch	
Cardholder authenticating with PIN.home	c_holder _pinhome	
Health Professional	h_prof	‘2A’, ‘3A’, ‘4A’, ‘5A’, ‘7A’
Health Professional (doct)	h_prof_d	‘2A’
Health Professional (pharmacy)	h_prof_p	‘3A’
Health Professional (psychotherapists)	h_prof_psy	‘4A’
Health Professional (extra)	h_prof_ext	‘5A’
Health Professional (emergency)	h_prof_not	‘7A’
Medical Assistant	m_assis	‘2A’, ‘3A’, ‘4A’, ‘5A’, ‘7A’
Medical Assistant (doct)	m_assis_d	‘2A’
Medical Assistant (pharmacy)	m_assis_p	‘3A’
Medical Assistant (psychotherapists)	m_assis_psy	‘4A’
Medical Assistant (extra)	m_assis_ext	‘5A’
Medical Assistant (emergency)	m_assis_not	‘7A’
Security Module Card	smc	‘2A’, ‘3A’, ‘4A’, ‘5A’,’6A’
Security Module Card without online pharmacy	smc_hc	‘2A’, ‘3A’, ‘4A’, ‘5A’, ‘7A’
Security Module Card (Online pharmacy)	smc_op	‘6A’
Security Module Card (doct)	smc_d	‘2A’
Security Module Card (pharmacy)	smc_p	‘3A’
Security Module Card (psychotherapists)	smc_psy	‘4A’
Security Module Card (extra)	smc_ext	‘5A’
Security Module Card (emergency)	smc_not	‘7A’
Self Service Terminal	Sst	‘1A’

table 7 read-, write-, delete-, activate-, deactivate-access rules for assets

data	access	subject	sm required
EF.PD, EF.VD,	write	h_ins, csp	yes
	read	All	no

EF.StatusVD			
EF.GVD	write	h_ins, csp	yes
	read	c_holder_pinhome, h_prof, m_assis, smc_hc	no
		smc_op, h_ins, csp	yes
EF.eRezept-Tickets,	read and write	h_prof_d, h_prof_ext, h_prof_p, m_assis_d, m_assis_ext, m_assis_p, smc_d, smc_ext, smc_p	no
	read and write	smc_op	yes
	deactivate, activate, delete	c_holder_pinhome + sst	no
	read	c_holder_pinhome	no
EF.eRezept_Container EF.StatusRezept	read	all	no
	write	h_prof_d, m_assis_d, smc_d	no
EF.Logging[118]	write	h_prof, m_assis, smc_hc, sst	no
	write	smc_op	yes
	read	c_holder_pinhome	no
EF.CVC	read	all	no
Display Message (EF.DM in DF.HCA and EF.DM in DF.ESIGN)	write	c_holder_pinhome	no
	read	All when using either mutual authentication based on asymmetric cryptography with establishment of a secure channel (Service_Asym_Mut_Auth_with_SM) or mutual authentication based on symmetric cryptography with establishment of a secure channel (Service_Sym_Mut_Auth_with_SM).	Yes
X.509 Certificates EF.C.CH.AUT, EF.C.CH.ENC, EF.C.CH.ENCV	read	all	no
	write	dsp, csp	yes
X.509 Certificate EF.C.CH.AUTN	read	h_prof_d, h_prof_p, m_assis_d, m_assis_p, smc_d, smc_p	no
	write	dsp, csp	no
EF.Einwilligung	read	c_holder_pinhome, h_prof_p, h_prof_d, m_assis_p, m_assis_d, smc_p, smc_d,	no
	read	smc_op	yes
	write	h_prof_d + c_holder_pinch, m_assis_d + c_holder_pinch, smc_d + c_holder_pinch, h_prof_p + c_holder_pinch,	no

[118] Only new entries can be appended, existing entries can not be modified (however, when fifty entries are full, the oldest entry is deleted, when adding a new one).

		m_assis_p + c_holder_pinch, smc_p + c_holder_pinch	
EF.Verweis	read	all	no
	write	csp, dsp	yes
	write	h_prof_p + c_holder_pinch, h_prof_d + c_holder_pinch, m_assis_p + c_holder_pinch, m_assis_d + c_holder_pinch, smc_p + c_holder_pinch, smc_d + c_holder_pinch	no
EF.eNotfalldaten EF.StatusNotfalldaten	write	h_prof_d + c_holder_pinch m_assis_d + c_holder_pinch smc_d + c_holder_pinch	no
	read	h_prof, m_assis, smc_hc	no
	Deactivate, activate,	c_holder_pinhome + sst	no
DF.HCA[119]	Deactivate, activate	h_ins, dsp. csp	yes

table 8 access rules for other data objects

ATR	read	all	no
Files and data for additional applications	create	dsp, csp	yes

4. <u>Access rules for the life-cycle phase 7 concerning usage of the PINs/PUCs:</u>

   - Data of type RAD (eHC): The PIN.CH and PIN.home may be modified only by the cardholder with the corresponding PIN or PUC. The corresponding resetting codes of the PIN.CH (PUC.CH) or of the PIN.home (PUC.home) cannot be modified. The retry counter for a blocked PIN.CH or the retry counter of a blocked PIN.home can be reseted by the cardholder after authentication with the corresponding PUC (PUC.CH to reset the retry counter of PIN.CH and PUC.home to reset the retry counter of PIN.home). The retry counter of an unblocked PIN.CH will be reseted, when the PIN.CH has been entered correctly. The retry counter of an unblocked PIN.home will be reseted, when the PIN.home has been entered correctly. Note: VAD (eHC) stands for PIN or resetting code values, which are entered by the cardholder in clear text and therefore require no specific rules by this policy.

[119] DF.HCA conatins all of the assets of this table except the CVC- or X.509-certificates.

5. Access for the life-cycle phase 7 concerning the usage of keys:

   - PrK.eGK.Aut can only be used for mutual authentication based on asymmetric cryptography either with or without secure messaging (Service_Asym_Mut_Auth_w/o_SM and Service_Asym_Mut_Auth_with_SM). These services include the verification of a CV certificate for the card or security module, with which the TOE interacts during the service.

   - PrK.CH.Aut and PrK.CH.AUTN can only be used for client-server authentication mechanism based on asymmetric cryptography (services Service_Client_Server_Auth). Prk.CH.ENC and PrK.CH.ENCV can only be used for the service of data decryption based on asymmetric cryptography according to PKCS#1 (Service_Data_Decryption). The usage of PrK.CH.Aut and of Prk.CH.ENC are only possible after authentication by c_holder_pinhome. The usage of the key PrK.CH.AUTN requires authentication by one of the following: sst, h_prof_p, h_prof_d, h_prof_psy, h_prof_ext, m_assis_p, m_assis d, m_assis psy, m_assis_ext, smc_p, smc_d, smc_psy, smc_ext. The usage of the key PrK.CH.ENCV requires authentication by one of the following: h_prof_p, m_assis_p, smc_p, smc_op. In case of smc_op this requires secure messaging with encryption and MAC.

   - EF.Puk can only be used for verification of certificates. Note: Additional Public keys may be stored temporarily in case of cross-certification. The above rule holds for the “root” key of the eHC.

   - The symmetric keys SK.VSDD, SKVSDDCAMS and SK.CAMS can only be used for establishment of trusted channels in the mutual authentication process based on symmetrical cryptography (service Service_Sym_Mut_Auth_with_SM).

6. Performing other TSF-mediated actions in life-cycle phase 7:

   All can always:

   - read data with access condition always
   - generate random numbers,
   - generate a hash.

An SOF claim for this TSF is not appropriate, as this TSF is not realised by a probabilistic or permutational noncryptographic meachnism.

7.1.2 SF.ADMIN Administration of the TOE

The administration of the TOE is managed by this Security Function. The TOE administration is partly done in the initialisation, personalisation and usage phase. This TSF conatins administration tasks for all of these phases.

1. The TOE Manufacturer authenticates with an authentication mechanism for the initialisation phase. Mechanism that guarantees that only initialisation data authorised by the TOE Manufacturer will be accepted by and loaded into the TOE. The Personalisation Service Provider authenticates with an authentication mechanism for the personalisation phase. Mechanism that guarantees that only personalisation data authorised by the Personalisation Service Provider will be accepted by and loaded into the TOE.
2. A mechanism to write initialisation data by the TOE Manufacturer.
3. A mechanism to write personalisation data by the Personalisation Service Provider (also known as personaliser in the eHC-PP [28]).
4. The Download Service Provider (using the symmetric key: SK.CAMS), the Health Insurance Agency Service Provider (using the symmetric key: SK.VSDD) and the Combined Services Provider (using the symmetric key: SK.VSDDCAMS) will be authenticated by a mutual authentication based on symmetric cryptography with random challenge and a corresponding response using fresh generated random numbers.
5. Performing the *Service_Card_Management* including creation of new applications and management of existing applications to the card management system which could either represent the Download Service Provider, the Health Insurance Agency Service Provider and the Combined Services Provider (see [8], 7 and 9).

An SOF claim for this TSF is not appropriate, as this TSF is not realised by a probabilistic or permutational noncryptographic meachnism.

7.1.3 SF.AUTH Authentication of the Cardholder

The authentication of the eHC cardholder is managed by this Security Function. This Security function is only active during the usage phase.

This Security Function is composed of:

1. The Cardholder will be identified and authenticated by a PIN authentication mechanism: There are two separately handled PIN/PUC-mechanism: PIN.CH and PIN.home and the corresponding PUCs. If there are more than 3 consecutive failed authentication attempts for PIN.CH the PIN.CH is blocked until successful unblock with PUC.CH. If there are

more than 3 consecutive failed authentication attempts for PIN.home the PIN.home is blocked until successful unblock with PUC.home.

2. Reseting Code (PUC) for the PIN: When 10 successful or unsuccessful authentication attempts with thePUC.CH have been met the PUC.CH is blocked. When 10 successful or unsuccessful authentication attempts with the PUC.home have been met the PUC.home is blocked.
3. Modification mechanism for PIN.home or PIN.CH for the Cardholder. Modification of an unblocked PIN (either PIN.CH or PIN.home) could be done by authentication of the Cardholder with his corresponding PIN (either PIN.CH or PIN.home). Modification of a blocked PIN (either PIN.CH or PIN.home) could be done by the Cardholder with his corresponding resetting code (either PUC.CH to modify PIN.CH or PUC.home to modify PIN.home).

This Security Function has the level of strength SOF-high.

7.1.4 SF.CRYPTO Cryptographic Support

This Security Function provides the cryptographic support for the other Security Functions or describes cryptographic services which could be used.

This Security Function is composed of:

1. Calculating hash values according to SHA-1, SHA-2 (224 bit, 256 bit, 384 bit, 512 bit) and RIPEMD-160 that meets the FIPS 180-2 standard.
2. Triple-DES in CBC mode callculation (encryption and decryption) with 112 bit key sizes in accordance with FIPS 46-3. This will be used e.g. for encryption of data in a trusted channel or for retail MAC calculation compliant to ANSI X9.19.
3. Random number generation, e.g. used for key generation and authentication process. There are two random number generators. The deterministic one is rated K3 (high) according to AIS20 [5]. To provide random numbers generated by the physical generator this security function calls SF.IC_SF.
4. RSA calculation with key sizes between 1024 and 2048 bit.
5. Support for client/server-authentication: Digital signature creation according to RSA with key sizes between 1024 and 2048 bit module length, which is compliant to PKCS#1. This service could be used to authenticate the TOE against a server in a client/server-authentication process.
6. Support for data decryption: RSA decryption with key sizes between 1024 and 2048 module length that is compliant to PKCS#1. This service allows to use the TOE as a data decryption token.
7. Calculation of block check values to insure data integrity.

This Security Function has the level of strength SOF-high.

7.1.5 SF.TRUST Authentication and Trusted Communication

This Security Function manages asymmetric Card-to-Card authentication for HPC- or SMC-owners, the establishing of a secure channel and the protection of communication data. This SF will only be used during end-usage phase.

1. The Health Professional, the Medical Assisstant,the Security Module Card (health care) and the Self Service Terminal will be identified by the role-id as part of a CV-certificate send to the TOE. These roles will be authenticated by mutual authentication based on asymmetric cryptography with random challenge and a corresponding response using fresh generated random numbers compliant to ISO/IEC9796-2 (DS scheme 1).
2. Establishment of a trusted channel with negotiation of randomly generated symmetric cryptographic 3-DES keys used for the protection of the communication data based on either a symmetric or an asymmetric mutual authentication process.
3. As part of the trusted channel: Ensuring the confidentiality of communication data by encrypting the communication data by using symmetric cryptography with a generated session key.
4. As part of the trusted channel: Ensuring the integrity of communication data sequences (= commands), e.g. by calculating a cryptographic checksum using symmetric cryptograhy with a generated session key to avoid data modification, or by command chaining with a random initial sequence counter to avoid deletion, insertion and replay of complete commands.
5. When the trusted channel will be terminated by reaching fail secure state, or a reset of the smart card the symmetric session keys used for the trusted channel will be physicaly deleted.

An SOF claim for this TSF is not appropriate, as this TSF is not realised by a probabilistic or permutational noncryptographic meachnism.

7.1.6 SF.PROTECTION Protection of TSC

This Security Function protects the TSF functionality, TSF data and user data.

This Security Function is composed of:

1. Upon de-allocation of resources from the PIN (PIN.home or PIN.CH), secret and private cryptographic keys the information content of these resources is physically deleted
2. At least upon allocation to all new created files the information content of these resources will be physically deleted.

3. Checking the integrity of PINs, cryptographic keys, security relevant status variables of the card, input data for electronic signatures, user data in files on the card, file management information and the card life cycle status, when using them and inform the connected entity in the case of integrity errors.
4. Test features of the TOE after TOE delivery: In life-cycle phase 5 selftests will be performed at the request of the authorised user to demonstrate the correct operation of the hard- and software including all TSFs. In addition test features are provided to the authorised users, in life cycle phase 5 to demonstrate the integrity of the TSF executable code.

   In life-cycle phase 7 only selftests could be triggered by the user. Triggering these selftests allows the user to verify the integrity of TSF data and of TSF executable code. In case of a security violation the user will be informed and the data or code will not be accessible.

   The selftests in all life-cycle phases are mechanisms separated from the rest of the TOE with very limited functionality. The selftests are not configurable and could be triggered but not modified. Disclosure or modification of assets by the test features is not possible.
5. Hiding information about IC power consumption and command execution time, to ensure that the IC contacts can not be used to gain access to PIN and PUC, Card Authentication Private Keys, Client-Server Authentication Private Key, Document Cipher Key Decipherment Key, secure messaging keys.
6. Before a command will be executed all TSFs are active.

An SOF claim for this TSF is not appropriate, as this TSF is not realised by a probabilistic or permutational noncryptographic meachnism.

7.1.7 SF.IC_SF Security Functions of the IC

This Security Function covers the Security Functions of the physical behaviour of the TOE.

This Security Function is composed of:

1. Detection of physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation.
2. Resistance to physical tampering of the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. This mechanism is not configurable. The design of the hardware protects it against analysing and physical tampering.
3. Random Number generation rated P2 (high) according to AIS31 [6].

4. Cryptographic support for DES calculations with cryptographic key sizes of 112 bit that comply to FIPS PUB 46-3, 1999 October 25, keying option 2 and support for RSA calculations, with cryptographic key sizes of 1024 to 2048 bit that comply with ISO/IEC 9796-1, Annex A, section A.4 and A.5 and Annex C.

This Security Function has the level of strength SOF-high.

7.2 Assurance Measures

This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 6.2.

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

Assurance Measures	Description
AM_ACM	The configuration management is described in GDM_eHC_ACM_00.
AM_ADO	The delivery, installation, generation and start-up of the TOE is described in GDM_eHC _ADO_00.
AM_ADV	The representing of the TSF is described in GDM_eHC _ADV_SPM_00 for security policy modelling, in GDM_eHC _ADV_FSP_00 for functional specification, in GDM_eHC _ADV_HLD_00 for high level design, in GDM_eHC _ADV_LLD_00 for low level design, in GDM_eHC _ADV_IMP_00 for implementation representation and in GDM_eHC _ADV_RCR_00 for representation correspondence.
AM_AGD	The guidance documentation is described in GDM_eHC _AGD_USR_00 for the user and in GDM_eHC _AGD_ADM_00 for the administrator.
AM_ALC	The life cycle support of the TOE during its development and maintenance is described in GDM_eHC _ALC_00
AM_ATE	The testing of the TOE is described in GDM_eHC _ATE_00.
AM_AVA	The vulnerability assessment for the TOE is described in GDM_eHC _AVA_MSU_00 for the misuse, in GDM_eHC _AVA_SOF_00 for the strength of TOE security functions and in GDM_eHC _AVA_VLA_00 for the vulnerability analysis.

Figure 7-1: Refeence of Assurance Measures

Note: Reference endnumbers may change during evaluation process (e.g. GDM_eHC _AVA_VLA_00 may become GDM_eHC _AVA_VLA_02).

8 PP Claims

8.1 PP Reference

The conformance of this ST to the eHC Protection Profile [28] is claimed.

There are no additional security objectives in this ST, that are not part of [28].

There are no additional security requirements in the ST, that are not part of [28] except of the following iterations:

- FIA_AFL.1/PIN from [28] has been iterated to FIA_AFL.1/PIN.CH and FIA_AFL.1/PIN.home
- FIA_AFL.1/PUC from [28] has been iterated to FIA_AFL.1/PUC.CH and FIA_AFL.1/PUC.home
- FDP_RIP.1 from [28] has been iterated to FDP_RIP.1/Res_Desal and FDP_RIP.1/Res_Al

9 Rationale

The section 9.1 have been taken from the sections 4.4 from [28] without modifications. In section 9.2 additional text has been included compared to section 5.4 of [28] to cover the interations that have been included in this document. In case of a change this has been described in a ‘note by the ST-author’.

9.1 Security Objectives Rationale

The following table shows, which Objectives for the TOE and the environment support which OSP, help to avert which threat and correspond to which assumption. The table shows, that for every OSP, threat and assumption there is at least one objective and vice versa.

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Services	OT.Cryptography	OT.Prot_Inf_Leak	OT.Prot_Phys_Tamper	OT.Prot_Malfunction	OT.Prot_Abuse_Func	OD.Assurance	OD.Material	OE.Users	OE.Legal_Decisions	OE.Data_Protection	OE.User_information	OE.Perso
OSP.eHC_Spec	X	X	X	X	X											
OSP.Additional_Applications			X													X
OSP.Electronic_Prescriptions		X											X	X		
OSP.User_Information															X	
OSP.Legal_Decisions													X			
OSP.Services				X												
OSP.Logging		X		X									X			
OSP.Manufact										X	X					
T.Compromise_Internal_Data	X	X		X	X								X	X		
T.Forge_Internal_Data	X	X		X	X								X	X		
T.Misuse	X	X		X	X								X	X		
T.Intercept	X	X		X	X								X	X		
T.Phys_Tamper							X									
T.Information_Leakage						X										
T.Malfunction								X								
T.Abuse_Func									X							
A.Users												X				
A.Perso																X

Table 9: Mapping of objectives to OSPs, threats, assumptions[120]

[120] In OSP.Electronic_Prescriptions a ‚x’ has been set in addition to the PP. Note, that the informal text below the table already covers this link in the eGK-PP and no additional text in the ST had to be included.

The following text describes for every OSP, Threat and Assumption, how they are covered by Security Objectives.

The organizational security policy **OSP.eHC_Spec** “Compliance to eHC specifications” is implemented by the following TOE security objectives:

- OT.Services requires that the TOE provides the security services, which are realised by the commands defined in the specification.
- OT.Cryptography requires that the cryptographic algorithms as defined in the specification are implemented.
- OT.Access_Rights requires that the access rights are defined according to the policy SFP_access_rules. These rules are chosen according to the access rights defined in the eHC specification, part 2, annex B.
- OT.Additional_Applications requires rules for the loading of additional applications, which is also compatible to the definitions in the specifications.
- The objectives for the TOE environment OD.Material and OE.Perso “Secure personalization” (the latter together with OT.AC_Pers “Access control for personalization” protecting the personalization functions of the TOE) ensure that the Personalisation Service Provider will provide a genuine TOE initialized and personalized according to the specification to the Cardholder.

OSP.Additional_Applications is fully covered by OT.Additional_Applications, which is essentially identical to OSP.Additional_Applications. In addition it is supported by OE.Perso because this security objective requires adequate organisational security, when loading additional applications during the operational phase.

OSP.Electronic_Prescriptions is covered by the combination of

- OT.Access_Rights, which restricts the access rights to the data in the card as required by OSP.Electronic_Prescriptions (see rule for the asset “electronic prescription”).
- OE.Data_Protection, which requires adequate protection of the medical data, when handled outside of the card.
- OE.Legal_Decisions, which requires use of IT systems according to legal requirements by authorised persons. This in particular implies that the access possibilities by HPC or SMC cards to data in the eHC is used according to the legal requirements.

OSP.User_Information is fully covered by OE.User_Information, which is essentially identical to OSP.User_Information.

OSP.Legal_Decisions is fully covered by OE.Legal_Decisions, which is essentially identical to OSP.Legal_Decisions.

OSP.Services is fully covered by OT.Services, which is essentially identical to OSP.Services.

OSP.Logging is realised in cooperation between the TOE and its operational environment:

- According to OT.Services the TOE provides the service “
-
- **Service_Logging**”. This service allows authorised users to write logging data into the card.
- According to OE.Legal_Decisions all authorised users are responsible for the correctness of the logging data, they write into the card. This compensates for the fact that the card cannot control the content of this file.
- According to OT.Access_Rights, access to the log file is protected.

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 OSP **OSP.Manufact** “Manufacturing of the Smart Card” in the development and manufacturing of the TOE.

The threats **T.Compromise_Internal_Data, T.Forge_Internal_Data, T.Misuse** and **T.Intercept** are all countered by the following combination of objectives:

- OT.Access_Rights (supported by OT.Services, OT.Cryptography) implies that data in the TOE can only be read, written or modified according to the access rules as defined in the access control policy SFP_access_rules, which was defined in OT.Access_Rights. The support by OT.Services is needed since several rules of SFP_access_rules restrict the access to certain subjects (cardholder, health professional, etc.) the authenticity of which is made sure by services required by OT.Services (e.g. Service_User_Auth_PIN, Service_Sym_Mut_Auth_with_SM, Service_Asym_Mut_Auth_with_SM, cf. section 2.2). The support by OT.Cryptography is needed since several services required by OT.Services rely on cryptographic mechanisms required by OT.Cryptography (e.g. DES-3 for Service_Sym_Mut_Auth_with_SM, RSA for Service_Asym_Mut_Auth_with_SM).

- OT.AC_Pers protects the personalization functions of the TOE against unauthorised use.
- OE.Legal_Decisions and OE.Data_Protection imply that authorised persons, who are allowed to read, write or modify data in the card, use these rights only in an environment, where unauthorised access to these data is prevented by the environment.

An example for this is as follows: The service

Service_Asym_Mut_Auth_w/o_SM allows health professionals to access electronic prescriptions in the card. This is allowed only in a closed environment, where attackers cannot access the data transmitted between eHC and the health professionals IT equipment. For the case of transmission over insecure lines the service

Service_Asym_Mut_Auth_with_SM is provided and the objectives for the environment imply that health professionals use these services adequately.

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

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

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

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

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

The security objectives for the environment OE.Perso “Secure personalization” implements the assumption **A.Perso** “Personalization of the Smart Card”.

9.2 Security Requirements Rationale

9.2.1 Security Functional Requirements Coverage

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

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Services	OT.Cryptography	OT.Prot_Inf_Leak	OT.Prot_Phys_Tamper	OT.Prot_Malfunction	OT.Prot_Abuse_Func
FCS_CKM.1/SM				X	X				
FCS_CKM.4				X	X				
FCS_COP.1/SHA				X	X				
FCS_COP.1/CCA_SIGN				X	X				
FCS_COP.1/CCA_VERIF				X	X				
FCS_COP.1/CSA				X	X				
FCS_COP.1/RSA_DEC				X	X				
FCS_COP.1/TDES				X	X				
FCS_COP.1/MAC				X	X				
FCS_RND.1				X	X				
FIA_AFL.1/PIN.CH		X		X					
FIA_AFL.1/PIN.home		X		X					
FIA_AFL.1/PUC.CH		X		X					
FIA_AFL.1/PUC.home		X		X					
FIA_ATD.1		X		X					
FIA_UID.1	X	X		X					
FIA_UAU.1	X	X		X					
FIA_UAU.4				X					
FDP_ACC.2		X		X					
FDP_ACF.1		X		X					
FDP_RIP.1/Res_Desal		X	X						
FDP_RIP.1/Res_Al		X	X						
FDP_SDI.2		X							
FDP_UCT.1		X		X					
FDP_UIT.1		X		X					
FTP_ITC.1		X		X					

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Services	OT.Cryptography	OT.Prot_Inf_Leak	OT.Prot_Phys_Tamper	OT.Prot_Malfunction	OT.Prot_Abuse_Func
FMT_SMF.1	X	X	X	X					
FMT_SMR.1	X	X	X	X					
FMT_LIM.1		X	X						X
FMT_LIM.2		X	X						X
FMT_MTD.1/Ini	X	X	X	X					
FMT_MTD.1/Pers	X	X	X	X					
FMT_MTD.1/CMS		X	X	X					
FMT_MTD.1/PIN		X	X	X					
FMT_MTD.1/KEY_MOD		X	X	X					
FPT_EMSEC.1						X			
FPT_FLS.1						X		X	
FPT_PHP.3						X	X	X	
FPT_TST.1						X		X	
FPT_RVM.1		X	X			X		X	X
FPT_SEP.1		X	X			X		X	X

Table 10: Coverage of Security Objectives for the TOE by SFRs

9.2.2 Functional Requirements Sufficiency

The security objective **OT.AC_Pers** “Access control for personalization” is implemented by following SFRs:

1. the SFR FMT_SMR.1 defines the Personaliser as known role of the TOE and the SFR FMT_SMF.1 defines personalization as security management function,
2. 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),
3. the SFR FMT_MTD.1/Pers limit right to write personalisation data to the Personalisation Service Provider and
4. the SFR FMT_MTD.1/INI limiting the right to write any data before personalisation to the TOE Manufacturer, which in particular implies that the Personaliser role shall be created by the TOE Manufacturer.

The security objective **OT.Access_Rights** is the central security requirement for the TOE. Therefore it is supported by many of the SFRs. It is mainly implemented by

1. the SFRs FDP_ACC.2 and FDP_ACF.1, which require to implement the access rules defined in the security policy SFP_access_rules as defined in OT.Access_Rights,

and supported by

2. SFRs FIA_AFL.1/PIN.CH, FIA_AFL.1/PIN.home, FIA_AFL.1/PUC.CH, FIA_AFL.1/PUC.home, FIA_ATD.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD/PIN, which all support the security of the Cardholders PINs (PIN.CH and PIN.home) and the corresponding PUCs (PUC.CH and PUC.home).

Note by the ST-author 48:

In this description the refinement in the ST according to FIA_AFL.1/PIN and FIA_AFL.1/PUC has been managed by including FIA_AFL.1/PIN.CH, FIA_AFL.1/PIN.home, FIA_AFL.1/PUC.CH and FIA_AFL.1/PUC.home.

3. SFRs FIA_UID.1 and FIA_UAU.1, which support timing of Identification and authentication,
4. SFRs FDP_RIP.1/Res_Desal, FDP_RIP.1/Res_Al and FDP_SDI.2 (as well as all the more low-level oriented SFRs, which are not repeated here) prevent unwanted knowledge of secret data or unauthorised modification of the assets.

Note by the ST-author 49:

In this description the refinement in the ST according to FDP_RIP.1 has been managed by including FDP_RIP.1/Res_Desal and FDP_RIP.1/Res_Al.

5. the SFRs FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1 provide the trusted channel for the protection of the confidentiality and integrity of transmitted data, which is required by some of the rules in SFP_access_rules.
6. the SFRs FMT_MTD.1/Ini, FMT_MTD.1/Pers, FMT_MTD.1/CMS, FMT_MTD.1/KEY_MOD restrict the management of applications to authorised subjects and FMT_LIM.1 and FMT_LIM.2 prevent unauthorised use of management functions. Together they prevent the attempt to use management commands in order to bypass the access control policy.
7. FPT_RVM.1 and FPT_SEP.1 (together with the SFRs against low-level attacks, which are not repeated here) prevent any bypass of the access rules with methods below the command level.

The security objective **OT.Additional_Applications** covers the rules for the download of additional applications into the TOE. Therefore it is mainly supported by

1. FMT_MTD.1/CMS, which restricts download of additional applications to the Download Service Provider (as also required by SFP_access_rules).
2. The other SFRs on management functions FMT_SMF.1, FMT_SMR.1, FMT_LIM.1, FMT_LIM.2, FMT_MTD.1/Ini, FMT_MTD.1/Pers, FMT_MTD.1/PIN, FMT_MTD.1/KEY_MOD support this, because they restrict other management functions to authorised subjects
3. A more “low level” support is given by FPT_SEP.1, FPT_RVM.1 and FDP_RIP.1/Res_Desal and FDP_RIP.1/Res_Al, which require domain separation (which holds in particular separation between existing and additional applications), non-bypassability of security functions and the deletion of secret data before any memory area is re-used. (All hardware-oriented SFRs, which are not repeated here, also support non-bypassability.)

Note by the ST-author 50:

In this description the refinement in the ST according to FDP_RIP.1 has been managed by including FDP_RIP.1/Res_Desal and FDP_RIP.1/Res_Al.

The security objective **OT.Services** addresses the implementation and the access control of the TOE security services. The security services are implemented by the following SFR:

1. 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_COP.1/SHA, FCS_RND.1 and FIA_UAU.4.
2. the TOE security service **Service_Asym_Mut_Auth_with_SM** is implemented by the SFR FCS_CKM.1/SM, FCS_CKM.4, FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/SHA, FCS_RND.1, FCS_COP.1/TDES, FCS_COP.1/MAC and FIA_UAU.4. The trusted channel established by this service is described by SFRs FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1.
3. the TOE security service **Service_Sym_Mut_Auth_with_SM** is implemented by the SFR FCS_CKM.1/SM, FCS_CKM.4, FCS_RND.1, FCS_COP.1/TDES, FCS_COP.1/MAC and FIA_UAU.4. The trusted channel established by this service is described by SFRs FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1.
4. the TOE security service **Service_User_Auth_PIN** and **Service_User_Auth_PUC** are implemented by the SFRs FIA_AFL.1/PIN.CH, FIA_AFL.1/PIN.home, FIA_AFL.1/PUC.CH, FIA_AFL.1/PUC.home, FIA_ATD.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD/PIN, which all support

the security of the Cardholders eHC-PIN and PUC. Also it is supported by FDP_ACC.2 and FDP_ACF.1, because these SFRs require implementation of SFP_access_rules, which involves PIN authentication.

Note by the ST-author 51:

In this description the refinement in the ST according to FIA_AFL.1/PIN and FIA_AFL.1/PUC has been managed by including FIA_AFL.1/PIN.CH, FIA_AFL.1/PIN.home, FIA_AFL.1/PUC.CH and FIA_AFL.1/PUC.home.

5. the TOE security service **Service_Privacy** is implemented mainly by the SFRs FDP_ACC.2 and FDP_ACF.1, because the possibility to activate and deactivate electronic prescription data is defined as a rule in SFP_access_rules, which is mainly supported by these two SFRs (in fact all other SFRs supporting OT.Access_Rights, as listed for that objective, also support this services).
6. the TOE security service **Service_Client_Server_Auth** is implemented by the SFR FCS_COP.1/CSA
7. the TOE security service **Service_Data_Decryption** is implemented by the SFR FCS_COP.1/RSA_DEC.
8. the TOE security service **Service_Card_Management** is implemented by the SFRs already listed for the service **Service_Sym_Mut_Auth_with_SM**, because this service is used for authentication of the Download Service Provider and for the establishment of secure messaging for the trusted channel. Also the SFRs listed for the objective OT.Additional_Applications support this service.
9. the TOE security service **Service_Logging** is implemented by access rules for the asset logging data defined in SFP_access_rules, so it is realised mainly by the SFRs FDP_ACC.2 and FDP_ACF.1 (and in fact all other SFRs supporting OT.Access_Rights, as listed for that objective, also support this service).

The human user authentication and the access control for all of these security services is implemented mainly by the SFRs FDP_ACC.1 and FDP_ACF.1, because the policy SFP_access_control includes rules for the use of the services. (This is described in SFP_access_control in the form of rules for the use of the keys, which are relevant for the services.)

The TOE security objective **OT.Cryptography** is implemented by the SFRs of the FCS class. They include Triple-DES as used for secure messaging, SHA-1, the RSA variants listed in the objective and random number generation.

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

1. The SFR FPT_EMSEC.1 protects user data and TSF data against information leakage through side channels.
2. 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.
3. 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.
4. 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.

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

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

1. 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.
2. The SFR FPT_RVM.1 and FPT_SEP.1 ensure that the TSF detecting errors or insecure operational can not by bypassed or corrupted.
3. The SFR FPT_PHP.3 resists physical manipulation of the TOE hardware controlling the operational conditions e.g. sensors.

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

1. 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,
2. 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.

9.2.3 Dependency Rationale

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/SM	[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 FDP_ITC.2 Import of user data with 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, FMT_MSA.2 Secure security attributes	justification 2 for non-satisfied dependencies
FCS_COP.1/CCA_SIGN	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation], 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 FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 3 for non-satisfied dependencies

SFR	Dependencies	Support of the 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 destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 1 for non-satisfied dependencies
FCS_RND.1	-	-
FIA_AFL.1/PIN.CH	FIA_UAU.1 Timing of authentication	fulfilled
FIA_AFL.1/PIN.home	FIA_UAU.1 Timing of authentication	fulfilled
FIA_AFL.1/PUC.CH	FIA_UAU.1 Timing of authentication	fulfilled
FIA_AFL.1/PUC.home	FIA_UAU.1 Timing of authentication	fulfilled
FIA_ATD.1	-	-
FIA_UID.1	-	-
FIA_UAU.1	FIA_UID.1 Timing of identification	fulfilled
FIA_UAU.4	-	-
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

SFR	Dependencies	Support of the Dependencies
FDP_RIP.1	-	-
FDP_SDI.1	-	-
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
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
FTP_ITC.1	-	-
FMT_SMF.1	-	-
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/Pers	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/CMS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/KEY_MOD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FPT_EMSEC.1	-	-
FPT_FLS.1	ADV_SPM.1	fulfilled by EAL4
FPT_PHP.3	-	-
FPT_RVM.1	-	-
FPT_SEP.1	-	-
FPT_TST.1	FPT_AMT.1 Abstract machine testing	justification 5 for non-satisfied dependencies

Table 11: Dependency rationale overview

Justification for non-satisfied dependencies:

No. 1: The TSF according to SFR FCS_CKM.1/SM 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 have to describe the management security attributes of theses keys.

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.

Note by the ST-author 52:

This argument is valid for RIPEMD-160 and SHA-2 that have been attached to the SFR by an refinement of the corresponding SFR in the eHC-PP as they also do not use any cryptographic key.

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 comprises the software and the hardware of the card, there is no underlying abstract machine the TSF relies upon. Hence the dependency of FPT_TST.1 (TSF self test) upon FPT_AMT.1 (Abstract machine testing) is not relevant here.

9.2.4 Rationale for the Assurance Requirements

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources.

EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

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

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.

The TOE shall be shown to be resistant to penetration attacks with high attack potential as described in the threats. Therefore the component AVA_VLA.4 was chosen in order to meet the security objectives

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

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.

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.

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.

9.2.5 Security Requirements – Mutual Support and Internal Consistency

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

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

- The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements.
- The dependency analysis for the additional assurance components in section 9.2.4 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 9.2.3 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 analysed, and non-dissolved dependencies are appropriately explained.
- The following additional reasons support consistency and mutual supportiveness of the SFRs:

  The chosen SFRs of class FCS implement the cryptographic algorithms as required by the eHC specification.

  The chosen SFRs of classes FIA and FDP support the access control policy SFP_access_control as defined in the objective OT.Access_Rights.

  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 eHC services as defined in the TOE description (section 2.1.2).

  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 9.2.2.

- 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 section 9.2.4. Furthermore, as also discussed in section 9.2.4, 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.

9.3 Rationale for TOE Summary Specification

9.3.1 Rationale for TOE Security Functions

9.3.1.1 Summary of the rational

The following table gives the coverage of the TOE Security Functional Requirements by the TOE Security Functions. The numbers in the table give the corresponding component of the Security Function covering the requirement.

Table 9-7 Functional Requirements to Security Function mapping

SFR / Security Function	SF.ACCESS	SF.ADMIN	SF.AUTH	SF.CRYPTO	SF.TRUST	SF.PROTECTION	SF.IC_SF
FCS_CKM.1.1/SM		4			1,2		
FCS_CKM.4.1					5		
FCS_COP.1.1/SHA				1	1,2		
FCS_COP.1.1/CCA_SIGN				4	1		4
FCS_COP.1.1/CCA_VERIF				4	1		4
FCS_COP.1.1/CSA				4,5			4
FCS_COP.1.1/RSA_DEC				4,6			4
FCS_COP.1.1/TDES				2	3		4
FCS_COP.1.1/MAC				2	4		4
FCS_RND.1.1				3			3
FIA_AFL.1.1/PIN.CH			1				
FIA_AFL.1.2/PIN.CH			1				
FIA_AFL.1.1/PIN.home			1				
FIA_AFL.1.2/PIN.home			1				
FIA_AFL.1.1/PUC.CH			2				
FIA_AFL.1.2/PUC.CH			2				
FIA_AFL.1.1/PUC.home			2				
FIA_AFL.1.2/PUC.home			2				
FIA_ATD.1.1	1						
FIA_UID.1.1	3,6						
FIA_UID.1.2	3,6						
FIA_UAU.1.1	3,6						
FIA_UAU.1.2	3,6	4	1		1		
FIA_UAU.4.1		4		3	1		3
FDP_ACC.2.1	3,4,5						
FDP_ACC.2.2	3,4,5						
FDP_ACF.1.1	3,4,5						
FDP_ACF.1.2	3,4,5						
FDP_ACF.1.3	3,4,5						
FDP_ACF.1.4	3,4,5						

SFR / Security Function	SF.ACCESS	SF.ADMIN	SF.AUTH	SF.CRYPTO	SF.TRUST	SF.PROTECTION	SF.IC_SF
FDP_RIP.1.1/RES_DEAL						1	
FDP_RIP.1.1/RES_AL						2	
FDP_SDI.2.1				7		3	
FDP_SDI.2.2				7		3	
FDP_UCT.1.1	3,5			2	3		4
FDP_UIT.1.1	3,5			2,3	2,4		3,4
FDP_UIT.1.2	3,5			2,3	2,4		3,4
FTP_ITC.1.1				2	2,3,4		4
FTP_ITC.1.2					2		
FTP_ITC.1.3	3,5						
FMT_SMF.1.1		2,3,5	3				
FMT_SMR.1.1	2						
FMT_SMR.1.2		1,4	1		1		
FMT_LIM.1.1						4	
FMT_LIM.2.1						4	
FMT_MTD.1.1/Ini		1,2					
FMT_MTD.1.1/pers		1,3					
FMT_MTD.1.1/CMS		1					
FMT_MTD.1.1/PIN	4						
FMT_MTD.1.1/KEY_MOD	3						
FPT_EMSEC.1.1						5	
FPT_EMSEC.1.2	3					5	
FPT_FLS.1.1							1,2
FPT_PHP.3.1							1,2
FPT_TST.1.1						4	
FPT_TST.1.2						4	
FPT_TST.1.3						4	
FPT_RVM.1.1						6	
FPT_SEP.1.1	3,4,5,6					4	2
FPT_SEP.1.2	3,4,5,6					4	2

9.3.1.2 Justification for the correspondence between functional requirements and security functions

FCS_CKM.1.1/SM the generation of cryptographic keys in accordance to the card-to-card authentication mechanism with secure messaging is managed by **SF.TRUST** and **SF.ADMIN**.

The card to card authentication algorithm with secure messaging with negotiation of 112 bit key sizes as required in **FCS_CKM.1.1/SM** is covered by the mutual authentication mechanism based on symmetric and asymmetric cryptography with random challenge (**SF.ADMIN.4** for symmetric authentication and **SF.TRUST.1** for asymmetric authentication) and negotiation of symmetric cryptographic 3-DES keys used for protection of the communication channel (**SF.TRUST.2**).

The physical deletion requirement for the keys that could be deleted and which concerns the Triple-DES encryption key and Retail-MAC authentication session key (see 'Note by the ST-author' 15) as specified in **FCS_CKM.4.1** will be covered by **SF.TRUST.5** that describes a physical deletion method for symmetric session keys after reset, termination of the trusted channel or by reaching a fail secure state. Other keys than the mentioned session keys could never be deleted. Some keys could be modified, which is equivalent with physical deletion as the same memory content will be overwritten with the new updating values.

The requirement that the TSF shall perform hashing in accordance with SHA-1, RIPEMD-160, SHA-2 (with 224 bit, 256 bit, 384 bit, 512 bit) in accordance with FIPS 180-2 from **FCS_COP.1.1/SHA** will be obviously covered by **SF.CRYPTO.1**. SHA-1 will be used in **SF.TRUST.2** for generation of the secure messaging keys (see E.3 in [7]) and in **SF.TRUST.1** for generation and verification of electronic signatures.

The requirements of **FCS_COP.1./CCA_SIGN** will be covered by **SF. CRYPTO** and **SF.IC_SF**. The TSF shall perform digital signature-creation in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes 1024 to 2048 bit module length (**SF.CRYPTO.4**) that meet the following: ISO/IEC9796-2 (DS scheme 1) will be covered by **SF.TRUST.1**, which uses the cryptographic support by the IC described in **SF.IC_SF.4**.

The requirements of **FCS_COP.1./CCA_VERIF** will be covered by **SF. CRYPTO** and **SF.IC_SF**. The TSF shall perform digital signature-verification in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes 1024 to 2048 bit module length (**SF.CRYPTO.4**) that meet the following: ISO/IEC9796-2 (DS scheme 1) will be covered by **SF.TRUST.1**, which uses the cryptographic support by the IC described in **SF.IC_SF.4**.

The requirement from **FCS_COP.1.1/CSA** that the TSF shall perform digital signature-creation in accordance with a specified cryptographic algorithm RSA that meet the PKCS#1 standard will be covered by **SF.CRYPTO.5,** which uses **SF.CRYPTO.4** and **SF.IC_SF.4** for RSA calculation.

The requirement from **FCS_COP.1.1/RSA_DEC** that the TSF shall perform decryption in accordance with RSA that meet PKCS#1 will be covered by **SF.CRYPTO.6** that is describing the RSA decryption compliant to PKCS#1**,** which uses **SF.CRYPTO.4** and **SF.IC_SF.4** for RSA calculation.

The encryption and decryption in accordance with Triple-DES in CBC mode (FIPS 46-3) as required by **FCS_COP.1.1/ TDES** will be covered by **SF.CRYPTO.2**. which uses the IC as described in **SF.IC_SF.4**. This will be used in the trusted channel part **SF.TRUST.3.**

The generation and verification of message authentication code in accordance with Retail MAC (ANSI X9.19 with DES) as required by **FCS_COP.1.1/ MAC** will be covered by **SF.CRYPTO.2** which uses the IC as described in **SF.IC_SF.4**. This will be used in the trusted channel part **SF.TRUST.4.**

The requirements for generation of random numbers as described in **FCS_RND.1.1** will be implemented by **SF.CRYPTO.3** and **SF.IC_SF.3.**

The requirements from **FIA_AFL.1.1/PIN.CH,** and **FIA_AFL.1.2/PIN.CH** of blocking the PIN.CH if there are more than 3 consecutive failed authentication attempts for PIN.CH has been covered by **SF.AUTH.1**.

The requirements from **FIA_AFL.1.1/PIN.home,** and **FIA_AFL.1.2/PIN.home** of blocking the PIN.home if there are more than 3 consecutive failed authentication attempts for PIN.CH has been covered by **SF.AUTH.1**.

The requirements from **FIA_AFL.1.1/PUC.CH, FIA_AFL.1.2/PUC.CH** for blocking the PIN unblocking code for the PIN.CH, when 10 successful or unsuccessful authentication attempts have been met is covered by **SF.AUTH.2**.

The requirements from **FIA_AFL.1.1/PUC.home, FIA_AFL.1.2/PUC.home** for blocking the PIN unblocking code for the PIN.home, when 10 successful or unsuccessful authentication attempts have been met is covered by **SF.AUTH.2.**

The requirement **FIA_ATD.1.1** for maintenance of the security attributes identity and role have been implemented by **SF.ACCESS.1**.

The list of actions that should be allowed before the user is identified as required by **FIA_UID.1.1** and **FIA_UID.1.2** is covered by the access rules for assets and other data in **SF.ACCESS.3** as access to data with read-access for all is described there. Other TSF-mediated actions allowed to all is covered in **SF.ACCESS.6**.

The list of actions that should be allowed before the user is authenticated as required by **FIA_UAU.1.1** is more or less the same than the list of actions that are allowed before the user is identified. The only difference is the processes for identification e.g. providing the certificates. These TSF-mediated actions are covered by **SF.ACCESS.3** and **SF.ACCESS.6**. In addition to these TSFs **FIA_UAU.1.2** is covered by the authentication mechanisms for the users in the usage phase as described in **SF.ADMIN.4**, **SF.AUTH.1** and **SF.TRUST.1**.

Reuse of authentication data as required by **FIA_UAU.4.1** will be prevented by the mechanism implemented in **SF.ADMIN.4** and **SF.TRUST.1**, which uses the SOF-high random number generator of **SF.CRYPTO.3** and **SF.IC_SF.3**.

All access rules coming from SFP_access_rules and required in **FDP_ACC.2.1** are implemented in **SF.ACCESS.3, SF.ACCESS.4, SF.ACCESS.5**. As these parts of SF.ACCESS explicitly mention that no other access rules between objects and subjects are allowed **FDP_ACC.2.2** is also implemented in this SF.

As all access rules, objects and subjects as well as the respective security attributes described in SFP_access_rules are implemented in **SF.ACCESS.3, SF.ACCESS.4, SF.ACCESS.5** the requirements from **FDP_ACF.1.1**, **FDP_ACF.1.2** and **FDP_ACF.1.4** are covered. As these parts of the TSF explicitly states that no other access between the specified access rules is allowed also **FDP_ACF.1.3** is covered as well.

FDP_RIP.1.1/RES_DEAL and **FDP_RIP.1.1/RES_AL** require secure deletion after deallocation or allocation of the resource. These requirements have been implemented in **SF.PROTECTION.1** for FDP_RIP.1.1/RES_DEAL and **SF.PROTECTION.2** for FDP_RIP.1.1/RES_AL.

SF.PROTECTION.3 in combination with **SF.CRYPTO.7** covers the requirements for integrity checked data required by **FDP_SDI.2.1** and **FDP_SDI.2.2**. Ensuring the integrity covers the requirements for integrity monitoring and the reaction required for the TSF like prohibiting the use and inform the connected entity.

Protection against disclosure (**FDP_UCT.1.1**) by enforcing the SFP_access_rules as defined in **SF.ACCESS.3** and **SF.ACCESS.5** will be managed by encryption of communication (**SF.TRUST.3**) data using the DES (**SF.CRYPTO.2**, **SF.IC_SF.4**).

Protection against and determination of modification, insertion, deletion and replay (**FDP_UIT.1.1** and **FDP_UIT.1.2**) by enforcing the SFP_access_rules as defined in **SF.ACCESS.3** and **SF.ACCESS.5** will be managed by a cryptographic checksum and a send sequence counter described in **SF.TRUST.2** and **SF.TRUST.4** using the cryptographic funtions of **SF.CRYPTO.2** and **SF.CRYPTO.3** with support of the **IC SF.IC_SF.3** and **SF.IC_SF.4.**

Only one communication channel exist for the TOE. Therefore **FTP_ITC.1.1** requirements are covered by the SF for secure messaging, which are **SF.TRUST.2**, **SF.TRUST.3** and **SF.TRUST.4**. This secure messaging has assured identification of its endpoints and protection of the channel data from modification or disclosure, which is based on encryption using **SF.CRYPTO.2**. and **SF.IC_SF.4**. As the remote trusted IT product could initiate the secure messaging by the authentication process **FTP_ITC.1.2** is covered by **SF.TRUST.2**. Requirements for the initiation of a trusted channel as required by **FTP_ITC.1.3** are implemented in **SF.ACCESS.3, SF.ACCESS.5**.

The security management function described in **FMT_SMF.1.1** are implemented in **SF.ADMIN.3** for personalisation **SF.ADMIN.2** for initialisation **SF.AUTH.3** for modification of the PIN and **SF.ADMIN.5** for Service_Card_Management.

Maintenance of the roles described in **FMT_SMR.1.1** is implemented in **SF.ACCESS.2**. The prior authentication of users and the ability to associate these users with roles as required by **FMT_SMR.1.2** is described in **SF.AUTH.1** for the cardholder, **SF.ADMIN.4** for the Download Service Provider, the Health Insurance Agency Service Provider, the Combined Services Provider and **SF.ADMIN.1** for the Personalisation Service Provider and the TOE Manufacturer and **SF.TRUST.1** for the health professional, Medical Assistant, SMC (health care) and the Self Service Terminal.

The requirements for limitation of capabilities (**FMT_LIM.1.1**) and availabilities (**FMT_LIM.2.1**) of test features after TOE delivery are implemented in **SF.PROTECTION.4**.

The requirements of **FMT_MTD.1.1/Ini** are implemented by **SF.ADMIN.1** which is responsible for authentication of the TOE-manufacturer and **SF.ADMIN.2** which restricts the initialisation to the TOE Manufacturer.

The requirements of **FMT_MTD.1.1/pers** are implemented by **SF.ADMIN.1** which is responsible for authentication of the Personalisation Service Provider and **SF.ADMIN.3** which restricts the personalisation to the Personalisation Service Provider.

Requirements for writing of data for new applications as listed in **FMT_MTD.1.1/CMS** are implemented by **SF.ADMIN.1**.

Requirements for the PIN as listed in **FMT_MTD.1.1/PIN** are implemented by **SF.ACCESS.4**.

Requirements for the public key for CV certification verification as listed in **FMT_MTD.1.1/KEY_MOD** are implemented by **SF.ACCESS.3**.

Requirements for the TOE to protect against side channel attacks as described in **FPT_EMSEC.1.1** and **FPT_EMSEC.1.2** have been implemented by **SF.PROTECTION.5** and for FPT_EMSEC.1.2 in addition by **SF.ACCESS.3** that allows no legal reading access for the assets mentioned in the SFR.

Requirements for the TOE to protect against tamper attacks as described in **FPT_FLS.1.1** are implemented by **SF.IC_SF.1** and **SF.IC_SF.2**. Unusual operating conditions will be recognised by sensors as described in SF.IC_SF.1 and the TOE will react as described in SF.IC_SF.2.

Physical manipulation and physical probing will be recognized by the TOE with sensors as described in **SF.IC_SF.1** and the TOE will react as described in **SF.IC_SF.2**, which fulfills the requirements of **FPT_PHP.3.1**.

The demonstration of the correct operation of the TSF as implemented in **SF.PROTECTION.4** covers the requirements of **FPT_TST.1.1**, **FPT_TST.1.2** and **FPT_TST.1.3.**

The SFR **FPT_RVM.1.1** requires that the TSP enforcement functions must be invoked and that should succeed before each function within the TSC is allowed to succeed. This has been covered directly by **SF.PROTECTION.6** as this implies that all policies resulting from all SFRs are invoked, before a command will be send, which leads to an execution of functions within the TSC

The test features of selftests and the tests done to preserve a secure state for exposure of operating conditions are not configurable as described in **SF.PROTECTION.4** and **SF.IC_SF.2**. In addition the separation of security domains of subjects is handeled generally by the access rules as described in **SF.ACCESS.3, SF.ACCESS.4, SF.ACCESS.5** and **SF.ACCESS.6** This set of TSFs therefore cover the requirements from **FPT_SEP.1.1** and **FPT_SEP.1.2**.

9.3.2 Rationale for Assurance Measures

The following table demonstrates the coverage of the Assurance Requirements by the Assurance measures (see section 7.2) by indicating the correspondence with crosses.

Table 9-8 Assurance Requirements to Assurance Measures mapping

Assurance Requirements / Assurance Measures	AM_ACM	AM_ADO	AM_ADV	AM_AGD	AM_ALC	AM_ATE	AM_AVA
ACM	X						
ADO		X					
ADV			X				
AGD				X			
ALC					X		
ATE						X	
AVA							X

9.3.3 Rationale for Strength of Function High

For the following Security Functions an SOF-claim is appropriate as permutational but not cryptographical mechanisms are involved:

SF.AUTH

SF.CRYPTO

SF.IC_SF

For all these TSF the claim is SOF-high, which is appropriate to meet the requirements for resistance against attackers with high attack potential. There is one explicit SOF-claim in the SFRs for FCS_RND and there are SOF-claims in the objectives that have

been covered by the SFRs. The direct SOF-claim in FCS_RND as well as all indirect SOF-claims for TSFs covering SFRs that cover itself objectives with an SOF-claim have been fulfilled.

10 Conventions and Terminology

Some types of terms are not described here, but at specific places in the text:

- The services provided by the TOE are defined in section 2.1.2
- The life cycle phases of the TOE are defined in section 2.1.3, Table 1.
- Assets (sensitive data) protected by the TOE are defined in section 3.1.1, Table 2.
- The subjects interacting with the TOE are defined in section 3.1.2, Table 3.

10.1 Glossary

Term	Definition
Application note	Optional informative part of the PP/ST 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).
IC dedicated software	The part of the TOE's software, which is provided by the hardware manufacturer
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.
Mutual Authentication	Type of those cryptographic protocols, were two entities mutually verify the authenticity of each other, for smart cards this is realised by suitable sequences of amt card commands and responses
Personalization	The process by which personal data are brought into the TOE before it is handed to the cardholder
*Rule_**	Naming convention for access control rules in the ST, defined in SFP_access_rules.
Role ID	A role identifier (Role ID) is a one-byte field in a card verifiable certificate used in an asymmetric card-to-card authentication procedure. Roles are assigned to entities. More information could be found in [11], section F.2.
Secure Channel	A connection between two devices, which is secured against interception or modification of the transmitted data. The TOE realises a secure channel to other devices using secure messaging.
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
*Service_****	Services provided by the TOE (e. g. Service_Privacy) are defined in section 2.1.2.
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]).

10.2 Acronyms

Acronyms	Term
*A.****	Naming convention for assumptions in this ST, e. g. A.Users, see section 3.4.
BMG	Bundesministerium für Gesundheit (the German Federal Ministry of Health)
*BSI-PP-****	Naming convention for Protection Profiles registered by BSI
CC	Common Criteria
CCIMB	Common Criteria Implementation Management Board
COS	Card Operating System
CVC	Card Verifiable Certificates
DES3	Data Encryption Standard 3 (symmetric cryptographic algorithm used by the TOE, also called Triple-DES)
EAL	Evaluation Assurance Level
eGK	elektronische Gesundheitskarte
eHC	electronic Health Card
HEC	Health Employee Card (technically a type of HPC)
HPC	Health Professional Card
MAC	Message Authentication Code
OSP	Operational Security Policy
*OSP.****	Naming convention for organisational security policies in this ST, e. g. OSP.User_Information (see section 3.2).
*OT.****	Naming convention for security objectives for the TOE in this ST, e. g. OT.Access_Rights (see section 4.1.
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PUC	PIN Unblocking Code
PP	Protection Profile
RAD	Reference Authentication Data (see Table 2).
RSA	Rivest Shamir Adleman (an asymmetric cryptographic algorithm used by the TOE)
SAR	Security assurance requirements
SHA-1	Secure Hash Algorithm 1 (a cryptographic hash algorithm)
SFP	Security Functional Policy
SFP_access_rules	Name of the security functional policy defining the access rights to assets (data) in the TOE. It is defined in OT.Access_Rights (see section 4.1.1) and used by access control SFRs (see section 6.1).
SFR	Security functional requirement
SM	Secure Messaging
SMC	Security Module Card
SSCD-PP	Secure Signature Creation Device Protection Profile, see [25]
SSVG-PP	Secure Silicon Vendor's Protection Profile, see [26]
*T.****	Naming convention used for naming threats in this ST, for example T.Forge_Internal_Data, see section 3.3.
TOE	Target of Evaluation
TOE_App	Application Part of the TOE
TOE_ES	TOE Embedded Software (operating system of the TOE)
TOE_IC	The integrated circuit of the TOE, the hardware part together with IC dedicated software
TSF	TOE security functions
VAD	Verification Authentication Data (see Table 2).

Acronyms	Term
X.509	A certificate format

11 References

Common Criteria

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

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

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

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

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

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

eHC specifications and further documents related to the German eHC

[7] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform, Version 1.1.0, 07.02.2006,gematik

[8] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Anwendungen und anwendugngsspezifische Strukturen, Version 1.2.1, 07.09.2006,gematik

[9] Beschreibung der zulässigen PIN- und PUC-Verfahren für die eGK, Version 1.0.0, 20.12.2006, gematik

[10] 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-Gesellschaf

[11] 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-Gesellschaf

[12] 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

[13] Erarbeitung einer Strategie zur Einführung der Gesundheitskarte, Sicherheitsanforderungen, Version 1.1, Project group bIT4health on behalf of the German Federal Ministry of Health and Social Security (Bundesministerium für Gesundheit und soziale Sicherung), 12. August 2004

[14] Erarbeitung einer Strategie zur Einführung der Gesundheitskarte, Sicherheitsarchitektur, Version 1.1, Project group bIT4health on behalf of the German Federal Ministry of Health and Social Security (Bundesministerium für Gesundheit und soziale Sicherung), 12. August 2004

[15] Erarbeitung einer Strategie zur Einführung der Gesundheitskarte, Use Case Modell Teil 1, Version 1.1, Project group bIT4health on behalf of the German Federal Ministry of Health and Social Security (Bundesministerium für Gesundheit und soziale Sicherung) , 12. August 2004

[16] Erarbeitung einer Strategie zur Einführung der Gesundheitskarte, Use Case Modell Teil 2, Version 1.1, Project group bIT4health on behalf of the German Federal Ministry of Health and Social Security (Bundesministerium für Gesundheit und soziale Sicherung), 12. August 2004

[17] Erarbeitung einer Strategie zur Einführung der Gesundheitskarte, Gesammelte Referenzen der bIT4health-Dokumente, Version 1.1, Project group bIT4health on behalf of the German Federal Ministry of Health and Social Security (Bundesministerium für Gesundheit und soziale Sicherung), 12. August 2004

[18] Erarbeitung einer Strategie zur Einführung der Gesundheitskarte, Glossar des Projekts bIT4health, Version 1.1, Project group bIT4health on behalf of the German Federal Ministry of Health and Social Security (Bundesministerium für Gesundheit und soziale Sicherung), 12. August 2004

Cryptography

[19] „Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV“, Bundesanzeiger Nr. 69, S.3759, 12.04.07

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

[21] 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

[22] 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

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

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

Protection Profiles / Security Targets

[25] 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 SSCD-PPs or CWA14169

[26] PP conformant to 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, also short SSVG-PP

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

[28] Common Criteria Protection Profile, electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK); version 2.00, 29th January 2007; Bundesamt für Sicherheit in der Informationstechnik.

[29] Security Target (Public), Infineon Technologies AG Security and Chipcard ICs SLE66CX680PE/m1534-a13 and SLE66CX360PE/m1536-a13, both with RSA2048 V1.4, Version 1.2, 28.07.05