Security Target lite

Electronic Health Card and SSCD 2.10

GEGKOS

GEMALTO, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.

Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90

Printed in France.

Document Reference: ASE02R10559 V0.9

September 8, 2009

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

OBJECTIVES OF THE CHAPTER

The objective of this chapter is to furnish document management and overview information such as labeling and descriptive information necessary to control and identify the ST and the TOE to which it refers, narrative form ST summary and state of any evaluatable claim of CC conformance for the TOE.

1.1 ST IDENTIFICATION

Title:	Security Target lite
Reference:	ASE02R10559
Version:	0.9
Date of creation:	08/09/09
Date of modification:	08/09/09
TOE:	Electronic Health Card and SSCD
TOE version:	2.10
Security Controller:	SLE66CX680PE
IT Security Evaluation scheme:	TUV Informationstechnik GmbH evaluation body.
IT Security Certification scheme:	BSI certification body.

This ST has been built with the:
Common Criteria for Information Technology Security Evaluation Version 2.3,August 2005 which comprises [CCPART1], [CCPART2], and [CCPART3].

Component	Version	Constructor
Embedded Software	2.10	GEMALTO
Micro Controller	SLE66CX680PE	INFINEON

Table 1 - Electronic Health Card and SSCD version 2.10

1.2 ST OVERVIEW

The TOE described herein is a Smart Card Integrated Circuit (IC) with a GEMALTO Embedded Software (ES) and Applicative Data Structures (APP) that meets "The Specification of the German electronic Health Card eHC – part 1 - Release 2.2.2, part 2 – Release 2.2.1 and part 3 – Release 2.1.0 - Gematik**"**.

The TOE is named "Electronic Health Card and SSCD" and includes:

- **Health application**[1]
- **Digital Signature application**

The IC, which is used to support the ES, is described in the Security Target [ST IC].

The aim of this document is to describe the Security Target (ST) of the "Electronic Health Card and SSCD", addressing the requirement of the Embedded Software (ES) including the **electronic Health Card application and the digital signature application**.

This security target is compliant to **the Protection profile - "Electronic Health Card (eHC)" rev 2.60 29/07/2008 BSI-PP-0020 [PP eHC] which defines the security objectives and requirements for the electronic Health Card (German: "elektronische Gesundheitskarte") based on the regulations for the German health care system. It addresses the security services provided by this card.**
In addition, it is based on the Protection Profile - "Secure Signature Creation Devices" Type 3 [PP SSCD3] which defines security requirements for SSCD in accordance with the "DIRECTIVE 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures" [DIRECTIVE], but without claiming formal compliance to it

The assets to be protected by the TOE are **those of the electronic health card** and those of the digital signature application as defined in section 3.1.

As described in [PP eHC] the Electronic Health Card and SSCD provides following services:

- **Mutual Authentication between the eHC and the Health Professional Card (HPC) or a Security Module Card (SMC)**
- **Mutual Authentication between the eHC and a security device**
- **Authentication of the card holder by use of one or two PINs (PIN.CH and PIN.home : Specific PINs for eHC functions)**
- **Secure storage of contractual and medical data, with respect to confidentiality, integrity and authenticity**
- **Authentication of the card using private key and X.509 certificate**
- **Document content key decipherment using an asymmetric private key**
- Management of application
- Electronic signature for the card holder :

  As described in [PP SSCD3] the Electronic Health Card and SSCD is used in conjunction with:

  1. The Signature-creation application (SCA) that:
     - Performs the presentation of the Data-To-Be-Signed (DTBS) to the signatory prior to the signature process.
     - Sends a DTBS-representation to the Electronic Health Card and SSCD, if the signatory indicates the intend to sign.
     - Attachs the qualified electronic signature generated by the Electronic Health Card and SSCD to the data or provides the qualified signature as separate data.
  2. The Certification generation application (CGA). The CGA requests the SVD from the Electronic Health Card and SSCD for generation of qualified certificate. The CGA verifies the authenticity of the SVD by means of:

[1] The convention is to use in the document bold blue typing for specific informations concerning Electronic Health Card

- the Electronic Health Card and SSCD proof of correspondence between SCD and SVD and
- checking the sender and integrity of the received SVD.

In addition it supports the generation of SCD/SVD pairs onboard during the personalisation process of the card.

The services mentioned are implemented with following cryptography:

- 3TDES, that is Triple DES using 168 bit symmetric keys.
- RSA with key size of 2048 bit[2].
- hashing with SHA-256 as specified in chapter 5.3 (subsection 5.3.2.1). The hash value can be transmitted directly to the card, computed completely by the TOE, or computed partly by the TOE.

The main objectives of this ST are:

- To describe the Target-Of-Evaluation (TOE).
- To define the limits of the TOE.
- To describe the security objectives for the TOE and for its environment,
- To describe the security requirements for the TOE.
- To describe the security environment of the TOE, the assets to be protected and the threats to be countered by the TOE itself and by the environment during the development and the operational phases of the smart card.

The TOE is conformant to the specification documents ”The specification of the German Electronic Health Card eHC” Part1,2 . [EHC spec part 1], [EHC spec part 2]

The TOE is aimed to be compliant to the requirement specified for products for electronic signatures in the German Digital Signature Act (SigG -§17(1)) [ACT], Ordinance (SigV - §15(1,4)), Appendix 1 [ORDI] and the [DIRECTIVE] Annex 3.

[2] Notification in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance Published in Federal Gazette No 13, pp 346 of 27 January 2009 (in German)

Minimum bit length :	1280 up to end 2008 - 2048 recommended
	1536 up to end 2009 - 2048 recommended
	1728 up to end 2010 - 2048 recommended
	1976 up to end 2015 - 2048 recommended

1.3 CC CONFORMANCE CLAIM

This ST is conformant with the Common Criteria for Information Technology Security Evaluation Version 2.3,August 2005, part 2 extended with the SFR FPT_EMSEC.1, FCS_RND.1, FMT_LIM.1 and FMT_LIM.2 [CCPART2], part 3 conformant [CCPART3].

The TOE includes an Integrated Circuit certified with CC EAL5+ according to PP0002-2001 [(BSI-DSZ-CC-0437-2008).
That follow [CEM], [AIS 34].
It is a composite evaluation, evaluated with application of [AIS36].

The assurance level is **EAL4** augmented on:

- **AVA_MSU.3 (Misuse - Analysis and testing for insecure states)**;
- **AVA_VLA.4 (Vulnerability Analysis - Highly resistant).**
- **ADV_IMP.2 (Implementation of the TSF)**

The minimum strength level for the Toe security functions is “SOF high” (Strength of functions high).

2. TOE DESCRIPTION

OBJECTIVES OF THE CHAPTER

The objective of this chapter is to furnish the TOE description as an aid to the understanding of its security requirements, an addressing to the product or the system type and, a TOE's scope and boundaries general terms description.

2.1 TOE ABSTRACT

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, in other words the operating system, branded GeGKOS ("Gemalto Elektronische GesundheitsKarte Operating System")

TOE_APP,
- the eHC applications (data structures and their content, not including card individual data like PIN and key values)
- the SSCD application. (data structures and their content, not including card individual data like PIN and key values)

and
guidance documentation delivered together with the TOE.

The TOE is named **Electronic Health Card and SSCD**. As shown in figure 1, the product **Electronic Health Card and SSCD** is the smart card IC with Embedded Software. As shown in figure 2, the physical scope of the TOE is the complete card framed by the grey line. The logical scope is highlighted in yellow.
The Electronic Health Card and SSCD HW platform is a Smart Card Integrated circuit certified EAL5+ (BSI-DSZCC-0437-2008)
.

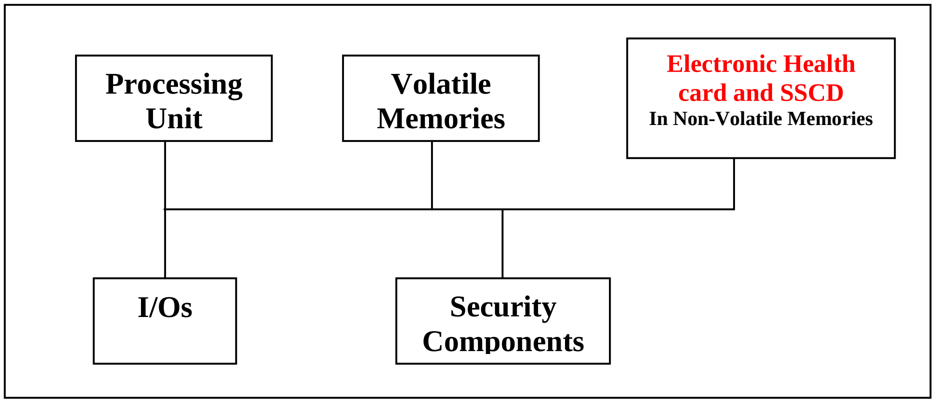


Figure 1 – Smart card IC with Embedded Software

The Smart Card Integrated circuit is the INFINEON SLE66CX680PE. The IC is certified at the level EAL5 augmented with ALC_DVS.2, AVA_VLA.4 and AVA_MSU.3 components. The evaluation of the **Electronic Health Card and SSCD** is built on the results of the evaluation of the SLE66CX680PE.

The GEGKOS operating system (TOE_ES) meets the specification **[EHC spec part 1]**.

The Applicative Data Structures, **Health application and Digital Signature application,** meet the specification **[EHC spec part 2]**, (herein the digital signature application is named "QES").

These specifications are defined according [ISO C4], [ISO C4'], [ISO C8], [ISO C9], [PKCS1], [DINSIG] and [DINSIG 4] standards.

Figure 2 describes how the Applications and the GEGKOS operating system are implemented on the IC.

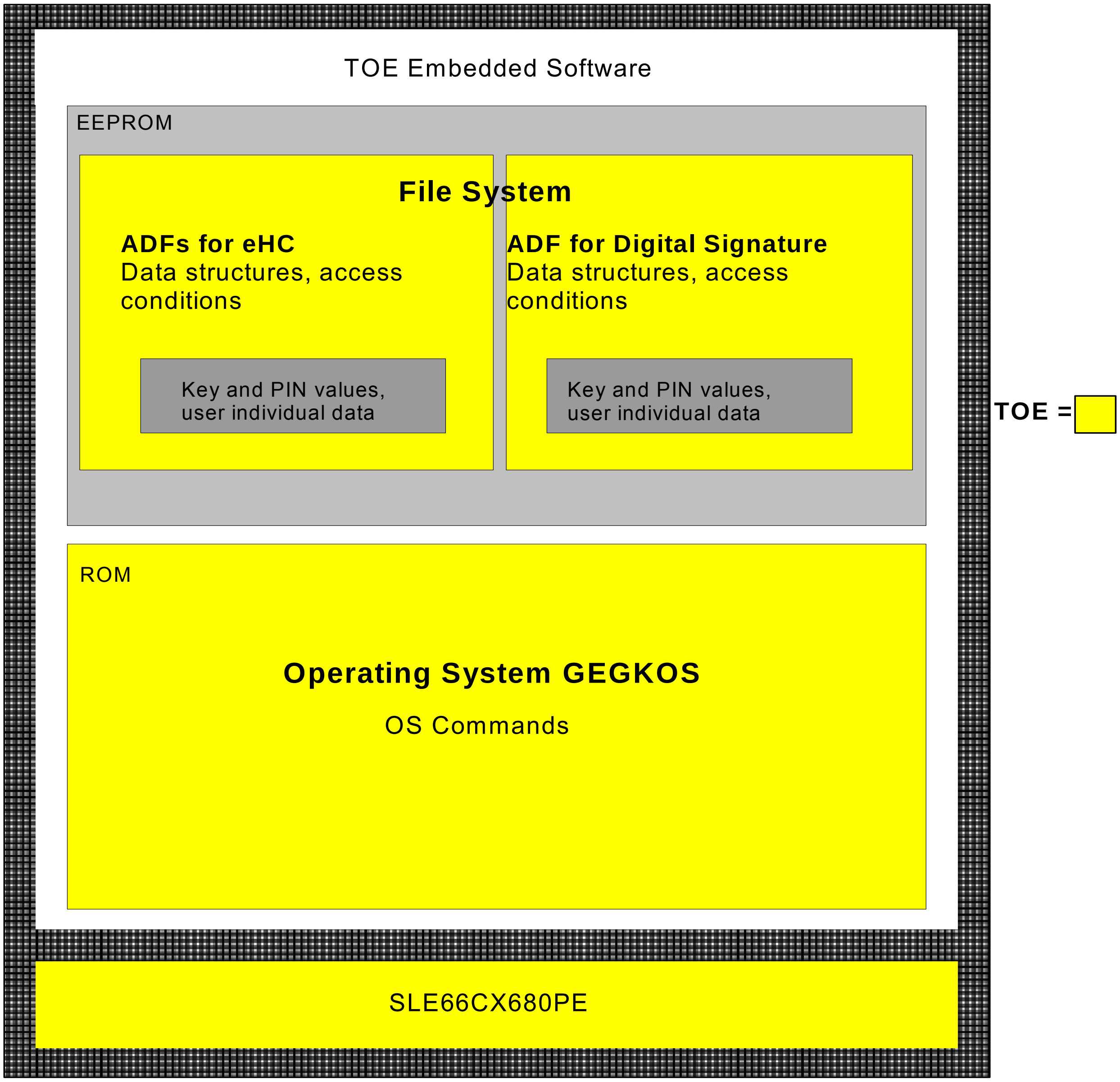

TOE Embedded Software
EEPROM
File System
ADFs for eHC
Data structures, access conditions
Key and PIN values, user individual data
ADF for Digital Signature
Data structures, access conditions
Key and PIN values, user individual data
TOE =
ROM
Operating System GEGKOS
OS Commands
SLE66CX680PE

Figure 2 – TOE description

The TOE Embedded Software is made of the Operating system and the data structures in EEPROM, including the ADFs (Application DFs) for the applications under evaluation (described in [EHC spec part 2]). It is implemented on a SLE66CX680PE controller.

By specification it is possible to create additional applications after card issuance, consequently there are parts in EEPROM outside the TOE scope (grey). Note that this mechanism is not able to influence the existing applications!

The ADFs cover all containers for the applicative data, including access conditions and OS dependent system data contents. Card individual data like PIN and key values are outside the scope of the TOE.

The OS provides the following functions:

- a file system according to [ISO C4],
- access control for the file system and the cryptographic services,

- secure messaging for external communication via a trusted channel (TC),
- selection and management of security environments;
- user authentication with passwords,
- component authentication with symmetric and asymmetric cryptographic keys,
- import of external public keys via CVC verification
- the generation of asymmetric key pairs,
- creation and verification of digital signatures,
- enciphering and deciphering with asymmetric cryptography.

The data structures of the ADFs determine the access to those functions and their execution modes by containing the appropriate access conditions and control information, e.g. key lengths or maximum PIN retry counters.

2.2 TOE SERVICES

2.2.1 The aim of the TOE

The TOE is aimed to

- **Protect health data by fighting the following risks :**
  - **Physical attacks : the physical tampering of the TOE user data, TSF data or by modification of security features**
  - **Information leakage : as emanations, variations in power consumption, I/O characteristics, clock frequency or by changes in processing requirements**
  - **Malfunction due to an environment stress**
  - **Use of functions in wrong phase to manipulate TOE's security functions or features or TSF data**
- create legal valid signatures and therefore protect the assets described in chapter 3.1.1, by fighting the following risks:
  - Cloning: Substitution of programmed microchip i.e. personalized or non-personalized Smart Card.
  - Confidential data disclosure: Disclosure of confidential data in programmed microchip, i.e. signature creation data (SCD), Application code, keys, PIN.
  - Non-integrity: Use of non-valid data.
  - Identity usurpation: Management (i.e. load, personalisation,) by unauthorized administrators. Use of Digital Signature Application by unauthorized user, i.e. other than the legitimate signatory.
  - Forgery of data: Forgery of the electronic signature. Forgery of the signature verification data (SVD). Forgery of the data to be signed (DTBS).
  - Derivation of data: Derivation of the signature creation data (SCD) from public known data like signature verification data.

2.2.2 Contribution of the TOE in the Application

The TOE contributes to the electronic health application by providing the following mechanisms:

- **Identity data or contractual data protection.**
- **"Verification Authentication Data" : check the PIN codes or a resetting code entered to activate certain functions of the TOE**
- **Store data as the "Reference Authentication Data" , initialisation data, personalisation data, logging data , emergency data, electronic prescription**
- **MAC calculation and encryption with symmetric keys inside a trusted channel (TC)**
- **Management of the medical data (including the emergency data) through the voluntary application**
- **Authentication of the card holder by use of the PIN.CH or PIN.home**
- **Authentication of health professional or Medical assistant (accredited)**
- **Authentication of the health insurance agency service provider**
- **Authentication of the self service terminal**
- **Confidentiality of keys: client-server authentication private key, decipher private key, card authentication private key**

The TOE contributes to the Digital Signature application by providing the following mechanisms:

- Creation of signatures with the SCD
- Generation or Import of the SCD/SVD pair
- Confidentiality of cryptographics keys, PIN, and ES.
- Integrity of cryptographic keys, PIN, ES, protected data.
- Authentication of the signatory
- Authentication of the administrators.
- Authentication of the TOE other users.
- External communication protection against disclosure and corruption (secure messaging).
- Files and datas protected by access conditions driven by ES.

2.3 TOE LIMITS

The figure 2 shows the global architecture of the **Electronic Health Card and SSCD**. All the software modules are included inside the TOE (see the ***TOE enforcing element***). This software uses the hardware and its firmware to provide the TOE functionality. The hardware and its firmware is part of the TOE.

2.3.1 TOE enforcing element

The TOE consists of the following software modules:

The APDU Manager

- For this TOE the APDU commands are defined in the specification **[eHC spec part 1]**

The Access Manager
The Access Manager:

- accesses the file system to find the relevant access rules for the command to be executed and the data to be accessed,
- checks if Authentication and Secure Messaging has occurred as requested by the access conditions.

The Access Protection Mechanisms
This module includes:

- Authentication,
- Secure Messaging.

The File System
The File System manages Data structured in DFs and EFs.
All persistent data of the electronic health application and of the digital signature application are stored in the file system.

The cryptographic Library

The cryptographic library is in charge of:

- cryptographic algorithms based on 3TDES (key size 24 bytes = 3 parts of 56 bits),
- cryptographic algorithms based on RSA (key size 2048[3] bits),
- Hash algorithms (SHA-256)[4] ,
- Providing K4-DRNG (AIS 20) also SOF-high.

The Micro-controller

The chip is the INFINEON SLE66CX680PE.
This certified IC is described in the Security Target [ST IC]

[3] Notification in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance Published in Federal Gazette No 13, pp 346 of 27 January 2009 (in German)
Minimum bit length : 1280 up to end 2008 - 2048 recommended
1536 up to end 2009 - 2048 recommended
1728 up to end 2010 - 2048 recommended
1976 up to end 2015 - 2048 recommended

[4] Notification in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance Published in Federal Gazette No No 13, pp 346 of 27 January 2009 (in German)
Hash functions : Suitable until end 2009 SHA1*,
Suitable until end 2010 SHA1**,
Suitable until end 2010 RIPEMD-160 ,
Suitable until end 2015 SHA-224, SHA-256, SHA-384, SHA-512, (SHA-1, RIPEMD-160)***

* i.e. for the generation and verification of qualified certificates but not for the generation and verification of other qualified signed data.

** i.e. for the generation of qualified certificates containing serial numbers with ≥ 20 bit entropy but not for the generation and verification of other qualified signed data.

*** exclusively for the verification of qualified certificates.

2.4 TOE LIFE CYCLE

The Smart Card life cycle is decomposed in several phases.

The table presents the users, administrators and smartcard phase, associated with each step of the life cycle.

TOE phase	Industrial phase	Industrial deliverable	Smartcard Phase	TOE administrator (responsible)	TOE user
Construction	Development	Software		Product developer	
Construction	Development	Hardmask set		IC manufacturer	
Construction	Production	Wafers with ICs	IC initialization	IC manufacturer	
Construction	Production	Modules		Module manufacturer	
Construction	Production	Cards / Modules with ES, Keys for Perso loaded	Card initialization	Card manufacturer	
Construction	Production	Cards / Modules with ES, Keys for Perso loaded, File System created	Card pre-personalization	Card manufacturer	
Construction	Production	Cards with ES, Keys for Perso loaded, File System created, SCD/SVD generated	Card pre-personalization	Card manufacturer	
Construction	Personalization	Card personalized	Card personalization	Card Personalizer	
Usage	Usage	Smartcard		Card issuer	Card issuer End User Terminal

Table 2 - TOE life cycle

The TOE is the **Electronic Health Card and SSCD** wich is composed of the IC and the ES.

The ES is developed by the Product developer.

Product 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 initialization and pre-personalization requirements.

The IC Manufacturer is responsible for:

- 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.
- producing the IC through three main steps:
  - IC manufacturing,
  - IC testing, and
  - IC pre-personalisation.

The Module Manufacturer is responsible for

- assembly of the module,
- perform an electrical test of the module after the assembly

The Card Manufacturer is responsible for

- the initialization of the TOE (in form of the initialization of the modules) and
- it's testing.

The smartcard product finishing process comprises the embedding of the modules for the TOE and the card production
The embedding service provider needs to have secure physical environment.

The Personalizer is responsible for

- the smartcard personalization and
- final tests.

The personalization of the smart card includes the printing of the (card holder specific) visual readable data onto the physical smart card, and the writing of (card holder specific) TOE User Data and TSF Data into the smart card.
The personalization service provider needs to have secure physical environment.

Then, the Smartcard Issuer is responsible for the Smartcard delivery to the Smartcard End-user for usage

The Card Issuer is responsible for

- the smartcard product delivery to the smartcard end-user (the card holder), and the end of life process.
- The authorized personalization agents (card management systems) might be allowed to add data for a new applications, 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.[5]

The TOE is used as eHC by the smart card holder in the Operational use phase.

[5] This wording is a copy from [PP eHC]. By the actual access conditions specified, the card management system is able to load new applications (outside TOE scope) and to deactivate and activate the eHC application (DF_HCA). Certain EFs of the eHC application can be updated or deleted by the card management system. Deleting the whole DF_HCA is not possible.

[7] The eHC authentication keys and the ESIGN keys are loaded (i.e. personalized), while the signature key can only be generated.

3. TOE SECURITY ENVIRONMENT

OBJECTIVES OF THE CHAPTER

The objective of this chapter is to furnish the description of the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed.

The statement of the TOE security environment shall describe the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed. This statement shall include the following:

- A description of assets that shall define the assets to be protected.
- A description of threats that shall include all threats to the assets against which specific protection, within the TOE or its environment is required. A threat shall be described in term of :
  - Identified threat agent,
  - Attack,
  - Asset that is the subject of the attack.
- A description of assumptions that shall described the security aspects of the environment in which the TOE will be used or is intended to be used.
- A description of organisational security policy that shall identify, and if necessary explain, any organisational security policy statements or rules with which the TOE must comply.

3.1 OBJECTS

3.1.1 Data objects (Assets)

Personal and health insurance data (open) EF PD, EF VD, EF.StatusVD	Identity data or contractual data, which can be read without authentication
Personal and health insurance data (protected) EF GVD	Identity data or contractual data, which can be read only with authentication
Electronic prescription EF. eVerordnungsTickets, EF.eVerordnungsContainer, EF.StatusVerordnungen.	A document containing one or more referrals (“Überweisungen”) or medications (“Verordnungen”).
VAD (eHC)	“Verification Authentication Data”: PIN codes or a resetting code entered by a card holder to activate certain functions of the TOE. Note: The eHC PIN is in particular **not** the same PIN as a PIN used for qualified electronic signatures.
RAD (eHC) PIN.CH, PIN.home	“Reference Authentication Data”: The PINs and corresponding resetting code values stored in the TOE and used for comparison with the VAD entered by the card holder. Note: Again this is **not** identical to similar values for an electronic signature provided by the eHC.
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 (EF Logging)	Data stored in the TOE in order to document the last fifty accesses to medical data by care providers.
Card Authentication Private Key PrK.eGK.AUT_CVC	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.

Card Verifiable Authentication Certificate MF/EF.C…	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) 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 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.
Client-Server Authentication Private Keys PrK.CH.AUT, PrK.CH.AUTN.	The Client-Server Authentication Private Keys are asymmetric cryptographic keys used for the authentication of a client application acting on behalf of the card holder to a server.
Decipher Private Keys PrK.CH.ENC PrK.CH.ENCV	The Document Cipher Key Decipher Keys are asymmetric private keys used for document decryption on behalf of the card holder.
Display message EF.DM	Used as a means for the card holder to check if a secure channel is established.
X.509 certificates EF.C.CH	Certificates for the keys used in the context of Service_Client_Server_Auth and Service_Data_Decryption. These certificates are provided by the card to other entities, who want to verify the validity of the card's keys used for these services.
Public Key for CV Certificate Verification PUK.RCA.CS	Public keys of Certification Authorities used for verification of the card verifiable certificates.
Secret Keys for interaction with the "health insurance agency service provider" SK.VSD	Two symmetric keys for MAC-Calculation and encryption purposes during interaction with the "health insurance agency service provider (VSDD)"
Secret Keys for interaction with the "download service provider" SK.CMS	Two symmetric keys for MAC-Calculation and encryption purposes during interaction with the "download service provider called card application management system (CAMS)"
Secret Keys for interaction with the "combined services provider" SK.VSDCMS	Two symmetric keys for MAC-Calculation and encryption purposes during interaction with the "combined services provider"
Permission data EF.Einwilligung	These data contain information about permissions given by the card holder to use specific applications in the card "freiwillige Anwendungen"
reference data (voluntary application) EF.Verweis	Data of a so called "freiwillige Anwendung" (these are application which may only be used if a patient has allowed this explicitly before the first use).
Emergency data EF.eNotfalldaten EFStatusNotfalldaten	Emergency data ("Notfalldaten") are a specific part of "medical data (voluntary application)".
D.SCD	Signature asymmetric Private key. It may be generated internally by the card (onboard generation). This key is unique, linked to **D.SVD**, and used only by the signatory.
D.SVD	Signature asymmetric Public key. The integrity of **D.SVD** must be ensured whenever it is exported from the TOE.
D.DTBS	Integrity of the Data To Be Signed (DTBS) and of the DTBS representation. (Set of data or its representation which is intended to be signed (their integrity must be maintained).
D.VAD	Confidentiality and authenticity of the Verification Authentication Data. VAD means authentication data provided as input by user (PIN)
D.RAD	Integrity and confidentiality of Reference Authentication Data. RAD means data to be persistently stored by the TOE for verification of the authentication attempt as authorized user (PIN).
D.SIGN_APPLI	Signature Application code using the SCD.
D.SIGNATURE	Signature generated by the SSCD. The unforgeability of **D.SIGNATURE** must be assured.

D.IMAGE	Image inclusive data to verify authenticity and integrity of EEPROM image during initialisation phase.

Table 3 – Data Objects list

3.1.2 Subjects

Card holder	The card holder 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 card holder: The patient is the person who uses the eHC in order to receive e. g. treatment by a doctor. Normally the patient is identical to the card holder. However, the patient may be incapable of using the card himself (e. g. children) and the card holder 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 card holder, however the latter may be for example a child of the former. However, since the TOE cannot distinguish these roles, only the card holder is defined as a subject.
Health Professional	Person acting as health professionals providing medical care to a patient (e.g. physician, dentist, pharmacist, psychotherapist …). 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’. Role id 2A: allows to write an electronic prescription to the eHC or to change it and allows comparable rights for other medical data. Role id 3A: also allows reading and modify/delete an (existing) electronic prescription. Role id 4A: allows no specific rights for an electronic prescription but may allow read and write access for certain other medical information. Role id 5A: also allows reading 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 emergency data and may be the Role-Id for emergency personnel
Medical Assistant	Persons supporting an Health Professional. These health employees usually hold a HPC with a Card Verifiable Certificate of the Card Authentication Key with Role ID corresponding to that of the health professional whom they support i.e. ‘2A’, ‘3A’, ‘4A’,’5A’ or ‘7A’. The additional Role IDs ‘6A’, ‘8A’ and ‘9A’ are defined for specific purposes
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 Role ID ‘2A’, ‘3A’, ‘4A’, ‘5A’ or ‘7A’. The additional Role IDs ‘6A’ , ‘8A’ and ‘9A’ are defined for specific purposes
Self Service Terminal	A self service terminal allows a card holder 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’.
Health insurance agency service provider	The “health insurance agency service provider” interacts with the TOE on behalf of the health insurance agency (VSDD). The service provider uses a security module (e. g. in form of a SMC), which is authenticated by use of the key SK.VSD. .
TOE manufacturer (2) **(2) The TOE manufacturer is named Card manufacturer in the ST**	Person(s) responsible for development and production of the TOE. Note: According to the life cycle description the initialisation of the card is either done by the TOE manufacturer or by the personalisation service provider.

Personalisation service provider	person(s) responsible for personalisation of the card Methods to authenticate this role may be TOE specific and have to be defined in the Security target of a TOE. Note: This role is only responsible for the personalisation in phase 6 of the TOE's life cycle and has no access rights in 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. (Card management system CMS) The service provider uses a security module (e. g. in form of a SMC), which is authenticated by use of the key SK.CMS. Note: There may be other more specific roles to produce data for the TOE like certificate service providers. However, since the card cannot distinguish such more specific roles technically according to an authentication mechanism in the card, such roles will not be defined as subjects.
combined services provider	name for the combination of the health insurance agency service provider and the download service provider (in case a decision 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 authorized (as one of the preceding roles).
S.User	End user of the TOE which can be identified as S.Admin or S.Signatory
S.Admin	User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions.
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.
S.OFFCARD	**Attacker**. A human (including S.User, S.Admin, S.Signatory) or a process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker is to access Application sensitive information. Since the current evaluation level is **EAL4+**, the attacker has a **high level potential attack** and **knows no secret.**

Table 4 – Subjects list

Notation remarks :

1/ As we tried to be closed to the PP SSCD, we keep the same acronyms.

So SCD is used for signature creation data and D.SCD is used for RSA private key.

It's the same for SVD used for signature verification data and D.SVD is used for the RSA public key

2/ RAD is used for eHC and D.RAD for SSCD. (Idem for VAD and D.VAD).

But sometimes we just note PIN (VAD) or Pin (RAD) to distinguish RAD type from VAD type.

3.2 THREATS

The threats are those defined by the eHC PP and SSCD PP. Additional threats are listed at the end of following table.

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.. Assets to be protected : TOE_ES and TOE_APP
T.Forge_Internal_Data	**Forge of User or TSF data :** An attacker with high attack potential try to forge internal user data or TSF data Assets to be protected : TOE_ES and TOE_APP
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 Assets to be protected : TOE_ES and TOE_APP
T.Intercept	**Interception of Communication** An attacker with high attack potential try 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 the transmitted sensitive data classified as assets Assets to be protected : TOE_ES and TOE_APP
T.Phys_Tamper	Physical Tampering An attacker with high attack potential may perform physical probing of the IC in order : • to disclose User Data, • to disclose/reconstruct the IC Embedded Software or • to disclose TSF data. An attacker may physically modify the IC in order to : • modify security features or functions of the IC, • modify security functions of the IC Embedded Software, • to modify User Data or • to modify TSF data. Assets to be protected : TOE_ES and TOE_IC
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. Assets to be protected : TOE_ES and TOE_IC
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 : • deactivate or modify security features or functions of the TOE or • circumvent or deactivate or modify security functions of the IC Embedded Software. Assets to be protected : TOE_ES and TOE_IC
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 to : • disclose or manipulate User Data,

	• to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or • to disclose or manipulate TSF Data. Assets to be protected : TOE_ES and TOE_IC
T.Hack_Phys	Physical attacks through the TOE interfaces The **S.OFFCARD** interacts with the TOE interfaces to exploit vulnerabilities to gain fraudulent access to the **Assets** .
T.SCD_Divulg	Storing, copying, and releasing of **D.SCD** The **S.OFFCARD** can store, copy **D.SCD** outside the TOE. **S.OFFCARD** can release **D.SCD** during generation, storage and use for signature-creation in the TOE.
T.SCD_Derive	Deduction of **D.SCD** The **S.OFFCARD** can deduce the **D.SCD** from public known data such as the **D.SVD**, signature created with the **D.SCD** or any data communicated outside the SSCD.
T.Sig_Forgery	Forgery of **D.SIGNATURE** The **S.OFFCARD** can forges the signed data object maybe together with its electronic signature **D.SIGNATURE** and the violation is not detectable by **S.Signatory** or by third parties.
T.Sig_Repud	Repudiation **D.SIGNATURE** The **S.OFFCARD** can successfully threaten any of the **assets**. Then the non-repudiation of **D.SIGNATURE** is compromised. This result in **S.Signatory** is able to deny having signed data using **D.SCD** in the TOE under his control even if **D.SIGNATURE** is successfully verified with **D.SVD** contained in his un-revoked certificate.
T.SVD_Forgery	Forgery of the **D.SVD** The **S.OFFCARD** forges **D.SVD** presented by the TOE. This result in loss of **D.SVD** integrity in the certificate of **S.Signatory**.
T.DTBS_Forgery	Forgery of **D.DTBS** The **S.OFFCARD** modifies **D.DTBS** sent by the SCA. Thus the **D.DTBS** used by the TOE for signing does not match the **D.DTBS** **S.Signatory** intended to sign.
T.SigF_Misuse	Misuse of the **D.SIGN_APPLI** of the TOE. The **S.OFFCARD** can use unauthorised instructions or commands or sequence of commands sent to the TOE in order to misuse the **D.SIGN_APPLI** with the aim of generating **D.SIGNATURE** for data that **S.Signatory** has not decided to sign.
Additional threats (not defined by eHC PP or SSCD PP)	
T.EEPROM (3) (3) T.EEPROM is an additional threat (not defined by the PP) – see chapter 7	Load wrong **D.IMAGE** The **S.OFFCARD** can load a **D.IMAGE** which authenticity and/or integrity is not given.

Table 5 – Threats list

3.3 Assumptions

A.Users	**Adequate usage of TOE and IT-Systems in the environment.** The card holder of the TOE uses the TOE adequately. In particular he doesn't tell the PIN (or PINs) of the eHC to others and doesn't hand the card to unauthorized persons. Other actors 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 smartcards, in order to prevent counterfeit of the TOE. The same requirements hold for all activities belonging to Initialisation phase, 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 delivered by the TOE manufacturer in form of smart card modules, which are the inserted into the plastic cards at a larger stage. .
A.CGA	Trustworthy **CGA** The CGA protects the authenticity of the signatory's name and the **D.SVD** in the qualified certificate by an advanced signature of the CSP.
A.SCA	Trustworthy **SCA** The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

Table 6 – Assumptions list

3.4 Organizational security policies

OSP.eHC_Spec	**Compliance to eHC specifications** The eHC shall be implemented according to the security relevant requirements of the specifications : [EHC spec part 1] [EHC spec part 2]
OSP.Additional_Applications	**Protection of additional Applications** ⇒ The TOE shall provide the possibility to authorized 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. 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.
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 Card holder has the following rights: He can read 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 Card holder of the eHC needs to be informed clearly about secure usage of the product.
OSP.Legal_Decisions	**Legal responsibility of authorized persons** The decision, which data are legally feasible for storage on the eHC has to be made by the persons authorized to deal with the data. The same holds for the decision, when data need to be deleted.
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 Servive_User_Auth_PUC • Service_Privacy • Service_Client_Server_Auth • Service_Data_Decryption • Service_Card_Management and • Service_Logging Note: The eHC also provides electronic signature services
OSP.logging	**Logging of access to medical data** All access to medical data (except reading access by the Card holder himself) must be logged. Access to the log file must be protected.
OSP.Manufact	**Manufacturing of the Smart Card** The IC Manufacturer shall ensure the quality and integrity of the manufacturing process and control the smart card material during development and production of the TOE.
P.CSP_Qcert	Qualified certificate The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive [DIRECTIVE], i.e., inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.
P.Qsign	Qualified electronic signatures The signatory uses a signature-creation system to sign data with qualified electronic signatures according to the Directive [DIRECTIVE], article 5, paragraph 1.The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate and is

	created by a SSCD.
P.Sigy_SSCD	TOE as secure signature-creation device The TOE implements the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

Table 7 – OSPs list for Digital Signature Application

Service_Asym_Mut_Auth_w/o_SM (5): 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.

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.

(5) 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. This service requires PIN entry.

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.

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 organization, 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 card holder 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.
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 card holder may deactivate sensitive medical data in the eHC. In order to use this service he authenticates himself with a PIN.

This service allows the card holder to prevent health care providers from accessing data, which the card holder 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.

Service_Client_Server_Auth: The eHC implements a PKI application, which in particular allows to use 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. In order to use this service the card holder authenticates himself with a

PIN. One of the keys can also be used without authentication by the card holder but requires authentication by a HPC or SMC in this case.

This service may for example be useful if the card holder wants to access a server provided by the health insurance organization, where confidential data of the card holder 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 following two possibilities of authentication for this service:

- In order to use this service the cardholder authenticates himself with a PIN. One of the key pairs requires that the cardholder authenticates himself with his PIN.home in order to access this service.

- One of the keys can also be used without authentication by the cardholder, but requires authentication by a HPC or SMC in this case. 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 cardholder's permission or with the authentication of a health professional. So it can also be seen as a privacy feature.

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.

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.

4. TOE SECURITY OBJECTIVES

OBJECTIVES OF THE CHAPTER

The objective of this chapter is to furnish the definition of the security objectives for the TOE and its environment. Security objectives address all the security environment aspects identified in the chapter above.

4.1 SECURITY OBJECTIVES FOR THE TOE

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 (define in following chapter) **Implementation of the security policies OSP.eHC_Spec, OSP.Electronic_Prescriptions, OSP.Logging** **Coverage of the threats T.Compromise_Internal_Data, T.Forge_Internal_Data, T.Misuse and T.Intercept**
OT.AC_Pers	**Access control for personalisation** The TOE must ensure that the Personalisation data can be written by an authorized personalisation service provider. **Implementation of the security policy OSP.eHC_Spec** **Coverage of the threats T.Compromise_Internal_Data, T.Forge_Internal_Data, T.Misuse and T.Intercept**
OT.Additional_Applications	**Protection of additional Applications** The TOE shall provide the possibility to authorized 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. **Implementation of the security policies OSP.eHC_Spec, OSP.Additional_Applications**
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 **Implementation of the security policies OSP.eHC_Spec, OSP.Services, OSP.Logging** **Coverage of the threats T.Compromise_Internal_Data, T.Forge_Internal_Data, T.Misuse and T.Intercept**
OT.Cryptography	**Implementation of cryptographic algorithms** The cryptographic algorithms required by the eHC specifications, are implemented according to their definition.

	These algorithms are: • RSA o PKCS #1 V1.5 o ISO 9796-2 (modes DS1 and DS2) o RSA OAEP • SHA-256 • 3TDES. **Implementation of the security policy OSP.eHC_Spec** **Coverage of the threats T.Compromise_Internal_Data, T.Forge_Internal_Data, T.Misuse and T.Intercept**
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 **Coverage of the threat T.Information_Leakage**
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. **Coverage of the threat T.Phys-Tamper**
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. **Coverage of the threat T.Malfunction**
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 • to disclose critical User Data, • to manipulate critical User Data of the Smartcard Embedded Software, • to manipulate Soft-coded Smartcard Embedded Software or • 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.

	Coverage of the threat T.Abuse_Func
OT.EMSEC_Design	**Physical emanations limitation** **The TOE shall be designed and build in such a way as to control the production of intelligible emanations within specified limits.** **Coverage of the threats T.Hack_Phys, T.Sig_Forgery, T.Sig_Repud**
OT.Lifecycle_Security	**Lifecycle_Security** **The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide safe destruction techniques for D.SCD in case of re-generation** **Coverage of the threats T.Sig_Forgery, T.Sig_Repud**
OT.Datas_Secrecy (6) (6) OT.Datas_Secrecy is equivalent to OT.SCD_Secrecy	**Secrecy of signature-creation datas** **The TOE shall ensure that the confidentiality of its temporally stored or persistently stored secrets is reasonably assured against attacks with a high attack level :** • **D.VAD: temporally stored data, used for signatory authentication.** • **D.RAD: persistently stored data, used for signatory authentication.** • **D.SCD: imported or generated and persistently stored data, used for signature generation.** **Coverage of the threats T.Hack_Phys, T.SCD_Divulg, T.Sig_Forgery, T.Sig_Repud**
OT.SCD_SVD_Corresp	**Correspondence between D.SVD and D.SCD** **The TOE shall ensure the correspondence between the D.SVD and the D.SCD, if they are generated by or imported into the TOE.** **The TOE shall verify on demand the correspondence between the D.SCD stored by the TOE and the D.SVD sent to the TOE on demand.** **Coverage of the threats T.Sig_Forgery, T.Sig_Repud**
OT.SVD_Auth_TOE	**TOE ensures authenticity of D.SVD** **The TOE shall provide means to enable the CGA to verify the authenticity D.SVD that has been exported by that TOE.** **Coverage of the threats T.Sig_Forgery, T.Sig_Repud, T.SVD_Forgery**
OT.Tamper_ID	**Tamper detection** **The TOE shall provide system features that detect physical tampering of a system component, and use those features to limit security breaches.** **Coverage of the threats T.Hack_Phys, T.Sig_Forgery, T.Sig_Repud**
OT.Tamper_Resistance	**Tamper resistance** **The TOE shall prevent or resist physical tampering with specified system devices and components.** **Coverage of the threats T.Hack_Phys, T.Sig_Forgery, T.Sig_Repud**
OT.Init	**Secure D.SCD/D.SVD generation** **The TOE shall provide security features to ensure that the generation of the D.SCD and the D.SVD is invoked by authorized users only.**

OT.SCD_Unique	**Uniqueness of D.SCD** **The TOE shall ensure the cryptographic quality of the D.SCD/D.SVD pair for the qualified electronic signature. D.SCD used for signature generation can practically occur only once and cannot be reconstructed from D.SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible low.** **Coverage of the threats T.SCD_Derive, T.Sig_Repud**
OT.DTBS_Integrity_TOE	**Verification of the D.DTBS-representation integrity** **The TOE shall verify that the D.DTBS-representation received from the SCA has not been altered in transit between the SCA and the TOE. The TOE itself shall ensure that the DTBS-representation is not altered by the TOE as well. Note, that this does not conflict with the signature-creation process where the DTBS itself could be hashed by the TOE.** **Coverage of the threats T.DBTS_Forgery,, T.SigF_Misuse, T.Sig_Repud**
OT.Sigy_SigF	**D.SIGN_APPLI for S.Signatory only** **The TOE shall provide the signature generation function for the legitimate signatory only and shall protect D.SCD against the use of others. The TOE shall resist attacks with high attack potential.** **Coverage of the threats T.SigF_Misuse, T.Sig_Repud**
OT.Sig_Secure	**Cryptographic security of D.SIGNATURE** **The TOE shall generate D.SIGNATURE that cannot be forged without knowledge of the D.SCD through robust encryption techniques. D.SCD cannot be reconstructed D.SIGNATURE. D.SIGNATURE shall be resistant against these attacks, even when executed with a high attack potential.** **Coverage of the threats T.SCD_Derive, T.Sig_Forgery, T.Sig_Repud**
OT.EEPROM (7) (7) OT.EEPROM is an additional security objective (not defined by the PP) – see chapter 7	**Verification of the D.IMAGE authenticity and integrity.** **The TOE shall only load and store the data object D.IMAGE if it is authentic and has not been altered.** **Coverage of the threats T.EEPROM**

Table 8 – TOE's objectives list

4.1.1 SFP access Rules for Electronic Health Application

The following subjects may interact with the TOE:
Card holder, Medical Assistant, Health professional, 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.

The following objects are covered by the policy:
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 Certificate, Client-Server Authentication Private Key, Decipher Private Key, Display message, X.509 certificates, Public Key for CV Certification Verification, SK.VSD, SK.CMS, permission data, reference data (voluntary application), emergency data.

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 and Service_User_Auth_PUC

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. 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, [eHC spec part 2].

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. The Download service provider and the Combined Services Provider have the right to delete the data. The commands used for this require protection by secure messaging with MAC (and therefore authentication by the service Service_Sym_Mut_Auth_with_SM).
Rule_2: Personal and health insurance data (protected) can be read by: Card holder, Health professional, Medical Assistant, Security Module Card (health care), (Role ‘7A’ requires additional authentication of the Card **holder** with PIN.CH), 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 (of the response) and MAC in case of health insurance agency service provider or combined services provider.
Rule_3: Data of type Electronic prescription can be read or deleted by Health Professional, Medical Assistant, Security Module Card (health care) with one of role ids ‘2A’, ‘3A’, ‘5A’, ‘6A’ and ‘9A’ (the last one only in connection with PIN.CH. The Card holder can read the data and he has the following rights: He can deactivate or activate and also delete an Electronic prescription. Only specific Health Professional or Medical Assistant with role ID 2A and Security Module Card (health care) with one of the role Ids ‘2A’, ‘3A’, ‘5A’ or ‘6A’ can write these data. Note: Technically the ability of the card holder to delete an Electronic prescription is realized by the right to modify EF.eVerordnungsTicket. The confidentiality of the contents of the electronic prescription is ensured by encryption of the EF_.eVerordnungsContainer with a key stored in EF.eVerordnungsTicket. The Download service provider and the Combined Services Provider have the right to delete EF. eVerordnungsContainer The commands used for this require protection by secure messaging with MAC (and therefore authentication by the service Service_Sym_Mut_Auth_with_SM).
Rule_4: Data of type RAD (eHC): The PIN.CH and PIN.home may be modified by the Card holder, 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 Card holder after authentication with the PUC. Note: VAD (eHC) stands for PIN or resetting code values, which are entered by the Card holder in clear text and therefore require are 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 (the last case requires additional authentication with PIN.CH). 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). The data can be read by the Card holder.

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 interact during the service.

Rule_7:
The Card Verifiable Authentication Certificate 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 Card holder (either with PIN.home or with PIN.CH combined with one of the roles ‘1A’, ‘2A’, ‘3A’, ‘4A’, ‘5A’, ‘6A’, in case of PrK.CH.Aut also PIN.CH combined with role ‘9A’) ..
For the second authentication key PrK.CH.AUTN the service Service_Client_Server_Auth is allowed for the Card holder or after authentication by Health Professional, Medical Assistant, Security Module Card (health care), all of these with Role IDs ‘2A’, ‘3A’, ‘4A’,‘5A’,’6A’ , ‘8A’, ‘9A’..

For the second decryption key PrK.CH.ENCV the service Service_Data_Decryption is also allowed for the Card holder or after authentication by Health Professional, Medical Assistant, Security Module Card (health care) all of these with Role ID ‘2A’, ‘3A’ , ‘4A’, ‘5A’, ‘6A’. In addition it is allowed for Role ID ‘9A’ in connection with PIN.CH.

Rule_9:
The Public Keys for CV Certification 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.VSD, SK.VSDCMS and SK.CMS cannot 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 (of the command message) and MAC.

Rule_12:
The Download 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 MAC (and therefore authentication by the service Service_Sym_Mut_Auth_with_SM).

Rule_13:
The Display message can be written only by the Card holder. 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 card holder.

Rule_14:
The X.509 Certificates EF.C.CH.AUTand EF.C.CH.ENC can be read by everybody.
Reading EF.C.CH.AUTN and EF.C.CH.ENCV is allowed for the Card holder, the Download service provider and the Combined service provider and for entities authenticated as one of the Role Ids ‘2A’, ‘3A’, ‘4A’, ‘5A’, ‘6A’. In addition EF.C.CH.AUTN can be read for Role IDs ‘8A’ and ‘9A’, while

EF.C.CH.ENCV can be read for Role ID ‘)A’ in connection with PIN.CH. All of the X.509 Certificates can be written by the download service provider and the combined service provider. Reading and writing by these entities requires protection by secure messaging with encryption for EF.C.CH.AUT and EF.C.CH.ENC and MAC for all of them.
Rule_15: The permission data can be read by the Card holder(using PIN.home or PIN.CH in combination with a self service terminal), and by those Health professional, Medical Assistant, Security Module Card (health care) who have Role Ids ‘2A’, ‘3A, ‘4A’ or ‘6A’’. They can be written by those Health professional, Medical Assistant and by Security Module Card (health care) with Role ID ‘2A’, ‘3A’ or ‘4A’. Reading and writing requires additional authentication using PIN.CH. (except if the Card holder reads or writes using PIN.home). They can be deactivated and activated by the Card holder in connection with a Self Service Terminal and by authenticated subjects with role ID ‘2A’, ‘3A’, ‘4A’ in combination with PIN.CH.
Rule_16: The reference data (voluntary application) can be read by the Card holder and by all authenticated subjects with role ID ‘2A’, ‘3A’, ‘4A’, ‘6A’, ‘9A’ in combination with PIN.CH.. They can be written by the Card holder and by Health professional, by Medical Assistant and by Security Module Card (health care) with specific Role IDs 2A, 3A or ‘4A’ or ‘9A’ together with the Card holder (using PIN.CH). They can be deactivated and activated by the Card holder in connection with a Self Service Terminal and by authenticated subjects with role ID ‘2A’, ‘3A’, ‘4A’ in combination with PIN.CH.
Rule_17: The Emergency data can be written by Health Professional, Medical Assistant and Security Module Card (health care) with Role ID ‘2A’ but only together with the Card holder (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’, ‘3A’ or ‘4A’ but for the last two IDs only together with the Card holder (PIN.CH) . They can be deactivated or activated by the Card holder .

Table 9: Access Control Policy for Usage Phase : SFP_ACCESS_RULES

4.2 SECURITY OBJECTIVES FOR THE 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. **Implementation of the security policy OSP.Manufact**
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 initialize, to pre-personalize genuine smart card materials in order to prevent counterfeit of the TOE. **Implementation of the security policy OSP.Manufact**
OE.Users	**Adequate usage of TOE and IT-Systems in the environment.** The Card holder 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 unauthorized persons.

	Implementation of the assumption A.Users
OE.legal_decisions	**Legal responsibility of authorized persons** The decision, which data are legally feasible for storage on the eHC has to be made by the persons authorized 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), except the Card holder (who's behavior is covered by other objectives) and the category "Other person", which includes attackers. **Implementation of the security policies OSP.Electronic_Prescriptions, OSP.Legal_Decisions, OSP.Logging** **Coverage of the threats T.Compromise_Internal_Data, T.Forge_Internal_Data, T.Misuse and T.Intercept**
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) use adequate protection for confidentiality and integrity of these data. **Implementation of the security policies OSP.Electronic_Prescriptions** **Coverage of the threats T.Compromise_Internal_Data, T.Forge_Internal_Data, T.Misuse and T.Intercept**
OE.User_information	**Information about secure usage** The Card holder of the TOE must be informed clearly about secure usage of the product. **Implementation of the security policy OSP.User_Information**
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 delivered by the TOE manufacturer in form of smart card modules, which are then inserted into the plastic cards at a later stage. **Implementation of the security policy OSP.Additional_Applications** **Implementation of the assumption A.Perso**
OE.CGA_Qcert	Generation of qualified certificates The CGA generates qualified certificates which include inter alia (a) the name of the signatory controlling the TOE, (b) **D.SVD** matching **D.SCD** implemented in the TOE under sole control of the signatory, (c) the advanced signature of the CSP.
OE.SVD_Auth_CGA	CGA verifies authenticity of **D.SVD**

	The CGA shall verify that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA shall verify the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.
OE.HI_VAD	Protection of **D.VAD** If an external device provides the human interface for user authentication, this device shall ensure confidentiality and integrity of **D.VAD** as needed by the authentication method employed.
OE.SCA_Data_Intend	Data intended to be signed The SCA (a) shall generate the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE, (b) shall send the DTBS-representation to the TOE and shall enable verification of the integrity of the DTBS-representation by the TOE (c) shall attached the signature produced by the TOE to the data or shall provide it separately.

Table 10 – Environment's objectives list for the Electronic Health Application

5. TOE SECURITY REQUIREMENT

OBJECTIVES OF THE CHAPTER

The objective of this chapter is to furnish the definition of the functional requirements for the TOE using security functional requirement components drawn from [CCPART2] extended and the definition of the assurance requirements for the TOE using only assurance components drawn from [CCPART3]. Some security functional requirements represents extension to [CCPART2]

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

The TOE Security functional requirements define the functional requirements for the TOE using functional requirement components drawn from [CCPART2] extended.
The minimum strength level for the TOE security functions is **SOF-high**. According to [CEM] part 2 section 422, the strength of cryptographic algorithms is outside the scope of the CC evaluation.

5.1.1 TOE security functional requirements list

Black highlighted in blue: SFR identical in both application (Electronic Health application and SSCD application)

Green : SFR itered in both application (Electronic Health application and SSCD application) but iteration are not identical most of the time

Black : SFR for SSCD application

Blue : SFR for Electronic Health application

The CC allows several operations. Each of these operations is used in this document :

- The *refinement* operation is used to add detail to a requirement. Refinement of security requirements is denoted by the word **refinement**.
- The *assignment* operation is used to assign a specific value . Assignment is denoted by using **bold**.
- 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.
- The *selection* operation is used to select one or more options. Selections are denoted as **underlined bold text.**

Identification	Description
FCS	Cryptographic support
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FCS_RND.1(9)	Random Number Generation
FDP	User data protection
FDP_ACC.1	Subset access control
FDP_ACC.2	Complete Access Control
FDP_ACF.1	Security attribute based access control
FDP_ETC.1	Export of user data without security attributes
FDP_ITC.1	Import of user data without security attributes
FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored Data integrity
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FIA	Identification and authentication
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.4	Single-use authentication mechanisms
FIA_UID.1	Timing of identification
FMT	Security management
FMT_LIM.1(9)	Limited capabilities
FMT_LIM.2(9)	Limited availability
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT	Protection of the TSF
FPT_AMT.1	Abstract machine testing
FPT_EMSEC.1 (9)	TOE Emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_TST.1	TSF testing
FTP	Trusted path/channels
FTP_ITC.1	Import of user data without security attributes
FTP_TRP.1	Trusted path

Table 11 – TOE security functional requirements list

(9) This requirement is an extension to [CCPART2].

5.1.1.1 FCS – Cryptographic support

5.1.1.1.1 FCS_CKM.1

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** and specified cryptographic key sizes ***168 bit*** that

	meet the following : **[EHC spec part 1]**
FCS_CKM.1.1 /GENKEY	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **GEMALTO Proprietary Algorithm** and specified cryptographic key size ***of 2048* bit** that meet the following: **[EHC spec part 1]**

5.1.1.1.2 FCS_CKM.4

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method : • **Volatile keys are destroyed by overwriting RAM area with 00** • **Permanently stored keys (in EEPROM) are overwritten by their new values if updated** that meets the following: **None**

5.1.1.1.3 FCS_COP.1.1

FCS_COP.1.1/ HASH	The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA 256** and cryptographic key sizes **none** that meet the following**: FIPS 180-2**
FCS_COP.1.1/ CCA_SIGN	The TSF shall perform **digital signature-creation** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key size of **2048 bits** that meet the following: **[EHC spec part 1]**
FCS_COP.1.1/ CCA_VERIF	The TSF shall perform **digital signature-verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key size of **2048 bits** that meet the following: **[EHC spec part 1]**
FCS_COP.1.1/ CSA	The TSF shall perform **digital signature-creation** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **2048 bits** that meet the following: **[EHC spec part 1]**
FCS_COP.1/ ASYM_DEC	The TSF shall perform **decryption** in accordance with a specified cryptographic algorithm **RSA PKCS#1 V1.5 and RSA OAEP** and cryptographic key **2048 bits length** that meet the following: **[EHC spec part 1]**
FCS_COP.1.1/ SYM	The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **3TDES in CBC mode** and cryptographic key size of **168 bits** that meet the following: **[EHC spec part 1]**
FCS_COP.1.1/ MAC	The TSF shall perform **generation and verification of message authentication code** in accordance with a specified cryptographic algorithm **Retail MAC** and cryptographic key size of **168 bits** that meet the following: **[EHC spec part 1]**
FCS_COP.1.1/CORRESP	The TSF shall perform **SCD/SVD correspondence verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key size of **2048 bit** that meet the following **[EHC spec part 1]**
FCS_COP.1.1/SIGNING	The TSF shall perform **digital signature generation** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key size of **2048 bit (10)** that meet the following: **[EHC spec part 1]** (10) Notification in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance Published in Federal Gazette No 13, pp 346 of 27 January 2009 (in German) Minimum bit length : 1280 up to end 2008 - 2048 recommended 1536 up to end 2009 - 2048 recommended 1728 up to end 2010 - 2048 recommended

	1976 up to end 2015 - 2048 recommended

5.1.1.1.4 FCS_RND.1.1

FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet **K4-DRNG** (**[AIS20]**) **with seed entropy at least 112 bits and with strength of mechanism set to high.**

5.1.1.2 FDP – User data protection

5.1.1.2.1 FDP_ACC.1

FDP_ACC.1.1/ SVD TRANSFER SFP	The TSF shall enforce the **SVD Transfer SFP** on **export of D.SVD by S.User**

FDP_ACC.1.1/ INITIALISATION	The TSF shall enforce the **Initialisation SFP** on **generation of D.SCD/D.SVD pair by S.User**

FDP_ACC.1.1/ PERSONALISATION SFP	The TSF shall enforce the **Personalisation SFP** on **creation of D.RAD by S.Admin .**

FDP_ACC.1.1/ SIGNATURE-CREATION SFP	The TSF shall enforce the **Signature-creation SFP** on 1. **Sending of D.DTBS-representation by the SCA** 2. Signing of D.DTBS-representation by S.Signatory

FDP_ACC.1.1/EEPROM SFP	The TSF shall enforce the **EEPROM SFP** on **loading D.IMAGE by S.Admin** **Note :** the loading of D.IMAGE is only possible during initialisation phase

5.1.1.2.2 FDP_ACC.2

FDP_ACC.2.1	The TSF shall enforce the **SFP access Rules** on **all subjects and objects defined by SFP access Rules** 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.

5.1.1.2.3 FDP_ACF.1

ACCESS RULES

FDP_ACF.1.1/ ACCESS RULES	The TSF shall enforce the **SFP access Rules** to objects based on the following: **all subjects and objects together with their respective security attributes as defined in SFP access Rules**
FDP_ACF.1.2/ ACCESS RULES	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.**
FDP_ACF.1.3/ ACCESS RULES	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules**: none.**
FDP_ACF.1.4/ ACCESS RULES	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

INITIALISATION SFP

FDP_ACF.1.1 /INITIALISATION SFP	The TSF shall enforce the **initialisation SFP** to objects based on **General attribute** and **Initialisation attribute group.**
FDP_ACF.1.2 /INITIALISATION SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.User with the security attribute "role" set to "S.Admin" and with the security attribute "SCD/SVD management" set to "authorized" is allowed to generate D.SCD/D.SVD pair.**
FDP_ACF.1.3/INITIALISATION SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**
FDP_ACF.1.4/INITIALISATION SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: **S.User with the security attribute "role" set to "S.Admin" and with the security attribute "SCD/SVD management" set to "not authorized" is not allowed to generate D.SCD/D.SVD pair.**

SVD TRANSFER SFP

FDP_ACF.1.1 / SVD TRANSFER SFP	The TSF shall enforce the **SVD Transfer SFP** to objects based on **General attribute.**
FDP_ACF.1.2 / SVD TRANSFER SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.User with security attribute "role" set to "S.Admin" is allowed to export D.SVD.**
FDP_ACF.1.3/ SVD TRANSFER SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**
FDP_ACF.1.4/ SVD TRANSFER SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: **none**

PERSONALISATION SFP

FDP_ACF.1.1 / PERSONALISATION SFP	The TSF shall enforce the **Personalisation SFP** to objects based on **General attribute.**
FDP_ACF.1.2 / PERSONALISATION SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.User with the security attribute "role" set to "S.Admin" is allowed to create D.RAD.**
FDP_ACF.1.3/ PERSONALISATION SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**
FDP_ACF.1.4/ PERSONALISATION SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: **none**

SIGNATURE CREATION SFP

FDP_ACF.1.1 / SIGNATURE CREATION SFP	The TSF shall enforce the **Signature-creation SFP** to objects based on **General attribute** and **Signature-creation attribute group.**
FDP_ACF.1.2 / SIGNATURE CREATION SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.User with the security attribute "role" set to "S.Signatory" is allowed to create D.SIGNATURE for D.DTBS sent by an authorized SCA with D.SCD which security attribute "SCD operational" is set to "yes".**
FDP_ACF.1.3/ SIGNATURE CREATION SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**
FDP_ACF.1.4/ SIGNATURE CREATION SFP	The TSF shall explicitly deny access of subjects to objects based on the rule:

	(a) **S.User with the security attribute "role" set to "S.Signatory" is not allowed to create D.SIGNATURE for D.DTBS which is not sent by an authorized SCA with D.SCD which security attribute "SCD operational" is set to "yes".** (b) **S.User with the security attribute "role" set to "S.Signatory" is not allowed to create D.SIGNATURE for D.DTBS sent by an authorized SCA with D.SCD which security attribute "SCD operational" is set to "no".**

EEPROM SFP

FDP_ACF.1.1 /EEPROM SFP	The TSF shall enforce the **EEPROM SFP** to objects based on **General attribute** and **State attribute.**
FDP_ACF.1.2 /EEPROM SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.User with the security attribute "role" set to "S.Admin" is allowed to load D.IMAGE and by this setting the security attribute "state" to the value representing Life Cycle State 7: Personalisation.**
FDP_ACF.1.3/EEPROM SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**
FDP_ACF.1.4/EEPROM SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: **none**

5.1.1.2.4 FDP_ETC.1

FDP_ETC.1.1/SVD TRANSFER	The TSF shall enforce the **SVD Transfer SFP** when exporting user data, controlled under the SFP(s), outside of the TSC.
FDP_ETC.1.2/SVD TRANSFER	The TSF shall export the user data without the user data's associated security attributes.

5.1.1.2.5 FDP_ITC.1

FDP_ITC.1.1/DTBS	The TSF shall enforce the **Signature-creation SFP** when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2/DTBS	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3/DTBS	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **D.DTBS-representation shall be sent by an authorized SCA**

5.1.1.2.6 FDP_RIP.1

FDP_RIP.1.1/HEALTH_OBJ	The TSF shall ensure that any previous information content of a resource is made unavailable upon **the deallocation of the resource from** the following objects: **PINs, secret and private cryptographic keys, data in all files, which are not freely accessible.**

FDP_RIP.1.1/SSCD_OBJ	The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of resource** for the following objects: • **D.SCD** • **D.VAD** • **D.RAD**

5.1.1.2.7 FDP_SDI.2

FDP_SDI.2.1/Persistent	The TSF shall monitor user data stored within the TSC for **integrity errors** on all objects, based on the following attributes: **integrity checked persistent stored data :** ➢ **PIN (RAD, D.RAD),** ➢ **Crypto keys : Private RSA keys, symmetric authentication keys (SK.VSD/CMS), public key for certificate verification (CVC),** ➢ **User data that must be integrity checked according to** [EHC spec part 2] **(some can be updated with respect to access condition, some need not be integrity checked),** ➢ **File management access rules for files (keys and pins - cannot be updated),** ➢ **Card Life Cycle Status.**
FDP_SDI.2.2/Persistent	Upon detection of a data integrity error, the TSF shall: **1. Prohibit the use of the altered data** **2. Inform the S.Signatory about integrity error.**

FDP_SDI.2.1/Volatile	The TSF shall monitor user data stored within the TSC for **integrity errors** on all objects, based on the following attributes: **integrity checked volatile data :** ➢ **Crypto keys : session keys, public keys entered via certificate verification,** ➢ **security states,** ➢ **input for electronic signatures.**
FDP_SDI.2.2/Volatile	Upon detection of a data integrity error, the TSF shall: **3. Prohibit the use of the altered data** **4. Inform the connected entity about integrity error.**

The DTBS-representation temporarily stored by TOE has the user attribute "integrity checked stored data".

FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored within the TSC for **integrity errors** on all objects, based on the following attributes: **integrity checked stored data.**
FDP_SDI.2.2/DTBS	Upon detection of a data integrity error, the TSF shall: **1. Prohibit the use of the altered data** **2. Inform the S.Signatory about integrity error.**

5.1.1.2.8 FDP_UCT.1

FDP_UCT.1.1	The TSF shall enforce the **SFP_access_rules** to be able to **transmit and receive** objects in a manner protected from unauthorized disclosure. **Application note**: The TOE supports secure messaging with symmetric encryption (cf. SFR FCS_COP.1/SYM) after card-to-card authentication with secure messaging

5.1.1.2.9 FDP_UIT.1

FDP_UIT.1.1/ ACCESS RULES	The TSF shall enforce the **SFP_access_rules** to be able to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors.
FDP_UIT.1.2/ ACCESS RULES	The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.

FDP_UIT.1.1/SVD Transfer	The TSF shall enforce the **SVD Transfer SFP** to be able to **transmit** user data **D.SVD** in a manner protected from **modification and insertion** errors.
FDP_UIT.1.2/SVD Transfer	The TSF shall be able to determine on receipt of user data, whether **modification and insertion** has occurred.

FDP_UIT.1.1/TOE DTBS	The TSF shall enforce the **Signature creation SFP** to be able to **receive** user data **D.DTBS-representation** in a manner protected from **modification, deletion and insertion** errors.
FDP_UIT.1.2/TOE DTBS	The TSF shall be able to determine on receipt of user data, whether **modification, deletion and insertion** has occurred.

5.1.1.3 FIA – Identification and Authentication

5.1.1.3.1 FIA_AFL.1

FIA_AFL.1.1/ PIN	The TSF shall detect when 3 unsuccessful authentication (PIN.CH and PIN.home) attempts occur related to **consecutive failed human user authentication for the health care application .**
FIA_AFL.1.2/ PIN	When the 3 unsuccessful authentication attempts has been met or surpassed, the TSF shall **block the PIN (PIN.CH and PIN.home) for authentication until successful unblock with resetting code.**
FIA_AFL.1.1/ PUC	The TSF shall detect when **10 successful** or unsuccessful authentication attempts occur related to **usage of the eHC-PIN unblocking code.**
FIA_AFL.1.2/ PUC	When the defined number of **successful** or unsuccessful authentication attempts has been met or surpassed, the TSF shall ***block the PIN unblocking code*.**
FIA_AFL.1.1/ D.RAD	The TSF shall detect when **3** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts using D.RAD**
FIA_AFL.1.2/ D.RAD	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **Block D.RAD.**
FIA_AFL.1.1/PUK	The TSF shall detect when **10** unsuccessful authentication attempt occur related to **authentication using PUK.**
FIA_AFL.1.2/PUK	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **Block PUK usage.**

5.1.1.3.2 FIA_ATD.1

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: **identity and role.** **Application note :** Applies to (i) the human user authentication, i.e. the card holder, 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_ATD.1.1/ D.RAD	The TSF shall maintain the following list of security attributes belonging to individual users: **D.RAD.**

5.1.1.3.3 FIA_UID.1

FIA_UID.1.1/ HEALTH	The TSF shall allow **(1) reading the ATR** **(2) reading the Card Verifiable Authentication Certificate,** **(3) reading the Certificate Service Provider Certificate** **(4) reading EF_GDO (containing ICCSN)** **(5) reading EF_DIR (listing all applications)** **(6) Selecting Applications (Select(AID)** **(7) Changing SE with ManageSecutityEnvironment (Restore)**

	on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/ HEALTH	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
FIA_UID.1.1	The TSF shall allow: 1. **Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE** 2. **Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS_import** 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

5.1.1.3.4 FIA_UAU.1

FIA_UAU.1.1/ HEALTH	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) Identification by providing the users eHC-PIN** **(5) identification by providing the users certificate** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/ HEALTH	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_UAU.1.1	The TSF shall allow: 1. **Identification of the user by means of TSF required FIA_UID.1** 2. **Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE** 3. **Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS_import** 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.

5.1.1.3.5 FIA_UAU.4

FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to **Card-to-Card Authentication Mechanism** **Application note:** The Card-to-Card Authentication Mechanism 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/SYM 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.

5.1.1.4 FMT – Security Management

5.1.1.4.1 FMT_LIM.1

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.

5.1.1.4.2 FMT_LIM.2

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.**

5.1.1.4.3 FMT_MOF.1

FMT_MOF.1.1 /	The TSF shall restrict the ability to **enable** the function **Signature-creation function** to **S.Signatory.**

5.1.1.4.4 FMT_MSA.1

FMT_MSA.1.1 / Administrator	The TSF shall enforce the **following functions** to restrict the ability to **do the following operations** on the **following security attributes** to **S.Admin.**		
Functions	**Operations**	**Attributes**	**Phase**
EEPROM SFP	**Switch from value 6 to 7**	**State attribute**	**5a**
Initialisation SFP	**Modify**	**SCD/SVD Management**	**5b**

FMT_MSA.1.1 / Signatory	The TSF shall enforce the **following functions** to restrict the ability to **do the following operations** on the **following security attributes** to **S.Signatory.**		
Functions	**Operations**	**Attributes**	**Phase**
Signature-Creation SFP	**Modify**	**SCD operational**	**7**

5.1.1.4.5 FMT_MSA.2

FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.

5.1.1.4.6 FMT_MSA.3

FMT_MSA.3.1	The TSF shall enforce **Initialisation SFP and Signature-creation SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2	The TSF shall allow the **S.Admin** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1 /EEPROM	The TSF shall enforce **EEPROM SFP** to provide **restrictive** default values "State" is set to "1" for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 /EEPROM	The TSF shall allow **none** to specify alternative initial values to override the default values when an object or information is created.

5.1.1.4.7 FMT_MTD.1

FMT_MTD.1.1/ ini	The TSF shall restrict the ability to **write** the **Initialisation data** to **the TOE manufacturer .**

FMT_MTD.1.1/ pers	The TSF shall restrict the ability to **write** the **Personalisation data** to **the Personalisation service provider .** Application note : 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.1.1/ CMS	The TSF shall restrict the ability to **write** 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 to the Download service provider.**
FMT_MTD.1.1/ PIN	The TSF shall restrict the ability **to modify and unblock** the **PIN** to **the Card Holder .** Application note : The cardholder modifies his or her PIN as special case of the User Authentication Reference Data by means of : * the command CHANGE REFERENCE DATA and providing the old and the new PIN or * the command RESET RETRY COUNTER and providing the PUC and the new PIN. He or she unblocks the PIN by means of : * the command RESET RETRY COUNTER and providing the PUC and the new PIN or * the command RESET RETRY COUNTER and providing the PUC (without a new PIN).
FMT_MTD.1.1/ KEY_MOD	The TSF shall restrict the ability to **modify** the **Public Key for CV Certification Verification** to **none .**
FMT_MTD.1.1/D.RAD	The TSF shall restrict the ability to **modify** the **D.RAD** to **S.Signatory**

5.1.1.4.8 FMT_SMF.1

FMT_SMF.1.1/ HEALTH	The TSF shall be capable of performing the following security management functions: **1. Initialisation** **2. Personalisation** **3. the "Service_Card_Management"** 4. **Modification of the PIN**
FMT_SMF.1.1/ SSCD	The TSF shall be capable of performing the following security management functions: • **Enable Signature creation function (FMT_MOF.1),** • **Restrict ability to modify security attributes and TSF data (FMT_MSA.1.1 /Administrator FMT_MSA.1.1 / Signatory FMT_MTD1.1).** • **Restrict ability to switch security attributes values (FMT_MSA.1.1 /Administrator).**

5.1.1.4.9 FMT_SMR.1

FMT_SMR.1.1/ HEALTH	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, Card**

	holder, Download service provider, Personalisation service provider, TOE manufacturer
FMT_SMR.1.2/ HEALTH	The TSF shall be able to associate users with roles.
FMT_SMR.1.1/ SSCD	The TSF shall maintain the roles **S.Admin** and **S.Signatory.**
FMT_SMR.1.2/ SSCD	The TSF shall be able to associate users with roles.

5.1.1.5 FPT – Protection of the TSF

5.1.1.5.1 FPT_AMT.1

FPT_AMT.1.1	The TSF shall run a suite of tests **during initial start-up, periodically during normal operation** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.1.5.2 FPT_EMSEC.1

FPT_EMSEC.1.1	The TOE shall not emit **electromagnetic radiation** in excess of **Unintelligible emission** enabling access to **1. PIN and PUC and** **2. Card Authentication Private Keys,** **3. Client-Sever Authentication Private Key** **4. Document Cipher Key Decipher Key** **5. secure messaging keys.** **6. D.RAD** **7. D.SCD**
FPT_EMSEC.1.2	The TSF shall ensure **any user** are unable to use the following interface **smart card circuit contacts** to gain access to **1. PIN and PUC and** **2. Card Authentication Private Key,** **3. Client-Sever Authentication Private Key** **4. Document Cipher Key Decipher Key** 5. **secure messaging keys .**
FPT_EMSEC.1.2/ S.OFFCARD	The TOE shall ensure **attacker S.OFFCARD** are unable to use the following interface: • **I/O** • **VCC** • **Ground** to gain access to **D.RAD and D.SCD.**

5.1.1.5.3 FPT_FLS.

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 .**

5.1.1.5.4 FPT_PHP.1

FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

5.1.1.5.5 FPT_PHP.3

FPT_PHP.3.1	The TSF shall resist the following **physical tampering scenarios to the following TSF devices/elements** by responding automatically such that the TSP is not violated.
Refinement :	
Devices/Elements	Physical tampering scenarios
Hardware random generator	Inappropriate random numbers
Software random generator	Modification of the secret data of the deterministic RNG
Active Shield	Physical access to or modification of internal circuits
Clock	Frequency out of allowed range
Power supply	Voltage out of allowed range
Temperature sensor	Ambient temperature out of allowed range
Light sensor	Electromagnetic irradiation
Probing sensor	Physical access to or modification of internal circuits
Glitch sensor	Short time variations in power supply

5.1.1.5.6 FPT_TST.

FPT_TST.1.1	The TSF shall run a suite of self tests at **the following period** and **conditions** to demonstrate the correct operation of **the TSF**. The TSF shall run a suite of self tests **at the conditions** **1. Integrity verification of TSF data stored in EEPROM whenever read internally and externally.** **2. Integrity verification of TSF patches at startup** **3. Keys and Security status stored in RAM, test of integrity whenever accessed** **4. Test on proper operation of the underlaying hardware (hardware sensors always active, sensor self test before each APDU processing, tests by software at random interrupts)** **5. Test of hardware random number generator after each reset, and additionally at seed generation for the DRNG** **6. Test of integrity of the software random generator data before generation of the next random number** **7. Test if Code patches are existing, done at specific points of the ROM code (hard coded)** to demonstrate the correct operation of **the TSF.**
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of **TSF data**
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

5.1.1.5.7 FPT_RVM.1

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.

5.1.1.5.8 FPT_SEP1

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

5.1.1.6 FTP – Trusted path/channels

5.1.1.6.1 FTP_ITC.1

FTP_ITC.1.1/ ACCESS RULES	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 / ACCESS RULES	The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel
FTP_ITC.1.3 / ACCESS RULES	The TSF shall initiate communication via the trusted channel for **all functions requiring a trusted channel as defined by SFP_access_rules**.

FTP_ITC.1.1 /SVD TRANSFER	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 /SVD TRANSFER	The TSF shall permit **the remote trusted IT product CGA** to initiate communication via the trusted channel.
FTP_ITC.1.3 /SVD TRANSFER	The TSF **or the remote trusted IT product CGA** shall initiate communication via the trusted channel for **D.SVD export.**

FTP_ITC.1.1 /DTBS IMPORT	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 /DTBS IMPORT	The TSF shall permit **the remote trusted IT product SCA** to initiate communication via the trusted channel.
FTP_ITC.1.3 /DTBS IMPORT	The TSF **or the remote trusted IT product SCA** shall initiate communication via the trusted channel for **signing D.DTBS-representation.**

5.1.1.6.2 FTP_TRP.1

FTP_TRP.1.1 /TOE	The TSF shall provide a communication path between itself and **local** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2 /TOE	The TSF shall permit **local users or TSF** to initiate communication via the trusted path.
FTP_TRP.1.3 /TOE	The TSF shall require the use of the trusted path for **none**

5.2 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE security assurance requirements define the assurance requirements for the TOE using only assurance components drawn from [CCPART3].

The assurance level is **EAL4** augmented on **ADV_IMP.2 (Implementations of the TSF), AVA_MSU.3 (Misuse - Analysis and testing for insecure states)** and **AVA_VLA.4 (Vulnerability Analysis - Highly resistant).**

Identification	Description	Direct dependencies
ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	ACM_CAP.3
ACM_CAP.4	Generation support and acceptance procedures	ACM_SCP.1 ALC_DVS.1
ACM_SCP.2	Problem tracking CM coverage	ACM_CAP.3
ADO	**Delivery and Operation**	
ADO_DEL.2	Detection of modification	ACM_CAP.3

ADO_IGS.1	Installation, generation and start-up procedures	AGD_ADM.1
ADV	**Development**	
ADV_FSP.2	Fully defined external interfaces	ADV_RCR.1
ADV_HLD.2	Security enforcing high-level design	ADV_FSP.1 ADV_RCR.1
ADV_IMP.2	**Implementation of the TSF**	**ADV_LLD.1** **ALC_TAT.1**
ADV_LLD.1	Descriptive low-level design	ADV_HLD.1 ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	None
ADV_SPM.1	Informal TOE security policy model	ADV_FSP.1
AGD	**Guidance documents**	
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ALC	**Life cycle support**	
ALC_DVS.1	Identification of security measures	None
ALC_LCD.1	Developer defined life-cycle model	None
ALC_TAT.1	Well-defined development tools	ADV_IMP.1
ATE	**Tests**	
ATE_COV.2	Analysis of coverage	ADV_FSP.1 ATE_FUN.1
ATE_DPT.1	Testing: high –level design	ADV_HLD.1 ATE_FUN.1
ATE_FUN.1	Functional testing	None
ATE_IND.2	Independent testing – sample	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1
AVA	**Vulnerability assessment**	
AVA_MSU.3	Analysis and testing for insecure states	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1 ADV_HLD.1
AVA_VLA.4	highly resistant	ADV_FSP.1 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 AGD_ADM.1 AGD_USR.1

Table 12 – TOE security assurance requirements list

5.3 Security Requirements for the IT Environment

Identification	**Description**
Certification Generation application CGA	
FCS	**Cryptographic support**
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.3	Cryptographic key access
FDP	**User data protection**
FDP_UIT.1	Data exchange integrity
FTP	**Trusted path/channels**
FTP_ITC.1	Inter-TSF trusted channel
Signature Creation Application SCA	
FCS	**Cryptographic support**

FCS_COP.1	Cryptographic operation
FDP	**User data protection**
FDP_UIT.1	Data exchange integrity
FTP	**Trusted path/channels**
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path
Health application data protection	
FDP	**User data protection**
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_UIT.1	Data exchange integrity
FIA	**User identification**
FIA_UID.1	Timing of Identification
FMT	**Security management**
FMT_MTD.1	Management of the TSF data
FMT_MTD.3	Secure TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security management roles
FTP	**Trusted path/channels**
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

Table 13 – IT environment security functional requirements list

5.3.1 Certification Generation application (CGA)

5.3.1.1 FCS_CKM.2

FCS_CKM.2.1 /CGA	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **qualified certificate** that meets the following: **[ALGO].**

5.3.1.2 FCS_CKM.3

FCS_CKM.3.1 /CGA	The TSF shall perform **import the SVD** in accordance with a specified cryptographic key access method **import through a secure channel** that meets the following: **[EHC spec part 2]**

5.3.1.3 FDP_UIT.1

FDP_UIT.1.1 /SVD import	The TSF shall enforce the **SVD Import SFP** to be able to **receive** user data in a manner protected from **modification** and **insertion** errors.
FDP_UIT.1.2 /SVD import	The TSF shall be able to determine on receipt of user data, whether **modification** and **insertion** has occurred.

5.3.1.4 FTP_ITC.1

FTP_ITC.1.1 /SVD Import	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 /SVD Import	The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.
FTP_ITC.1.3 /SVD Import	The TSF **or the remote trusted product** shall initiate communication via the trusted channel for **Import SVD**

5.3.2 Signature creation application (SCA)

5.3.2.1 FCS_COP.1

FCS_COP.1.1 /SCA Hash	The TSF shall perform **hashing DTBS** in accordance with **RIPE-MD-160 and SHA-256** cryptographic algorithm and cryptographic key sizes **none** that meet the following: **all [ALGO]; for SHA-256 and for RIPEMD160: [ISO HF3] and [RIPEMD].**

5.3.2.2 FDP_UIT.1

FDP_UIT.1.1 /SCA DTBS	The TSF shall enforce the **Signature-creation SFP** to be able to **transmit** user data in a manner protected from **modification, deletion, and insertion** errors.
FDP_UIT.1.2 /SCA DTBS	The TSF shall be able to determine on receipt of user data, whether **modification, deletion,** and **insertion** has occurred.

5.3.2.3 FTP_ITC.1

FTP_ITC.1.1 /SCA DTBS	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 / SCA DTBS	The TSF shall permit **the TSF** to initiate communication via the trusted channel.
FTP_ITC.1.3 / SCA DTBS	The TSF **or the remote trusted product** shall initiate communication via the trusted channel for **sending D.DTBS-representation by means of the SSCD.**

5.3.2.4 FTP_TRP.1

FTP_TRP.1.1 / SCA	The TSF shall provide a communication path between itself and **local** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2 / SCA	The TSF shall permit **the TSF or local users** to initiate communication via the trusted path.
FTP_TRP.1.3 / SCA	The TSF shall require the use of the trusted path for **none**

5.3.3 Health application data protection

All SFRs listed in this chapter are additional SFRs not defined by the PP

5.3.3.1 FDP_ACC.2

FDP_ACC.2.1/Data Protection	The TSF shall enforce the **SFP environment Rules** on all subjects and **objects defined by SFP environment Rules** and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2/Data Protection	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.

SFP environment Rules

The medical data must be protected outside of the card.
Authorized persons who are allowed to read, write or modify data in the card have to use their rights only in an environment where unauthorized access are prevent
The data transmitted between eHC and health professionals IT equipment must be protected against attackers access in a closed environment.
The health professionals have to use security services adequately in case of transmission over insecure lines.
As these persons are in charge of handling sensitive data outside of the eHC, they must use correct confidentiality and integrity protection.
Deletion or storage of data on the eHC must be done by persons authorized to deal with the data.

5.3.3.2 FDP_ACF.1

FDP_ACF.1.1/ Data Protection	The TSF shall enforce the **SFP environment Rules** to objects based on the following: **all subjects and objects together with their respective security attributes as defined in SFP access Rules**

5.3.3.3 FDP_UIT.1

FDP_UIT.1.1/ Data Protection	The TSF shall enforce the **SFP_access_rules** to be able to **transmit** and receive user data in a manner protected from **modification, deletion, insertion and replay** errors.
FDP_UIT.1.2/ Data Protection	The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.

5.3.3.4 FIA_UID.1

FIA_UID.1.1/Data Protection	The TSF shall allow: **Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/Data Protection** On behalf of the user to be performed before the user is identified.
FIA_UID.1.2 /Data Protection	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user

5.3.3.5 FMT_MTD.1

FMT_MTD.1.1/ Perso Data	The TSF shall restrict the ability to **write** the **Personalisation data** to **the Personalisation service provider .**

5.3.3.6 FMT_MTD.3

FMT_MTD.3.1/ Perso Data	The TSF shall ensure that only secure values are accepted for TSF data

5.3.3.7 FMT_SMF.1

FMT_SMF.1.1/ Perso Data	The TSF shall be capable of performing the following security management functions: **Personalisation**

5.3.3.8 FMT_SMR.1

FMT_SMR.1.1/ Perso Data	The TSF shall maintain the role, **Personalisation service provider**
FMT_SMR.1.2/ Perso Data	The TSF shall be able to associate users with roles.

5.3.3.9 FTP_ITC.1

FTP_ITC.1.1 /Data protection	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 / Data protection	The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

5.3.3.10 FTP_TRP.1

FTP_TRP.1.1 / Data protection	The TSF shall provide a communication path between itself and **local** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2 / Data protection	The TSF shall permit **the TSF or local users** to initiate communication via the trusted path.

5.4 Security Requirements for the Non-IT Environment

R.Administrator_Guide *Application of Administrator Guidance*
The implementation of the requirements of the Directive, ANNEX II “Requirements for certification-service-providers issuing qualified certificates”, literal (e), stipulates employees of the CSP or other relevant entities to follow the administrator guidance provided for the TOE. Appropriate supervision of the CSP or other relevant entities shall ensures the ongoing compliance.

R.Sigy_Guide *Application of User Guidance*
The SCP implementation of the requirements of the Directive, ANNEX II “Requirements for certification-service-providers issuing qualified certificates”, literal (k), stipulates the signatory to follow the user guidance provided for the TOE.

R.Sigy_Name *Signatory’s name in the Qualified Certificate*
The CSP shall verify the identity of the person to which a qualified certificate is issued according to the Directive [1], ANNEX II “Requirements for certification-service-providers issuing qualified certificates”, literal (d). The CSP shall verify that this person holds the SSCD which implements the SCD corresponding to the SVD to be included in the qualified certificate.

R.SCA_Environment_Protection (12) *Trusted environment for the TOE and local user*
In case the VAD or DTBS is not transmitted via a cryptographically protected trusted path or channel, respectively, the environment of the TOE protects (a) the confidentiality and integrity of the VAD entered by the user via the SCA human interface provided and sent to the TOE and (b) the integrity of the DTBS sent by the SCA to the TOE.

(12) R.SCA_Environment_Protection is an additional security requirement (not defined by the PP)

R.Logging(15) *Usage of Logging file*
Stored informations in logging file have to be written correctly by the authorized persons.

R.Privacy(15) *Prevent accessing data*
The card holder has to deactivate sensitive data in the eHC if he wants to prevent health care providers from accessing data. He has to follow user guidance.

R.Trusted_Server(15) *Trusted server after Card to Card authentication*

The fact that key decipherment is possible after Card-To-Card authentication means, that the environment needs to provide additional means for the card holder, to prevent access to server data in case of a lost card, or in cases, where he doesn’t want to see a specific health professional to see specific data on a server. So an analogue to the activate/deactivate mechanism on the card may also be necessary on the server.

R.Closed_Environment(15) *Trusted environment for health professionals IT equipment*
Health professionals are allowed to access Electronic prescriptions in the card only in a closed environment, where attackers cannot access the data transmitted between eHC and the health professionals IT equipment.

R.Data_Protection(15) *Adequate Service usage*
In 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.
(15) : Additional security requirement (Not defined by the PP)

6. TOE SUMMARY SPECIFICATION

OBJECTIVES OF THE CHAPTER

The objective of this chapter is to furnish the definition of the instantiation of the security requirements for the TOE and provide a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

6.1 TOE SECURITY FUNCTIONS

This part covers the IT security functions and specifies how these functions satisfy the TOE security functional requirement with:
- the security function supplied by the IC (automatically) and utilized by the ES.,
- the security functions supplied by the ES.

6.1.1 TOE security functions list

Identification	Name	Supplied by
SF1	Operating State checking	IC
SF6	TSF self test	
SF7	Notification of physical attack	
SF_TSF_PROTECTION	Protection of the TSF	ES for the TOE
SF_CRYPTO	Cryptographic computation	
SF_AUTHENTICATION	Authentication management	
SF_ACCESS	Access control	
SF_CARD_INIT	Card Initialisation and Personalisation	

Table 14 – TOE security functions list

6.1.2 Security function provided by the IC

The security functions listed here after are shortly described in the IC Security Target [ST IC] and covered by the IC evaluation.

6.1.2.1 SF1- Operating state checking.

Correct function of the SLE66CX680PE is only given in the specified range. To prevent an attack exploiting those circumstances it is necessary to detect if the specified range is left (FPT_PHP.1- SSCD application).
All operating signals are filtered to prevent malfunction.
In addition the operating state is monitored with sensors for the operating voltage, clock signal, frequency, and temperature and electro magnetic radiation (FPT_PHP.3- SSCD application and eHC application). The TOE falls into the defined secure state in case of a specified range violation.

6.1.2.2 SF6- TSF self test

The TSF of the SLE66CX680PE has either a hardware controlled self test which can be started from the user software. The TSF shall provide detection of physical tampering (FPT_PHP.1- SSCD application) and shall resist to physical tampering scenarios (FPT_PHP.3- SSCD application and eHC application).

6.1.2.3 SF7- Notification of physical attack

The entire surface of the SLE66CX680PE is protected with the active shield. Attacks over the surface are detected when the shield lines are cut or get contacted (FPT_PHP.1- SSCD application and FPT_PHP.3- SSCD & eHC applications).

6.1.3 Security function provided by the ES

6.1.3.1 SF_TSF_PROTECTION

Protection of the TSF
This security function sets the TOE to a secure state before the normal operation of the TSF starts, even after an unexpected abortion of TSF execution and observes the correct behavior of the TSF.

During start-up and periodically during the normal operation a suite of tests are performed to verify the correct behavior of the underlying hardware:

- The environmental sensors of the hardware (clock, voltage, temperature, glitch, and irradiation) are checked for proper function by calling a test routine provided with the hardware (RMS) (FPT_AMT.1 – SSCD Application).
- The sensor signals of the Active Shield are checked explicitly by the ES, whereas the other sensors automatically stop the hardware on detection of an event ("security reset" managed by the IC).
- The software performs dummy operations and checks if the results are the expected ones (FPT_AMT.1, FPT_PHP.1– SSCD Application).

In case the "security reset" functionality of the hardware is broken by an attacker, a sensor event would result in an interrupt. The corresponding Interrupt Service Routines of the ES lead to a halt of the TOE.

If during the TSF execution unexpected behavior is detected, a secure state of the TOE will be preserved by completely halting the TOE execution (FPT_FLS.1 – SSCD & eHC applications). Then only a restart is possible, with setting a secure state as described above.

This SF verifies the integrity of the TSF data code patches (TSF executable code in EEPROM) and card life-cycle status during the start-up. Software RNG data are integrity checked every time they are accessed. On failing verification the TOE is blocked (FPT_TST.1, FDP_SDI.2 – SSCD & eHC applications).
Those TSF data can only be accessed internally, and therefore are separated from the user data (FPT_SEP.1 - eHC application).

The integrity of the user data stored in permanently in EEPROM or temporarily in RAM like D.SCD, D.RAD, D.SVD, RAD (eHC) (in particular the eGK-PINs PIN.CH, PIN.home, StatusPIN, PIN.QES), DTBS, and sensitive user data is checked every time when it is accessed (FDP_SDI.2 - SSCD & eHC applications, FPT_RVM.1 - eHC application). Integrity protection is provided by a checksum. In the case of an integrity error the use of this data is prohibited and the user will be informed by an error code.
The same mechanism applies to the access conditions, logically belonging to TSF internal data, which in this OS are stored in dedicated EFs of the files system.

The calls to all TSF functions are hard coded in the execution of the interface routines. Consequently they are executed unconditionally. This automatically ensures that the TSP enforcement functions cannot be bypassed (FPT_RVM.1 - eHC application).

When seeding the software random generator (exclusively done during initialisation phase) the hardware random generator used is checked for undisturbed operation.

In addition, this SF is responsible to store sensitive data, especially D.SCD, D.SVD, RAD and D.RAD, in a protected form: the data are masked so even in case an attacker (S.OFFCARD) succeeds in retrieving a memory dump those data are not available in plain. This hinders access to the plain data in case of a fraudulent memory dump. The mask is individual for the file in which the data are permanently stored. When copying to volatile memory (RAM) the data are kept in masked format, so they are never stored in plain text, except when this is absolutely necessary, e.g. directly before being used by some cryptographic operation (FMT_LIM.1, FMT_LIM.2 – eHC application).

6.1.3.2 SF_CRYPTO

Cryptographic computation

This security function provides the cryptographic procedures supported by the TOE.

The cryptographic algorithm 3TDES (FCS_CKM.1 - eHC application) is supported for a key length of 24 bytes (3 parts of 56 bits) with following modes:

- 3TDES in CBC mode for message confidentiality, and
- RetailMAC for message integrity.

Both are executed with message padding according [ISO-C4] 5.6.3.1 (“ISO-Padding”).

For usage in trusted channels 3TDES keys are temporarily generated by key negotiation algorithms (FCS_CKM.1/SM – eHC Application).

The basic DES operation is performed by the dedicated hardware. Allocated keys are deallocated as soon as they are not needed anymore, and their content is destroyed by explicitly calling a dedicated function.

The Hash algorithm SHA-256 is supported. (FCS_COP.1/HASH – eHC Application))

This SF can generate RSA key pairs for a given key length of 2048 bit. (FCS_CKM.1 - SSCD application). If this functionality is called with a reference to a key which was already generated previously, the operation is aborted (FCS_CKM.4 – SSCD & eHC applications).

SF_CRYPTO provides different signature algorithms based on RSA. The basic RSA operations are performed by a coprocessor of the underlying hardware. It is possible to use following signature schemes with a key length of 2048 bit for creating and verifying signatures:

- “ISO9796-2” scheme in the two modes DS1 and DS2.
- “PKCS#1” V1.5.
- “PKCS#1-PSS” (using SHA-256 in internal computations).

These algorithms are used in following functionalities:

- Signature generation, where the hash value can be
  - transmitted directly to the card in the PSO ComputeDigitalSignature command,
  - computed completely by the TOE beforehand via chained PSO Hash commands, or
  - computed partly by the TOE, where an external intermediate value and the last data block is transferred via a PSO Hash command.
- The verification of CV certificates according ISO 9796-2.
- Client/Server authentication according PKCS#1-PSS.
- Data en/deciphering with PKCS#1 V1.5 padding and RSA OAEP.

In the case of signature creation this SF imports the DTBS without associated security attributes (FDP_ITC – SSCD application). The integrity of D.DTBS is checked when it is accessed (FDP_SDI.2/DBTS – SSCD application).

This SF can be used to prove the correspondence of D.SCD and D.SVD by calculating the hash value of the SVD and calling the method FSP_CRY_CDS to compute the digital signature (FCS_COP.1/CORRESP). The user can verify this proof by verifying this signature.

Allocated keys, especially D.SCD, are deallocated as soon as they are not needed anymore, and their content is made unavailable upon the deallocation of the resource by explicitly calling a dedicated function (FDP_RIP.1 – SSCD & eHC applications).

This SF uses a permutational mechanism for the random number generation with a K4-DRNG (AIS 20), SOF-high, utilizing the hardware platform's TRNG evaluated as P2-class in [AIS31] frame (FCS_RND.1 – eHC application).

This SF ensures that from TOE emanations no access to SCD and D.RAD, RAD is possible by using the features of the underlying hardware and implementing own counter measures (FPT_EMSEC.1 – SSCD & eHC applications).

6.1.3.3 SF_AUTHENTICATION

This security function manages all authentication mechanisms provided by the TOE.
Card users are authenticated by presenting a PIN (VAD) which is compared with the corresponding RAD (FIA_ATD.1, FIA_UID.1, FIA UAU.1 – SSCD and eHC applications).
This SF uses a permutational mechanism for the Authentication of the users (PIN code) (FIA_UAU.4 – eHC applications).
There are two PINs dedicated for usage with eHC applications, and one dedicated for usage of the SSCD application, thereby separating the associated roles as follows:

PINs for eHC application:

A successful presentation of PIN.CH or PIN.home identifies and authenticates the Card Holder (i.e. sets the corresponding role), allowing to use functionalities of the eHC application in different environments (FMT_SMF.1 - eHC applications, FMT_SMR.1 – eHC applications): PIN.CH is used in environments of health service providers, PIN.home is used exclusively in private environment or at Self Service Terminals.
This SF ensures that both PINs (RAD (eHC)) are at least 6 digits long. In the case of 3 consecutive failed authentication attempts the corresponding PIN will be blocked.
In order to protect VAD (eHC) and RAD (eHC), temporarily copies of them are deleted after usage and counter measures are undertaken to avoid access to them via emanations of the TOE (FPT_EMSEC.1- eHC applications). The previous information content of presented and stored PIN values is made unavailable upon the deallocation of the resource. (FDP_RIP.1 – eHC applications)
If one of those PINs is blocked due to 3 consecutive failed authentication attempts, the Card holder is able to unblock it again by presenting a corresponding PUC, which will identify and authenticate him in this situation. The unblocking codes have a usage counter to limit the number of unblocking. A blocked unblocking code cannot be unblocked again (FIA_AFL.1 – eHC applications).

PIN for SSCD application:

A successful authentication with PIN.QES identifies and authenticates S.Signatory (i.e. sets the corresponding role) (FMT_MSA.2 – SSCD application).
Only S.Signatory is able to enable the signature-creation function (FMT_SMF.1 – SSCD application, FMT_SMR.1/SSCD – SSCD application) by replacing the transport PIN introduced during the personalisation phase by his own PIN (D.RAD). SF_AUTHENTICATION ensures this by asking for the correct D.VAD (FMT_MOF.1 – SSCD application, FMT_MSA.1 – SSCD application, FMT_MSA.2 – SSCD application, FMT_MTD.1 – SSCD application).
This SF ensures that the signatory PIN (D.RAD) is at least 6 digits long. In the case of 3 consecutive failed authentication attempts the corresponding PIN will be blocked.
After correct presentation of D.VAD, S.Signatory is able to execute the signature functionality for exactly one time. Afterwards he has to authenticate anew for a further execution.
In order to protect D.VAD and D.RAD, temporarily copies of them are deleted after usage and counter measures are undertaken to avoid access to them via emanations of the TOE (FPT_EMSEC.1- SSCD application). The previous information content of presented and stored PIN values is made unavailable upon the deallocation of the resource. (FDP_RIP.1 – SSCD application)
If PIN.QES is blocked due to 3 consecutive failed authentication attempts, S.Signatory is able to unblock it again by presenting a corresponding unblocking code, which will identify and authenticate him in this situation. The unblocking code has a usage counter to limit the number of unblocking attempts to 10. A blocked unblocking code cannot be unblocked again (FIA_AFL.1 – SSCD application).

SF_AUTHENTICATION also covers symmetric and asymmetric one-time cryptographic challenge-response protocols to identify and authenticate S.Admin, the Personalisation service provider, and following subjects in field operation, represented by trusted system components:

- Health Professional
- Medical Assistant
- Security Module Card
- Self Service Terminal
- Health insurance agency service provider
- Download service provider
- Combined services provider

These protocols are able to establish a trusted channel or a trusted path to secure the subsequent transactions (FTP_ITC.1/ACCESS RULES - Health application, FTP_ITC.1/DBTS Import – SSCD application, FTP_TRP.1/TOE – SSCD application).

With these different authentication mechanisms and secrets, the TSF is able to distinguish between the Signatory, the Card holder, the several trusted system components, and the Administrator.

The strength of the functions is SOF-high.

6.1.3.4 SF_ACCESS

Access control

This security function controls the access to data stored in the TOE and to the functionality provided by the TOE. This includes evaluation of access conditions as well as support for a “deactivated” state for records and files.

There are access conditions linked to the data stored in the TOE specifying the rules which have to be fulfilled to be authorized to request a TOE operation on this selected and perhaps additionally given data (FDP_ACC.2 – eHC application). If user data shall be read or overwritten by new ones this will be controlled by SF_ACCESS.

The access conditions fall under TSF internal data and are themselves protected by this access condition mechanism. To separate them from the user data, write or update access is forbidden without exception (FPT_SEP.1 - eHC application).

For signing D.DTBS it is required that the role is set to “S.Signatory” via entering PIN.QES, which is only possible after setting "SCD operational" to "yes" by replacing the “Transport RAD” with D.RAD (FIA_UAU.1, FIA_UID.1, FDP_ACC.1, FDP_ACF.1, FMT_MTD.1, FMT_MSA.2, FMT_SMF.1 – SSCD & eHC applications).

Modifying of D.RAD is only possible if the check of access conditions has been performed. The same holds for RAD (eHC) (i.e. PIN.CH and PIN.home) (FMT_SMF.1, FMT_MOF.1, FMT_MSA.1, FMT_MTD.1 – SSCD & eHC applications).

With the access conditions it can be specified which kind of protection is required for exchanged data.

SF_ACCESS for example controls if a user authentication is required before specific operations are allowed (FIA_ATD.1 – SSCD & eHC applications).
It is possible to establish a trusted path and a trusted channel before the user is authenticated. (FIA_UAU.1, FTP_TRP – SSCD application)

With the access conditions it can be required that authentication has to be performed and that data exchanged in external communication must be protected (FTP_ITC.1 – SSCD and eHC applications). This SF provides the functionality to ensure this protection by authenticity, integrity and confidentiality of the exchanged data (FDP_UCT.1 - eHC application, FDP_UIT.1, FIA_UAU.4 – SSCD & eHC application). The authenticity and integrity is ensured by adding a Message Authentication Code (MAC) to the data and the confidentiality is achieved by encrypting the exchanged data.

6.1.3.5 SF_CARD_INIT

Card Initialisation and Personalisation
This security function ensures the administration of the card during the phase initialisation (including SCD/SVD generation) and personalisation, and ensures the secure evolution of the TOE from the initialisation phase to the usage phase.
This SF also ensures the correct initialisation of the Software deterministic random generator (DRNG).
This SF controls the access to the data stored in the TOE and the functions provided by the TOE during the initialisation and personalisation phases. (FMT_MTD.1 – eHC application)
The SF identifies and authenticates S.Admin by verifying the entered password data (FIA_UAU.1-SSCD application). In the case of successful authentication “role” is set to “S.Admin” and “SCD/SVD management” to “authorize”. (FMT_MSA.1, FMT_MSA.2, FMT_SMF.1- SSCD & eHC application, FMT_SMR.1 – SSCD & eHC application)

It is ensured that only the administrator is able to import authentic EEPROM images (verifying authenticity and integrity of D.IMAGE), the SCD and to manage the SCD/SVD pair. (FDP_ACC.1, FDP_ACF.1, FIA_UAU.1, , FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1 - SSCD application)
The only possibility to load or generate a key again[7] is to perform a DELETE EEPROM and start initialisation and personalisation phase from the beginning. (FCS_CKM.4 – SSCD & eHC application)
This SF controls if an authentication of the administrator is required for specific TOE operations like calling interfaces or modifying security attributes. This SF also has the ability to restart from the initialisation phase.

At the end of the productions phases this SF brings the TOE irreversibly into user phase, and the functionalities of SF_CARD_INIT as no longer available.

6.2 ASSURANCE MEASURES

This chapter defines the list of the assurance measures required for the TOE security assurance requirements.

Assurance measures list

Measure	Name
AM_ACM	Configuration management, reference ACM01R10559
AM_ADO	Delivery and Operation, reference ADO01R10559
AM_ADV	Development, reference ADV01R10559
AM_AGD	Guidance documents, reference AGD01R10559
AM_ALC	Life cycle, reference ALC01R10559
AM_ATE	Tests, reference ATE01R10559
AM_AVA	Vulnerability assessment, reference AVA01R10559

Table 15 – Assurance measures

6.2.1 AM_ACM: Configuration management

This assurance measure ensures the configuration management. The CM responsible is in charge to write the CM plan, use the CM system and validate the CM system in order to confirm that ACM_XXX.Y components are completed.

6.2.2 AM_ADO: Delivery and Operation

This assurance measure ensures the delivery and operation. The delivery responsible is in charge to write delivery documentation and validate it in order to confirm that the procedure is applied.

6.2.3 AM_ADV: Development

This assurance measure ensures the development. The development responsible is in charge to design the TOE, write development documentation and validate it in order to confirm that the related security functional requirements are completed by security functions.

6.2.4 AM_AGD: Guidance documents

This assurance measure ensures the guidance documents. The guidance responsible is in charge to write administrator and user guidance. The documentation provides the rules to use and administrate the TOE in a secured manner.

6.2.5 AM_ALC: Life cycle

This assurance measure ensures the life cycle. Life cycle responsible is in charge to confirm that the life cycle process is applied.

6.2.6 AM_ATE: Tests

This assurance measure ensures the tests. The test responsible is in charge to write tests and execute it in order to confirm that the security functions are tested.

6.2.7 AM_AVA: Vulnerability assessment

This assurance measure ensures the vulnerability assessment. The security responsible is in charge to confirm that the security measures are suitable to meet the TOE security objectives conducing a vulnerability analysis.

7. PP CLAIMS

OBJECTIVES OF THE CHAPTER

The objective of this chapter is to furnish an optional claiming that the TOE conforms with the requirements of one, or more than one, PP.

This security target is based to the Protection Profiles “Secure Signature Creation Devices” Type 3 [PP SSCD3] . The PP “Secure Signature-Creation device” Type 3 [PP SSCD 3] (listed as BSI-PP-0006-2002) is certified at the German Certification Body

This security target is conform to “Electronic Health Card (eHC)” Protection Profile rev 2.60 29/07/2008 BSI-PP-0020 which defines the security objectives and requirements for the electronic Health Card (German: “elektronische Gesundheitskarte”).

7.1 PP ADDITION

	Addition in ST	**Not defined by the PP**
Assets	-	
Threats	X	**T.EEPROM**
Assumptions	-	
Organizational Security Policies	-	
Security objectives for the TOE	X	**OT.EEPROM**
Security objectives for the operational environment	-	
Security functional requirements	-	
security assurance requirements	-	
Security Requirements for the IT Environment	X	**FDP_ACC.2.1/Data Protection , FDP_ACC.2.2/Data Protection , FDP_ACF.1.1/ Data Protection , FDP_UIT.1.1/ Data Protection, FDP_UIT.1.2/ Data Protection, FIA_UID.1.1/Data Protection, FIA_UID.1.2 /Data Protection, FMT_MTD.1.1/ Perso Data, FMT_MTD.3.1/ Perso Data, FMT_SMF.1.1/ Perso Data, FMT_SMR.1.1/ Perso Data, FMT_SMR.1.2/ Perso Data, FTP_ITC.1.1 /Data protection, FTP_ITC.1.2 / Data protection, FTP_TRP.1.1 / Data protection, FTP_TRP.1.2 / Data protection.**
Security Requirements for the Non IT Environment	X	**R.SCA_Environment_Protection, R.Logging, R.Privacy, R.Trusted_Server, R.Closed_Environment, R.Data_Protection.**

7.2 PP REFINEMENT

The following functional requirements found in PPs are refined for the TOE .

Identification	Iteration	Assignment	Selection	Refinement
FCS_CKM.1.1/.SM		X		
FCS_CKM.1.1/GENKEY		X		
FCS_CKM.4.1		X		
FCS_COP.1.1/HASH		X		
FCS_COP.1.1/CCA_SIGN		X		
FCS_COP.1.1/CCA_VERIF		X		
FCS_COP.1.1/CSA		X		
FCS_COP.1.1/ASYM_DEC		X		
FCS_COP.1.1/SYM		X		
FCS_COP.1.1/MAC		X		
FCS_COP.1.1/CORRESP		X		
FCS_COP.1.1/SIGNING		X		
FCS_RND.1[14]		X		
FDP_ACC.1.1/SVD TRANSFER SFP		X		
FDP_ACC.1.1/INITIALISATION		X		
FDP_ACC.1.1/PERSONALISATION SFP		X		
FDP_ACC.1.1/SIGNATURE-CREATION SFP		X		
FDP_ACC.1.1/EEPROM SFP		X		
FDP_ACC.2.1		X		
FDP_ACC.2.2				
FDP_ACF.1.1/ACCESS RULES		X		
FDP_ACF.1.2/ACCESS RULES		X		
FDP_ACF.1.3/ACCESS RULES		X		
FDP_ACF.1.4/ACCESS RULES		X		
FDP_ACF.1.1/INITIALISATION SFP		X		
FDP_ACF.1.2/INITIALISATION SFP		X		
FDP_ACF.1.3/INITIALISATION SFP		X		
FDP_ACF.1.4/INITIALISATION SFP		X		
FDP_ACF.1.1/SVD TRANSFER SFP		X		
FDP_ACF.1.2/SVD TRANSFER SFP		X		
FDP_ACF.1.3/SVD TRANSFER SFP		X		
FDP_ACF.1.4/SVD TRANSFER SFP		X		
FDP_ACF.1.1/PERSONALISATION SFP		X		
FDP_ACF.1.2/PERSONALISATION SFP		X		
FDP_ACF.1.3/PERSONALISATION SFP		X		
FDP_ACF.1.4/PERSONALISATION SFP		X		
FDP_ACF.1.1/SIGNATURE CREATION SFP		X		

Identification	Iteration	Assignment	Selection	Refinement
FDP_ACF.1.2/SIGNATURE CREATION SFP		X		
FDP_ACF.1.3/SIGNATURE CREATION SFP		X		
FDP_ACF.1.4/SIGNATURE CREATION SFP		X		X
FDP_ACF.1.1/EEPROM SFP		X		
FDP_ACF.1.2/EEPROM SFP		X		
FDP_ACF.1.3/EEPROM SFP		X		
FDP_ACF.1.4/EEPROM SFP		X		
FDP_ETC.1.1/SVD TRANSFER		X		
FDP_ETC.1.2/SVD TRANSFER				
FDP_ITC.1.1/DBTS		X		
FDP_ITC.1.2/DBTS				
FDP_ITC.1.3/DBTS		X		X
FDP_RIP.1.1/HEALTH_OBJ		X	X	
FDP_RIP.1.1/SSCD_OBJ		X	X	
FDP_SDI.2.1/Persistent		X		
FDP_SDI.2.2/Persistent		X		
FDP_SDI.2.1/Volatile		X		
FDP_SDI.2.2/Volatile		X		
FDP_SDI.2.1/DBTS		X		
FDP_SDI.2.2/DBTS		X		
FDP_UCT.1		X	X	
FDP_UIT.1.1/ACCESS RULES		X	X	
FDP_UIT.1.2/ACCESS RULES			X	
FDP_UIT.1.1/SVD Transfer		X	X	
FDP_UIT.1.2/SVD Transfer			X	
FDP_UIT.1.1/TOE DBTS		X	X	
FDP_UIT.1.2/TOE DBTS			X	
FIA_AFL.1.1/PIN		X		
FIA_AFL.1.2/PIN		X		
FIA_AFL.1.1/PUC		X		
FIA_AFL.1.2/PUC		X		
FIA_AFL.1.1/D.RAD		X		
FIA_AFL.1.2/D.RAD		X		
FIA_AFL.1.1/PUK		X		
FIA_AFL.1.2/PUK		X		
FIA_ATD.1.1		X		
FIA_ATD.1.1/D.RAD		X		
FIA_UAU.1 .1/HEALTH		X		
FIA_UAU.1 .2/HEALTH		X		
FIA_UAU.1 .1		X		
FIA_UAU.1 .2				
FIA_UAU.4.1		X		
FIA_UID.1.1/HEALTH		X		
FIA_UID.1.2/HEALTH				
FIA_UID.1.1		X		
FIA_UID.1.2				
FMT_LIM.1.1[(14)]		X		
FMT_LIM.2.1[(14)]		X		
FMT_MTD.1.1/ini		X	X	
FMT_MTD.1.1/pers		X	X	
FMT_MTD.1.1/CMS		X	X	
FMT_MTD.1.1/PIN		X	X	
FMT_MTD.1.1/KEY_MOD		X	X	
FMT_MTD.1.1/D.RAD		X	X	

Identification	Iteration	Assignment	Selection	Refinement
FMT_MOF.1.1		X	X	
FMT_MSA.1.1/Administrator		X	X	
FMT_MSA.1.1/Signatory		X	X	
FMT_MSA.2.1				
FMT_MSA.3 .1		X	X	X
FMT_MSA.3 .2		X	X	
FMT_MSA.3 .1/ EEPROM		X	X	X
FMT_MSA.3 .2/ EEPROM		X	X	
FMT_SMF.1.1/HEALTH		X		
FMT_SMF.1.1/SSCD		X		
FMT_SMR.1.1/HEALTH		X		
FMT_SMR.1.2/HEALTH				
FMT_SMR.1.1/SSCD		X		
FMT_SMR.1.2/SSCD				
FPT_AMT.1.1		X	X	
FPT_EMSEC.1.1[14]		X		
FPT_EMSEC.1.2[14]		X		
FPT_EMSEC.1.2/S.OFFCARD[14]		X		
FPT_FLS.1.1		X		
FPT_PHP.1.1				
FPT_PHP.1.2				
FPT_PHP.3.1		X		X
FPT.RVM.1.1				
FPT_SEP.1.1				
FPT_SEP.1.2				
FPT_TST.1.1		X	X	
FPT_TST.1.2		X	X	
FPT_TST.1.3				
FTP_ITC.1.1/ACCESS RULES				
FTP_ITC.1.2/ACCESS RULES			X	
FTP_ITC.1.3/ACCESS RULES		X		
FTP_ITC.1.1/SVD TRANSFER				
FTP_ITC.1.2/SVD TRANSFER			X	
FTP_ITC.1.3/SVD TRANSFER		X		
FTP_ITC.1.1/DBTS IMPORT				
FTP_ITC.1.2/DBTS IMPORT			X	
FTP_ITC.1.3/DBTS IMPORT		X		
FTP_TRP.1.1/TOE			X	
FTP_TRP.1.2/TOE			X	
FTP_TRP.1.3/TOE		X		

Table 16 – Mapping of the performed operations and the TOE security functional requirements

[14] This requirement is an extension to [CCPART2].

7.3 PP REFINEMENT FOR IT ENVIRONMENT

The following functional requirements found in the based PP are refined for the IT environment .

Identification	Iteration	Assignment	Selection	Refinement
FCS_COP.1	X	X		
FCS_CKM.2		X		
FCS_CKM.3		X		
FDP_UIT.1		X	X	
FTP_ITC.1	X	X	X	X
FTP_TRP.1		X	X	
FDP_ACC.2		X		
FDP_ACF.1		X		
FDP_UIT.1		X	X	
FIA_UID.1		X		
FMT_MTD.1		X	X	
FMT_MTD.3				
FMT_SMF.1		X		
FMT_SMR.1		X		
FTP_ITC.1			X	
FTP_TRP.1			X	

Table 17 – Mapping of the performed operations and the IT environment security functional requirements

8. RATIONALE

OBJECTIVES OF THE CHAPTER

The objective of this chapter is to furnish the evidence to be used for the ST evaluation and supporting the claims that the ST is a complete and cohesive set of requirements, that a conformant TOE would provide an effective set of IT security countermeasures within the security environment, that the TOE summary specification leveling the requirements and that any PP conformance claims are valid.

8.1 TOE SECURITY OBJECTIVES RATIONALE

The purpose of this chapter is to demonstrate the coverage of threats, assumptions and organizational security policies by the security objectives defined in the **chapter 3**.

8.1.1 Assets coverage

The following table shows the correspondence between threats and assets.

Threats / Assets	Card Authentication Private Key	Card Verifiable Authentication Certificate	Client-Server Authentication Private Key	Decipher Private Key	D.DTBS	D.IMAGE	Display message	D.SCD	D.SIGN_APPLI	D.SIGNATURE	D.SVD	D.RAD	D.VAD	Emergency data	Electronic prescription	Initialisation data	Logging data	Medical data	Permission data	Personal and health insurance data (open)	Personal and health insurance data (protected)	Personalisation data	Public Key for CV Certification Verification	Secret Keys for interaction with the “download service provider”	Secret Keys for interaction with the “health insurance agency service provider”insurance agency service provider”	RAD (eHC)	VAD (eHC)	X.509 certificates
T.Abuse_Func																X						X						
T.Compromise_Internal_Data							X							X	X	X	X	X	X	X	X	X				X		
T.DTBS_Forgery					x																							
T.EEPROM						x																						
T.Forge_Internal_Data							X							X	X	X	X	X	X	X	X	X				X		
T.Hack_Phys								x	x		x	x	x															
T.Information_Leakage	X		X	X			X																X	X	X	X		
T.Intercept							X							X	X	X	X	X	X	X	X	X						
T.Malfunction																										X	X	
T.Misuse							X							X	X	X	X	X	X	X	X	X					X	
T.Phys_Tamper	X		X	X			X																X	X	X	X	X	
T.SCD_DERIVE								x																				
T.SCD_Divulg								x																				
T.SigF_Misuse									x				x															
T.Sig_Forgery										x																		
T.Sig_Repud										x																		
T.SVD_Forgery											x																	

Table 18 – Threats / Assets correspondence analysis

8.1.2 Security objectives coverage

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Cryptography	OT.Datas_Secrecy	OT.DTBS_Integrity_TOE	OT.EEPROM	OT.EMSEC_Design	OT.Init	OT.Lifecycle_Security	OT.SCD_SVD_Corresp	OT.SCD_Unique	OT.Services	OT.Sig_Secure	OT.Sigy_SigF	OT.SVD_Auth_TOE	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Tamper_ID	OT.Tamper_Resistance		OD.Assurance	OD.Material		OE.CGA_Qcert	OE.Data_Protection	OE.HI_VAD	OE.Legal_Decisions	OE.Perso	OE.SVD_Auth_CGA	OE.SCA_Data_Intend	OE.Users	OE.User_Information
A.CGA																											x					x			
A.Perso																															X				
A.SCA																																	x		
A.Users																																		X	
OSP.Additional_Applications			X																												X				
OSP.eHC_Spec	X	X	X	X									X																						
OSP.Electronic_Prescriptions		X																										X		X					
OSP.Legal_Decisions																														X					
OSP.Logging		X											X																	X					
OSP.Manufact																								X	X										
OSP.Services													X																						
OSP.User_Information																																			X
T.Abuse_Func																	X																		
T.Compromise_Internal_Data	X	X		X									X															X		X					
T.DTBS_Forgery						x																											x		
T.EEPROM							x																												
T.Forge_Internal_Data	X	X		X									X															X		X					
T.Hack_Phys					x			x													x	x													
T.Information_Leakage																		X																	

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Cryptography	OT.Datas_Secrecy	OT.DTBS_Integrity_TOE	OT.EEPROM	OT.EMSEC_Design	OT.Init	OT.Lifecycle_Security	OT.SCD_SVD_Corresp	OT.SCD_Unique	OT.Services	OT.Sig_Secure	OT.Sigy_SigF	OT.SVD_Auth_TOE	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Tamper_ID	OT.Tamper_Resistance	OD.Assurance	OD.Material		OE.CGA_Qcert	OE.Data_Protection	OE.HI_VAD	OE.Legal_Decisions	OE.Perso	OE.SVD_Auth_CGA	OE.SCA_Data_Intend	OE.Users	OE.User_Information
T.Intercept	X	X		X									X														X		X					
T.Malfunction																				X														
T.Misuse	X	X		X									X														X		X					
T.Phys Tamper																			X															
T.SCD_Derive												x		x																				
T.SCD_Divulg					x																													
T.SigF_Misuse						x									x													x				x		
T.Sig_Forgery					x			x		x	x			x		x					x	x				x					x	x		
T.Sig_Repud					x	x		x		x	x	x		x	x	x					x	x				x					x	x		
T.SVD_Forgery																x															x			
P.CSP_Qcert											x															x								
P.Qsign														x	x											x						x		
P.Sigy_SSCD									X			x			x																			

Table 19 – Security objectives / Threats-Assumptions-Policies correspondence analysis

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 spec], 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 personalisation” (the latter together with OT.AC_Pers “Access control for personalisation” protecting the personalisation functions of the TOE) ensure that the Personalisation service provider will provide a genuine TOE initialized and personalized according to the specification to the Card holder.

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” Table **14** – Rules summarize).
- 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 authorized users to write logging data into the card.
- According to OE.Legal_Decision   uthorizedorised 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 (card holder, health professional, etc.) the authenticity of which is made sure by services required by OT.Services (f.i. Service_User_Auth_PIN, Service_Sym_Mut_Auth_with_SM, Service_Asym_Mut_Auth_with_SM, cf. 3.4**.** chapter). The support by OT.Cryptography is needed since several services required by OT.Services rely on cryptographic mechanisms required by OT.Cryptography (f.i. a symmetric encryption algorithm is needed for Service_Sym_Mut_Auth_with_SM, an asymmetric algorithm for Service_Asym_Mut_Auth_with_SM).

- OT.AC_Pers protects the personalisation 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 initialisation and the personalisation of the TOE and which must not be accessible after TOE delivery.

The security objective 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 objective for the environment OE.Perso “Secure personalisation” implements the assumption **A.Perso** “Personalisation of the Smart Card”.

T.Hack_Phys (Exploitation of vulnerabilities in the physical environment) which is a generic threat deals with physical attacks exploiting vulnerabilities in the environment of the TOE. OT.Datas_Secrecy preserves the secrecy of the datas including D.SCD. Physical attacks through the TOE interfaces are countered by OT.EMSEC_Design. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tamper attacks on the IC.

T.SCD_Divulg (Storing, copying, and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [1], recital (18). This threat is countered by OT.Datas_Secrecy which assures the secrecy of the datas including the SCD used for signature generation.

T.SCD_Derive (Derive the signature-creation data) deals with attacks on the SCD via public known data produced by the TOE. This threat is countered by OT.SCD_Unique that provides cryptographic secure generation of the SCD/SVD-pair. OT.Sig_Secure ensures cryptographic secure electronic signatures.

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

T.SigF_Misuse (Misuse of the signature-creation function of the TOE) addresses the threat of misuse of the TOE signature-creation function to create SDO by others than the signatory for data the signatory has not decided to sign as required by the Directive [1], Annex III, paragraph 1, literal I. This threat is addressed by the OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OE.SCA_Data_Intend (Data intended to be signed), and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity), and OE.HI_VAD (Protection of the VAD) as follows: OT.Sigy_SigF ensures that the TOE provides the signature-generation function for the legitimate signatory only. OE.SCA_Data_Intend ensures that the SCA sends the DTBS-representation only for data the signatory intends to sign. The combination of OT.DTBS_Integrity_TOE and OE.SCA_Data_Intend counters the misuse of the signature generation function by means of manipulation of the channel between the SCA and the TOE. If the SCA provides the human interface for the user authentication, OE.HI_VAD provides confidentiality and integrity of the VAD as needed by the authentication method employed.

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. This threat is in general addressed by OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OE.CGa_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.Datas_Secrecy (Secrecy of datas), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance) and OT.Lifecycle_Security (Lifecycle security), as follows:
OT.Sig_Secure ensures by means of robust encryption techniques that the signed data and the electronic signature are securely linked together. OE.SCA_Data_Intend provides that the methods used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation is appropriate for the cryptographic methods employed to generate the electronic signature. The combination of OE.CGa_QCert, OT.SCD_SVD_Corresp,OT.SVD_Auth_TOE, and OE.SVD_Auth_CGA provides the integrity and authenticity of the SVD that is used by the signature verification process. OT.Sig_Secure, OT.Datas_Secrecy, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

T.Sig_Repud (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGa_QCert **(**Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique **)** (Uniqueness of the signature-creation data), OT.datas_Secrecy (Secrecy of datas), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity).
OE.CGa_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGa_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. OE.CGa_QCert and OT.SCD_SVD_Correspensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OT.SCD_Unique provides that the signatory's SCD can practically

occur just once. OT.Sig_Secure, OT.Datas_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD. OT.Sigy_SigF provides that only the signatory may use the TOE for signature generation. OT.Sig_Secure ensures by means of robust cryptographic techniques that valid electronic signatures may only be generated by employing the SCD corresponding to the SVD that is used for signature verification and only for the signed data. OE.SCA_Data_Intend and OT.DTBS_Integrity_TOE ensure that the TOE generates electronic signatures only for DTBS-representations which the signatory has decided to sign as DTBS.

T.SVD_Forgery (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.SVD_Auth_TOE which ensures that the TOE provide means to enable CGA to verify the authenticity SVD exported by the TOE, as well as by OE.SVD_Auth_CGA which provides verification of SVD authenticity by the CGA.

T.EEPROM (Forgery of the signature-verification data) deals with the forgery of the EEPROM image loaded by the TOE during the initialisation and personalisation phases. T.EEPROM is addressed by OT.EEPROM which ensures that only authentic and integer EEPROM image is loaded into the TOE.

A.CGA (Trustworthy certification-generation application) establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGa_QCert (Generation of qualified certificates) which ensures the generation of qualified certificates and by OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) which ensures the verification of the integrity of the received SVD and the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

A.SCA (Trustworthy signature-creation application) establishes the trustworthiness of the SCA according to the generation of DTBS-representation. This is addressed by OE.SCA_Data_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS-representation of the data that has been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

P.CSp_QCert (CSP generates qualified certificates) establishes the qualified certificate for the signatory and provides that the SVD matches the SCD that is implemented in the SSCD under sole control of this signatory. P.CSp_QCert is addressed by the TOE by OT.SCD_SVD_Corresp concerning the correspondence between the SVD and the SCD, in the TOE IT environment, by OE.CGa_QCert for generation of qualified certificates by the CGA, respectively.

p.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with qualified electronic signatures, as defined by the Directive [1], article 5, paragraph 1. Directive [1], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The requirement of qualified electronic signatures being based on qualified certificates is addressed by OE.CGa_QCert. OE.SCA_Data_Intend provides that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. OT.Sig_Secure and OT.Sigy_SigF address the generation of advanced signatures by the TOE.

P.Sigy_SSCD (TOE as secure signature-creation device) establishes the TOE as secure signature-creation device of the signatory with practically unique SCD. This is addressed by OT.Sigy_SigF ensuring that the SCD is under sole control of the signatory and OT.SCD_Unique ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. OT.Init and provide that generation of the SCD/SVD pair is restricted to authorised users.

8.2 TOE SECURITY REQUIREMENTS RATIONALE

The purpose of this chapter is to demonstrate the coverage of security objectives by the security requirements defined in the **chapter 5.**

8.2.1 Choice of TOE security functional requirements

This protection profile uses components defined as extensions to CC part 2.

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.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.

FMT_LIM

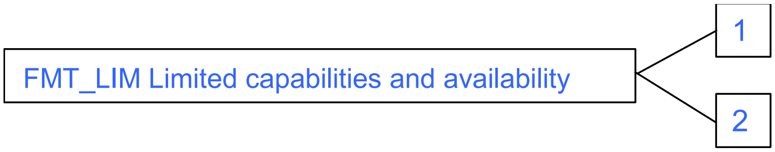
The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

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

Component levelling:



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

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

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

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.

FPT_EMSEC TOE Emanation

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

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC.1 TOE emanation has two constituents:

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

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

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

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

Dependencies: No other components.

8.2.2 Choice of TOE security assurance requirements

The choice of assurance requirements is based on the analysis of the security objectives for the TOE and on functional requirements defined to meet these objectives.

The assurance level is **EAL4** augmented on **ADV_IMP.2 (Implementation representation - Implementation of the TSF)**, **AVA_MSU.3 (Misuse - Analysis and testing for insecure states)** and **AVA_VLA.4 (Vulnerability Analysis - Highly resistant).**

Evaluation Assurance Level rationale
EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products which can be applied to moderate to high security functions. Smart cards are just such a product.

Assurance augmentation rationale
Additional assurance requirements are also required due to the definition of the TOE.
The TOE is intended to function in a variety of signature generation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

In **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 by the evaluator. 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.

AVA_VLA.4 Vulnerability Asses–me–t - Vulnerability Analysis – Highly resistant
The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.EMSEC_Design, OT.Datas_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. 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

OT.EMSEC_Design doesn't imply the need for additional documentary evidence.
All of these are met or exceeded in the EAL4 assurance package.

ADV.IMP.2 provides a higher assurance for the implementation of the TOE especially for the absence of unintended functionality
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.

8.2.3 TOE security functional requirements rationale

8.2.3.1 Cross table correspondence

The following table gives the relationship between the environment security requirements and the environment security objectives.

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Cryptography	OT.Datas_Secrecy	OT.DTBS_Integrity_TOE	OT.EEPROM	OT.EMSEC_Design	OT.INIT	OT.Lifecycle_Securit	OT.SCD_SVD_Corresp	OT.SCD_UNIQUE	OT.Services	OT.Sig_Secure	OT.Sigy_SigF	OT.SVD_Auth_TOE	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.1/SM				X									X									
FCS_CKM.1/GENKEY					X						X	X										
FCS_CKM.4				X	X					X			X									
FCS_COP.1/HASH				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/ASYM_DEC				X									X									
FCS_COP.1/SYM				X		X				X			X									
FCS_COP.1/MAC				X									X									
FCS_COP.1/CORRESP											X											
FCS_COP.1/SIGNING														X								
FCS_RND.1				X									X									
FDP_ACC.1/SVD TRANSFER SFP																X						
FDP_ACC.1/INITIALISATION SFP					X				X													
FDP_ACC.1/PERSONALISATION SFP															X							
FDP_ACC.1/SIGNATURE-CREATION SFP						X									X							
FDP_ACC.1//EEPROM SFP							X															
FDP_ACC.2		X											X									
FDP_ACF.1/ACCESS RULES		X											X									
FDP_ACF.1/INITIALISATION SFP					X				X													
FDP_ACF.1/SVD TRANSFER SFP																X						
FDP_ACF.1/PERSONALISATION SFP															X							
FDP_ACF.1/SIGNATURE-CREATION SFP						X									X							
FDP_ACF.1//EEPROM SFP							X															
FDP_ETC.1/SVD TRANSFER																X						
FDP_ITC.1/DTBS						X																
FDP_RIP.1/HEALTH_OBJ		X	X																			

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Cryptography	OT.Datas_Secrecy	OT.DTBS_Integrity_TOE	OT.EEPROM	OT.EMSEC_Design	OT.INIT	OT.Lifecycle_Securit	OT.SCD_SVD_Corresp	OT.SCD_UNIQUE	OT.Services	OT.Sig_Secure	OT.Sigy_SigF	OT.SVD_Auth_TOE	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Tamper_ID	OT.Tamper_Resistance
FDP_RIP.1/SSCD_OBJ					X										X							
FDP_SDI.2/Persistent		X			X						X			X	X							
FDP_SDI.2/Volatile		X																				
FDP_SDI.2/DTBS						X																
FDP_UCT.1		X											X									
FDP_UIT.1/ACCESS RULES		X											X									
FDP_UIT.1/SVD TRANSFER																X						
FDP_UIT.1/TOE DTBS						X																
FIA_AFL.1/PIN		X											X									
FIA_AFL.1/PUC		X											X									
FIA_AFL.1/D.RAD									X						X							
FIA_AFL.1/PUK															X							
FIA_ATD.1		X											X									
FIA_ATD.1/D.RAD									X						X							
FIA_UID.1/ HEALTH	X	X											X									
FIA_UID.1									X						X							
FIA_UAU.1/HEALTH	X	X											X									
FIA_UAU.1									X						X							
FIA_UAU.4													X									
FMT_LIM.1		X	X														X					
FMT_LIM.2		X	X														X					
FMT_MOF.1					X										X							
FMT_MSA.1/ADMINISTRATOR					X		X		X													
FMT_MSA.1/SIGNATORY					X										X							
FMT_MSA.2															X							
FMT_MSA.3/					X				X						X							
FMT_MSA.3/EEPROM							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									
FMT_MTD.1/D.RAD															X							
FMT_SMF.1/HEALTH	X	X	X										X									
FMT_SMF.1/SSCD					X		X		X						X							
FMT_SMR.1/HEALTH	X	X	X										X									
FMT_SMR.1/SSCD					X										X							
FPT_AMT.1					X					X				X								
FPT_EMSEC.1.1								X										X				

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Cryptography	OT.Datas_Secrecy	OT.DTBS_Integrity_TOE	OT.EEPROM	OT.EMSEC_Design	OT.INIT	OT.Lifecycle_Securit	OT.SCD_SVD_Corresp	OT.SCD_UNIQUE	OT.Services	OT.Sig_Secure	OT.Sigy_SigF	OT.SVD_Auth_TOE	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Tamper_ID	OT.Tamper_Resistance
FPT_EMSEC.1.2																		X				
FPT_EMSEC.1.2/S.OFFCARD								x														
FPT_FLS.1					X													X		X		
FPT_PHP.1																					X	
FPT_PHP.3																		X	X	X		X
FPT_TST.1										X				X				X		X		
FPT_RVM.1		X	X														X	X		X		
FPT_SEP.1		X	X														X	X		X		
FTP_ITC.1/ACCESS RULES		X											X									
FTP_ITC.1/SVD TRANSFER																X						
FTP_ITC.1/DTBS IMPORT						X																
FTP_TRP.1/TOE															X							

Table 20 – Coverage of TOE security objectives by security functional requirements

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

- the SFR FMT_SMR.1/HEALTH defines the Personaliser as known role of the TOE and the SFR FMT_SMF.1/HEALTH defines personalisation as security management function,
- the SFR FIA_UID.1/ HEALTH and FIA_UAU.1/ HEALTH require identification and authentication as necessary precondition for the personalisation (i.e. this TSF mediated function is not allowed before the user is identified and successfully authenticated),
- the SFR FMT_MTD.1/Pers limit right to write Personalisation data to the Personalisation service provider and
- 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

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

and supported by :

- SFRs FIA_AFL.1/PIN, FIA_AFL.1/PUC, FIA_ATD.1, FMT_SMF.1/HEALTH, FMT_SMR.1/HEALTH, FMT_MTD/PIN, which all support the security of the Card holders eHC-PIN and PUC.
- SFRs FIA_UID.1/ HEALTH and FIA_UAU.1/ HEALTH, which support timing of Identification and authentication,

- SFRs FDP_RIP.1/HEALTH_OBJ, FDP_SDI.2/Persistent and FDP_SDI.2/Volatile (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.

- the SFRs FDP_UCT.1, FDP_UIT.1/ ACCESS RULES and FTP_ITC.1/ACCESS RULES 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.

- 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.

- 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

- FMT_MTD.1/CMS, which restricts download of additional applications to the Download service provider (as also required by SFP_access_rules).

- The other SFRs on management functions FMT_SMF.1/HEALTH, FMT_SMR.1/HEALTH, 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

- A more “low level” support is given by FPT_SEP.1, FPT_RVM.1 and FDP_RIP.1/HEALTH_OBJ, 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.)

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:

- 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/HASH, FCS_RND.1 and FIA_UAU.4.

- 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/HASH, FCS_RND.1, FCS_COP.1/SYM, 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/ ACCESS RULES and FTP_ITC.1/ACCESS RULES.

- 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/SYM, 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/ ACCESS RULES and FTP_ITC.1/ACCESS RULES.

- the TOE security services **Service_User_Auth_PIN** and **Service_User_Auth_PUC** are implemented by the SFRs FIA_AFL.1/PIN, FIA_AFL.1/PUC, FIA_ATD.1, FMT_SMF.1/HEALTH, FMT_SMR.1/HEALTH, FMT_MTD/PIN, which all support the security of the Card holders eHC-PIN and PUC. Also it is supported by FDP_ACC.2 and FDP_ACF.1/ACCESS RULES, because these SRFs require implementation of SFP_access_rules, which involves PIN authentication.

- the TOE security service **Service_Privacy** is implemented mainly by the SFRs FDP_ACC.2 and FDP_ACF.1/ACCESS RULES, 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).

- the TOE security service **Service_Client_Server_Auth** is implemented by the SFR FCS_COP.1/CSA
- the TOE security service **Service_Data_Decryption** is implemented by the SFR FCS_COP.1/ASYM_DEC.
- 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.
- 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/ACCESS RULES (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/ACCESS RULES, 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 symmetric algorithms as used for secure messaging, hash functions, asymmetric algorithms and random number generation.

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

- The SFR FPT_EMSEC.1 protects user data and TSF data against information leakage through side channels.
- 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.
- The SFR FPT_PHP.3 resists physical manipulation of the TOE hardware to enforce information leakage e.g. by deactivation of countermeasures or changing the operational characteristics of the hardware.
- The 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:

- 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.
- The SFR FPT_RVM.1 and FPT_SEP.1 ensure that the TSF detecting errors or insecure operational can not by bypassed or corrupted.
- 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:

- The SFR FMT_LIM.1 and FMT_LIM.2 prevent the misuse of TOE functions intended for the testing, the initialisation and the personalisation of the TOE in the operational phase of the TOE,
- The SFR FPT_RVM.1 and FPT_SEP.1 ensure that the protection of TOE functions intended for the testing, the initialisation and the personalisation of the TOE can not by bypassed or corrupted.

OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by FPT_EMSEC.1.1 and FPT_EMSEC.1.2/S.OFFCARD.

OT.Init (SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication. FIA_ATD.1/D.RAD defines RAD as the corresponding user attribute. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The attributes of the authenticated user are provided by FMT_MSA.1/ADMINISTRATOR and FMT_MSA.3 for static attribute initialisation. Access control is provided by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1/D.RAD. The security management function is provided by FMT_SMF.1/SSCD (ability to modify).

OT.Lifecycle_Security (Lifecycle security) is provided by the security assurance requirements ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ADO_DEL.2, and ADO_IGS.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functions FPT_TST.1 and FPT_AMT.1 provide failure detection throughout the lifecycle. FCS_CKM.4 provides secure destruction of the SCD. Authenticity and integrity failure detection is ensured by FCS_COP.1/SYM.

OT.Datas_Secrecy (Secrecy of datas) counters that storage or copying of secrets including the SCD causes a threat to the legal validity of electronic signatures. OT.Datas_Secrecy is provided by the security functions specified by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP that ensure that only authorised user can initialise the TOE and create the SCD. The authentication and access management functions specified by FMT_MOF.1, FMT_MSA.1/ADMINISTRATOR, FMT_MSA.1/SIGNATORY, FMT_SMF.1/SSCD, FMT_MSA.3, and FMT_SMR.1/SSCD ensure that only the signatory or administrator can use (signatory) or manage (administrator) the SCD, and thus avoid that an attacker may gain information on it. The security functions specified by FDP_RIP.1/SSCD_OBJ and FCS_CKM.4 ensure that residual information on SCD, VAD, and RAD is destroyed after usage and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD (FCS_CKM.1/GENKEY). The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD, VAD, and RAD. FPT_AMT.1 and FPT_FLS.1 test the working conditions of the TOE and guarantee a secure state when integrity is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS is differential fault analysis (DFA).
The assurance requirements ADV_IMP.2 by requesting evaluation of the TOE implementation, AVA_SOF.1 by requesting strength of function high for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1/GENKEY to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Cryptographic correspondence is provided by FCS_COP.1/CORRESP.

OT.SCD_Unique (Uniqueness of the signature-creation data) implements the requirement of practically unique SCD as laid down in the Directive [1], Annex III, article 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1/GENKEY

OT.DTBS_Integrity_TOE (Verification of DTBS-representation integrity) covers that integrity of the DTBS-representation to be signed is to be verified, as well as the DTBS-representation are not altered by the TOE. This is provided by integrity failure detection (FCS_COP.1/SYM) and the trusted channel integrity verification mechanisms of FDP_ITC.1/DTBS, FTP_ITC.1/DTBS IMPORT, and by FDP_UIT.1/TOE DTBS. The verification that the DTBS-representation has not been altered by the TOE is done by integrity functions specified by FDP_SDI.2/DTBS. The access control requirements of FDP_ACC.1/SIGNATURE-CREATION SFP and FDP_ACF.1/ SIGNATURE CREATION SFP keeps unauthorised parties off from manipulating the TOE to alter the DTBS-representation. Authenticity

OT.Sigy_SigF (Signature generation function for the legitimate signatory only) is provided by FIA_UAU.1 and FIA_UID.1 that ensure that no signature generation function can be invoked before the signatory is identified and authenticated. The security functions specified by FDP_ACC.1/PERSONALISATION SFP, FDP_ACC.1/SIGNATURE-CREATION SFP, FDP_ACF.1/PERSONALISATION SFP, FDP_ACF.1/SIGNATURE-CREATION SFP, FMT_MTD.1/D.RAD, FMT_SMF.1/SSCD and FMT_SMR.1/SSCD ensure that the signature process is restricted to the signatory. The security functions specified by FIA_ATD.1/D.RAD, FMT_MOF.1, FMT_SMF.1/SSCD, FMT_MSA.2, and FMT_MSA.3 ensure that the access to the signature generation functions for usage remain under the sole control of the signatory, as well as FMT_MSA.1/SIGNATORY provides that the control of corresponding security attributes is under signatory's control.
The security functions specified by FDP_SDI.2/Persistent and FPT_TRP.1/TOE ensure the integrity of stored data both during communication and while stored. The security functions specified by FDP_RIP.1/SSCD_OBJ and FIA_AFL.1/D.RAD and FIA_AFL.1/PUK provide protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.
The assurance measures specified by AVA_MSU.3 by requesting analysis of misuse of the TOE implementation, AVA_SOF.1 by requesting high strength level for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1/SIGNING which ensures the cryptographic robustness of the signature algorithms. The security functions specified by FPT_AMT.1 and FPT_TST.1 ensure that the security functions are performing correctly. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE.

OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD) is provided by a trusted channel guaranteeing SVD origin and integrity by means of FTP_ITC.1/SVD TRANSFER and FDP_UIT.1/SVD TRANSFER. The cryptographic algorithms specified by FDP_ACC.1/SVD TRANSFER SFP, FDP_ACF.1/SVD TRANSFER SFP and FDP_ETC.1/SVD TRANSFER ensure that only authorised user can export the SVD to the CGA.

OT.Tamper_ID (Tamper detection) is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to resist physical attacks.

OT.EEPROM (Verification of the D.IMAGE authenticity) is provided by FDP_ACC.1/EEPROM SFP and FDP_ACF.1/ EEPROM SFP that keeps unauthorised parties off from manipulating the TOE to alter the D.IMAGE Authenticity and integrity. The attributes of the authenticated D.IMAGE are provided by FMT_MSA.3/EEPROM for static attribute initialisation. FMT_SMF.1/SSCD, FMT_MSA.1/ADMINISTRATOR provide that the control of corresponding security attributes is under administrator's control.

8.2.4 Environment security requirements rationale

8.2.4.1 Cross table correspondence

Environment Security Requirement / Environment Security objectives	OE.CGA_Qcert	OE.Data_Protection	OE.HI_VAD	OE.Legal_Decisions	OE.Perso	OE.SVD_Auth_CGA	OE.SCA_Data_Intend	OD.Assurance	OD.Material	OE.Users	OE.User_Information
FCS_CKM.2/CGA	X										
FCS_CKM.3/CGA	X										
FDP_UIT.1/SVD IMPORT						X					
FTP_ITC.1/SVD IMPORT						X					
FCS_COP.1/SCA HASH							X				
FDP_UIT.1/SCA DTBS							X				
FTP_ITC.1/SCA DTBS							X				
FTP_TRP.1/SCA			X								
FDP_ACC.2/Data Protection		X		X							
FDP_ACF.1/Data Protection		x		x							
FDP_UIT.1/Data Protection		X		X							
FIA_UID.1/Data Protection		X		X							
FMT_SMF.1/Perso data					X						
FMT_SMR.1/Perso data					X						
FMT_MTD.1/Perso data					X						
FMT_MTD.2/Perso data					X						
FTP_ITC.1/Data Protection		X		X							
FTP_TRP.1/Data Protection		X		X							
ALC_DVS								X	X		
ALC_TAT									X		
AGD_USR										X	X

The following table gives the relationship between the environment security requirements and the environment security objectives.

Table 21 – Coverage of Environment security objectives by security requirements for Digital Signature Application

OE.CGA_QCert (Generation of qualified certificates) addresses the requirement of qualified certificates. The functions specified by FCS_CKM.2/CGA provide the cryptographic key distribution method. The functions specified by FCS_CKM.3/CGA ensure that the CGA imports the SVD using a secure channel and a secure key access method. R.Sigy_Name ensures that the identity of the person is verified in the corresponding qualified certificate according Annex 2 of [DIRECTIVE].

OE.HI_VAD (Protection of the VAD) covers confidentiality and integrity of the VAD which is provided by the trusted path FTP_TRP.1/SCA.

OE.SCA_Data_Intend (Data intended to be signed) is provided by the functions specified by FDP_UIT.1/SCA DTBS that ensures that the DTBS can be checked, by FTP_ITC.1/SCA DTBS that protects the DTBS by using a trusted channel to transmit the DTBS to the TOE, and FCS_COP.1/SCA HASH that provides that the hashing function corresponds to the approved algorithms.

OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) is provided by FTP_ITC.1/SVD IMPORT which assures identification of the sender and by FDP_UIT.1/SVD IMPORT which included it's integrity.

OE.Legal_Decisions and OE.Data_Protection are provided by FDP_ACC.2, FDP_ACF.1, FDP_UIT.1/Data Protection, FTP_ITC.1/Data Protection and FTP_TRP.1/Data Protection which insure that authorized persons, who are allowed to read, write or modify data in the card, work only in an environment, where unauthorized access to these data is prevented.

OE.Perso is provided by FMT_SMF.1/Perso data, FMT_SMR.1/Perso data, FMT_MTD.1/Perso data and FMT_MTD.2/Perso data which insure that data produced during personalisation or additional personalisation steps are correct

OD.Assurance is provided by the security assurance requirements ALC_DVS.1 that ensure the protection of the TOE in development and manufacturing environment.

OD.Material is provided by the security assurance requirements ALC_DVS.1 and ALC_TAT.1 that ensure the protection of the TOE in development and manufacturing environment, and the usage of the correct tools.

OE.Users, OE.User_Information is provided by the security assurance requirements AGD_USR that ensure that the developer provide a user guidance including security recommendations (adequate usage, information about secure usage, description of requirements concerning the IT environment)
.

8.2.5 TOE security functional requirements dependencies

SFR	Dependency	Which is
FCS_CKM.1/SM	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	- Included Included Included (justification 1)
FCS_CKM.1/GENKEY	FCS_CKM.2 or FCS_COP.1/SIGNING] FCS_CKM.4 FMT_MSA.2	- Included Included Included
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/SM, FCS_CKM.1/GENKEY], FMT_MSA.2	- - included Included (justification 1)
FCS_COP.1/HASH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/SM], FCS_CKM.4, FMT_MSA.2	- - Not needed (justification 2)
FCS_COP.1/CCA_SIGN	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/SM], FCS_CKM.4, FMT_MSA.2	- - Not needed(justification 3)
FCS_COP.1/CCA_VERIF	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/SM], FCS_CKM.4, FMT_MSA.2	- - Not needed (justification 3)
FCS_COP.1/CSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/SM], FCS_CKM.4, FMT_MSA.2	- - Not needed (justification 3)
FCS_COP.1/ASYM_DEC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/SM], FCS_CKM.4, FMT_MSA.2	- - Not needed (justification 3)
FCS_COP.1/SYM	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/SM], FCS_CKM.4, FMT_MSA.2	- - included included Included (justification 1)
FCS_COP.1/MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/SM], FCS_CKM.4, FMT_MSA.2	- - included included included (justification 1)

SFR	Dependency	Which is
FCS_COP.1/SIGNING	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/GENKEY] FCS_CKM.4 FMT_MSA.2	- - Included Included Included
FCS_COP.1/CORRESP	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1/GENKEY] FCS_CKM.4 FMT_MSA.2	- - included included included
FCS_RND.1	-	-
FDP_ACC.1/INITIALISATION SFP	FDP_ACF.1/INITIALISATION SFP	Included
FDP_ACC.1/PERSONALISATION SFP	FDP_ACF.1/ PERSONALISATION SFP	Included
FDP_ACC.1/SIGNATURE CREATION SFP	FDP_ACF.1/SIGNATURE CREATION SFP	Included
FDP_ACC.1/SVD TRANSFER SFP	FDP_ACF.1/SVD TRANSFER SFP	Included
FDP_ACC.1/EEPROM SFP	FDP_ACF.1/EEPROM SFP	Included
FDP_ACC.2	FDP_ACF.1/ACCESS RULES	Included
FDP_ACF.1/ACCESS RULES	FDP_ACC.1, FMT_MSA.3	Fulfilled by FDP_ACC.2 Not included (justification 4)
FDP_ACF.1/INITIALISATION SFP	FDP_ACC.1/INITIALISATION SFP FMT_MSA.3	Included Included
FDP_ACF.1/PERSONALISATION SFP	FDP_ACC.1/ PERSONALISATION SFP FMT_MSA.3	Included Included
FDP_ACF.1/SIGNATURE CREATION SFP	FDP_ACC.1/SIGNATURE CREATION SFP FMT_MSA.3	Included Included
FDP_ACF.1/ SVD TRANSFER SFP	FDP_ACC.1/SVD TRANSFER SFP FMT_MSA.3	Included Included
FDP_ACF.1/ EEPROM SFP	FDP_ACC.1/EEPROM SFP FMT_MSA.3 /EEPROM	Included Included
FDP_ETC.1/SVD TRANSFER	[FDP_ACC.1/SVD TRANSFER SFP or FDP_IFC.1]	Included -
FDP_ITC.1/DTBS	[FDP_ACC.1/ SIGNATURE CREATION SFP or FDP_IFC.1] FMT_MSA.3	Included - Included
FDP_RIP.1/HEALTH_OBJ	-	
FDP_RIP.1/SSCD_OBJ	None	-
FDP_SDI.2/persistent	None	-
FDP_SDI.2/volatile	None	-
FDP_SDI.2/DBTS	None	-
FDP_UCT.1	[FTP_ITC.1/ACCESS RULES, or FTP_TRP.1], [FDP_ACC.1, or FDP_IFC.1]	Included - Fulfilled by FDP_ACC.2 -
FDP_UIT.1/ ACCESS RULES	[FTP_ITC.1/ACCESS RULES, or FTP_TRP.1],	Included -

SFR	Dependency	Which is
	[FDP_ACC.1, or FDP_IFC.1]	Fulfilled by FDP_ACC.2 -
FDP_UIT.1/SVD TRANSFER	[FDP_ACC.1/SVD TRANSFER or FDP_IFC.1] [FTP_ITC.1/SVD TRANSFER or FTP_TRP.1]	Included - Included -
FDP_UIT.1/TOE DTBS	FDP_ACC.1/SIGNATURE CREATION SFP or FDP_IFC.1] [FTP_ITC.1/DTBS IMPORT or FTP_TRP.1]	Included - Included -
FIA_AFL.1/PIN	FIA_UAU.1	Included
FIA_AFL.1/PUC	FIA_UAU.1	Included
FIA_AFL.1/D.RAD	FIA_UAU.1	Included
FIA_AFL.1/PUK	FIA_UAU.1	Included
FIA_ATD.1	None	
FIA_ATD.1/D.RAD	None	-
FIA_UID.1/ HEALTH	-	
FIA_UID.1	-	
FIA_UAU.1/ HEALTH	FIA_UID.1/ HEALTH	Included
FIA_UAU.1	FIA_UID.1	Included
FIA_UAU.4	None	
FMT_LIM.1	FMT_LIM.2	Included
FMT_LIM.2	FMT_LIM.1	Included
FMT_MOF.1	FMT_SMR.1/SSCD FMT_SMF.1/SSCD	Included Included
FMT_MSA.1/ADMINISTRATOR	[(FDP_ACC.1/INITIALISATION SFP or FDP_IFC.1] FMT_SMR.1/SSCD FMT_SMF.1/SSCD	Included - Included Included
FMT_MSA.1/SIGNATORY	[FDP_ACC.1/SIGNATURE CREATION or FDP_IFC.1] FMT_SMR.1/SSCD FMT_SMF.1/SSCD	Included - Included Included
FMT_MSA.2	ADV_SPM.1 [FDP_ACC.1/ PERSONALISATION SFP or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	Included Included - Included Included
FMT_MSA.3	FMT_MSA.1/ADMINISTRATOR FMT_MSA.1/SIGNATORY FMT_SMR.1/SSCD	Included Included Included
FMT_MSA.3/EEPROM	FMT_MSA.1/ADMINISTRAT FMT_SMR.1/SSCD	Included Included
FMT_MTD.1/INI	FMT_SMF.1/HEALTH, FMT_SMR.1/HEALTH	Included included
FMT_MTD.1/PIN	FMT_SMF.1/HEALTH, FMT_SMR.1/HEALTH	Included included

SFR	Dependency	Which is
FMT_MTD.1/Pers	FMT_SMF.1/HEALTH, FMT_SMR.1/HEALTH	Included included
FMT_MTD.1/CMS	FMT_SMF.1/HEALTH, FMT_SMR.1/HEALTH	Included included
FMT_MTD.1/KEY_MOD	FMT_SMF.1/HEALTH, FMT_SMR.1/HEALTH	Included included
FMT_MTD.1/D.RAD	FMT_SMR.1/SSCD FMT_SMF.1/SSCD	Included Included
FMT_SMF.1/HEALTH	-	
FMT_SMF.1/SSCD	-	
FMT_SMR.1/HEALTH	FIA_UID.1/HEALTH	Included
FMT_SMR.1/SSCD	FIA_UID.1	Included
FPT_AMT.1	None	-
FPT_EMSEC.1	None	-
FPT_FLS.1	ADV_SPM.1	Included
FPT_PHP.1	None	
FPT_PHP.3	None	-
FPT_TST.1	FPT_AMT.1	Included
FPT_RVM.1	None	-
FPT_SEP.1	None	-
FTP_ITC.1/ACCESS RULES	None	-
FTP_ITC.1/DBTS IMPORT	None	-
FTP_ITC.1/SVD TRANSFER	None	-
FTP_TRP.1/TOE	None	-

8.2.5.1.1 Justification of unsupported security functional requirements dependencies

Justification 1 : For the health application protection profile the inclusion of the FMT_MSA2 is not necessary. The TOE does not support logical channels.
Justification 2: The cryptographic algorithm for hashing 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.
Justification 3: The SFR FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/CSA and FCS_COP.1/ASYM_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.
Justification 4: The access control TSF according to FDP_ACF.1/ACCESS RULES uses security attributes which are defined during the personalisation and are fixed over the whole life time of the TOE. No management of these security attribute is necessary here.

8.2.5.2 IT environment security functional requirements dependencies

The following table gives the dependencies of the IT environment security functional requirements.

SFR	Dependency	Which is
CGA		
FCS.CKM.2/CGA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Included - - Not included Not included
FCS.CKM.3/CGA	[FDP_ITC.1/SVD IMPORT or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Included - - Not included Not included
FDP_UIT.1/ CGA SVD IMPORT	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1/SVD IMPORT or FTP_TRP.1]	Not included - Included -
FTP_ITC.1/CGA SVD IMPORT	None	-
SCA		
FCS_COP.1/SCA HASH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Not included Not included Not included Not included Not included
FDP_UIT.1/SCA DTBS	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	Not Included - Included Included
FTP_ITC.1/SCA DTBS	None	
FTP_TRP.1/SCA	None	-
FDP_ACC.2/Data Protection	FDP_ACF.1/Data Protection	Included
FDP_ACF.1/Data Protection	FDP_ACC1 FMT_MSA.3/Data Protection	Fulfilled by FDP_ACC2/Data Protection Not Included
FDP_UIT.1/Data Protection	[FDP_ACC.1 Or FDP_IFC.1] [FTP_ITC.1/Data Protection Or FTP_TRP.1/Data Protection]	Fulfilled by FDP_ACC2/Data Protection - Included Included
FIA_UID.1/Data protection	None	
FMT_SMF.1/Perso Data	None	
FMT_SMR.1/Perso Data	None	
FMT_MTD.1/Perso Data	FMT_SMF.1/Perso Data FMT_SMR.1/Perso Data	Included Included
FMT_MTD.3/Perso Data	ADV_SPM.1 FMT_MTD.1/Perso Data	 Included
FTP_ITC.1/Data Protection	None	
FTP_TRP.1/Data Protection	None	

Table 22 – Security functional requirement dependencies

8.2.5.2.1 Justification of unsupported IT environment security functional requirements dependencies

FCS_CKM.2/CGA	The CGA generates qualified electronic signatures including the SVD imported from the TOE. The dependency for the import is supported by FDP_ITC.1/SVD IMPORT. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this ST.

FCS_CKM.3/CGA	The CGA imports SVD via trusted cannel implemented by FDP_ITC.1/ SVD import. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this ST.
FDP_UIT.1/SVD IMPORT (CGA)	The Access control policy (FDP_ACC.1.1) for the CGA are outside of the scope of this ST.
FCS_COP.1/SCA HASH	The hash algorithm implemented by FCS_COP.1/SCA HASH does not require any key or security management. Therefore FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2 are not required for FCS_COP.1/SCA HASH in the SCA.
FDP_UIT.1/SCA DTBS	The Access control policy (FDP_ACC.1.1) for the SCA are outside of the scope of this ST
FCS_CKM.1/ SSCD	The SSCD generates the SCD/SVD pair. The dependency for cryptographic secure key generation is supported by FCS_COP.1/CORRESP, verification of SCD/SVD correspondence, and the key destruction by FCS_CKM.4/SSCD. The Secure security attribute SFR, FMT_MSA.2 is outside the scope of this PP.
FCS_CKM.4/ SSCD	The SSCD destroys the SCD once it has been exported. The dependency for key generation is supported by FCS_CKM.1. The Secure security attribute SFR, FMT_MSA.2 is outside the scope of this PP.
FCS_COP.1/ SSCD CORRESP	The SSCD does a cryptographic operation when creating the SCD/SVD pair, FCS_CKM.1 and when destroying it, FCS_CKM.4/SSCD. The Secure security attribute SFR, FMT_MSA.2 is outside the scope of this PP.
FDP_ACC.1/SSCD SCD Export SFP	The SSCD will follow the SCD export SFP when exporting the SCD. The access control required by this SFP, FDP_ACF.1 Security attribute based access control, is outside the scope of this PP.
FDP_ACF.1/Data Protection	The Static attribute initialisation SFR (FMT_MSA.3) is outside of the scope

8.2.6 TOE security assurance requirements rationale

8.2.6.1 Security assurance requirements / TOE security objectives correspondence analysis

The following table shows how the security assurance requirements are appropriated to complete TOE security objectives.

Requirement	Security Objectives
Security Assurance Requirements	
ACM_AUT.1	EAL 4
ACM_CAP.4	EAL 4
ACM_SCP.2	EAL 4
ADO_DEL.2	EAL 4
ADO_IGS.1	EAL 4
ADV_FSP.2	EAL 4
ADV_HLD.2	EAL 4
ADV_IMP.2	All executable software in the TOE has to be covered by the evaluation.
ADV_LLD.1	EAL 4
ADV_RCR.1	EAL 4
ADV_SPM.1	EAL 4
AGD_ADM.1	EAL 4
AGD_USR.1	EAL 4
ALC_DVS.1	EAL4, OT.Lifecycle_Security
ALC_LCD.1	EAL4, OT.Lifecycle_Security
ALC_TAT.1	EAL4, OT.Lifecycle_Security
ATE_COV.2	EAL 4
ATE_DPT.1	EAL 4

Requirement	Security Objectives
ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_MSU.3	OT.Sigy_SigF
AVA_SOF.1	EAL 4, OT.Datas_Secrecy, OT.Sigy_SigF
AVA_VLA.4	OT.Datas_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.EMSEC_Design

Table 23 – Security assurance requirements / TOE security objectives correspondence analysis

8.2.7 TOE security assurance requirements dependencies

The following table gives the dependencies of the security assurance requirements.

SAR	Dependency	Which is
ADO_IGS.1	AGD_ADM.1	Included
ADV_FSP.2	ADV_RCR.1	Included
ADV_HLD.2	ADV_FSP.1 ADV_RCR.1	Included Included
ADV_IMP.2	ADV_LLD.1 ADV_RCR.1 ALC_TAT.1	Included Included Included
ADV_LLD.1	ADV_HLD.2 ADV_RCR.1	Included Included
ADV_RCR.1	None	-
ADV_SPM.1	ADV_FSP.1	Included
AGD_ADM.1	ADV_FSP.1	Included
AGD_USR.1	ADV_FSP.1	Included
ALC_DVS.1	None	-
ALC_LCD.1	None	-
ALC_TAT.1	ADV_IMP.1	Fulfilled by ADV_IMP.2
ATE_COV.2	ADV_FSP.1 ATE_FUN.1	Included Included
ATE_DPT.1	ADV_HLD.1 ATE_FUN.1	Included Included
ATE_FUN.1	None	-
ATE_IND.2	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	Included Included Included Included
AVA_MSU.3	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	Included Included Included Included
AVA_SOF.1	ADV_FSP.1 ADV_HLD.1	Included Included
AVA_VLA.4	ADV_FSP.1 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 AGD_ADM.1 AGD_USR.1	Included Included Fulfilled by ADV_IMP.2 Included Included Included

Table 24 – Security assurance requirement dependencies

8.2.8 Mutually supportive and internally consistent rationale

This part shows that the security functional requirements are complete and internally consistent by demonstrating that they are mutually supportive and provide an ‘integrated effective whole’.

The interactions between security functional requirements are not limited to the dependencies between these security functional requirements and, due to the environment of the TOE, security functional requirements for IT environment are included in the dependencies.
It is the same for security assurance requirements.

8.3 TOE SUMMARY SPECIFICATION RATIONALE

The purpose of this chapter is to demonstrate the coverage of security requirements by the security functions and assurance measures defined in the **chapter 6**.

8.3.1 SOF level rationale

The minimum strength level for the TOE security functions is **SOF-high**. According to [CEM] part 2 section 424, the strength of cryptographic algorithms is outside the scope of the CC evaluation.
The security functions SF_TSF_PROTECTION, SF_ACCESS, SF_CARD_INIT do not use probalistic or permutational effects.

8.3.1.1 SF_CRYPTO

The strength of the functions is SOF-high.

8.3.1.2 SF_AUTHENTICATION

The strength of the functions is SOF-high.
The SOF-High for the authentication of the users is achieved with the combination of the following SFRs:
FIA_ATD.1/D.RAD (PIN), FMT_MSA.2 ,FIA_AFL.1/D.RAD, FIA_AFL/PUK FIA_AFL/PUC TOE security functions rationale

8.3.1.3 Cross table correspondence

TOE Security Functional Requirements / TOE Security functions	**SF_TSF_PROTECTION**	**SF_CRYPTO**	**SF_AUTHENTICATION**	**SF_ACCESS**	**SF_CARD_INIT**	**SF1.Operating state checking**	**SF6.TSF self tests**	**SF7.Notification of physical attack**
FCS_CKM.1/SM		X						
FCS_CKM.1 /GENKEY		X						
FCS_CKM.4		X			X			
FCS_COP.1/HASH		X						
FCS_COP.1/CCA_SIGN		X						
FCS_COP.1/CCA_VERIF		X						
FCS_COP.1/CSA		X						
FCS_COP.1/ASYM_DEC		X						
FCS_COP.1/SYM		X						
FCS_COP.1/MAC		X						
FCS_COP.1/CORRESP		X						
FCS_COP.1/SIGNING		X						
FCS_RND.1		X						
FDP_ACC.1/SVD TRANSFER SFP				X				
FDP_ACC.1/INITIALISATION SFP					X			
FDP_ACC.1/PERSONALISATION SFP					X			
FDP_ACC.1/SIGNATURE-CREATION SFP				X				

TOE Security Functional Requirements / TOE Security functions	SF_TSF_PROTECTION	SF_CRYPTO	SF_AUTHENTICATION	SF_ACCESS	SF_CARD_INIT	SF1.Operating state checking	SF6.TSF self tests	SF7.Notification of physical attack
FDP_ACC.1//EEPROM SFP					X			
FDP_ACC.2				X				
FDP_ACF.1/ACCESS RULES				X				
FDP_ACF.1/INITIALISATION SFP					X			
FDP_ACF.1/SVD TRANSFER SFP				X				
FDP_ACF.1/PERSONALISATION SFP					X			
FDP_ACF.1/SIGNATURE-CREATION SFP				X				
FDP_ACF.1//EEPROM SFP					X			
FDP_ETC.1/SVD TRANSFER				X				
FDP_ITC.1/DTBS		X						
FDP_RIP.1/HEALTH_OBJ		X	X					
FDP_RIP.1/SSCD_OBJ		X	X					
FDP_SDI.2/Persistent	X							
FDP_SDI.2/Volatile	X							
FDP_SDI.2/DTBS		X						
FDP_UCT.1				X				
FDP_UIT.1/ ACCESS RULES				X				
FDP_UIT.1/SVD TRANSFER				X				
FDP_UIT.1/TOE DTBS				X				
FIA_AFL.1/PIN			X					
FIA_AFL.1/PUC			X					
FIA_AFL.1/D.RAD			X					
FIA_AFL.1/PUK			X					
FIA_ATD.1			X	X				
FIA_ATD.1/D.RAD			X	X				
FIA_UID.1/ HEALTH			X	X				
FIA_UID.1			X	X				
FIA_UAU.1/ HEALTH			X	X				
FIA_UAU.1			X	X	X			
FIA_UAU.4			X	X				
FMT_LIM.1	X							
FMT_LIM.2	X							
FMT_MOF.1			X	X				
FMT_MSA.1/ADMINISTRATOR					X			
FMT_MSA.1/SIGNATORY			X	X				
FMT_MSA.2			X	X	X			
FMT_MSA.3					X			
FMT_MSA.3/EEPROM					X			
FMT_MTD.1/ini				X	X			
FMT_MTD.1/perso				X	X			
FMT_MTD.1/CMS				X				
FMT_MTD.1/PIN				X				
FMT_MTD.1/KEY_MOD				X				
FMT_MTD.1/D.RAD			X	X				
FMT_SMF.1/HEALTH			X	X	X			
FMT_SMF.1/SSCD			X	X	X			

TOE Security Functional Requirements / TOE Security functions	SF_TSF_PROTECTION	SF_CRYPTO	SF_AUTHENTICATION	SF_ACCESS	SF_CARD_INIT	SF1.Operating state checking	SF6.TSF self tests	SF7.Notification of physical attack
FMT_SMR.1/HEALTH			X		X			
FMT_SMR.1/SSCD			X		X			
FPT_AMT.1	X						X	
FMT_EMSEC.1		X	X					
FPT_FLS.1	X							
FPT_PHP.1	X					X	X	X
FPT_PHP.3						X	X	X
FPT_TST.1	X							
FPT_RVM.1	X							
FPT_SEP.1	X			X				
FTP_ITC.1/ACCESS RULES			X	X				
FTP_ITC.1/SVD TRANSFER			X	X				
FTP_ITC.1/DTBS IMPORT			X	X				
FTP_TRP.1/TOE			X	X				

Table 25 – Coverage of TOE security functional requirements by TOE security

FCS-CKM.1/SM Cryptographic key generation – Secure Messaging Keys : SF_CRYPTO can generate cryptographic keys SCD/SVD for length specified by the standard [eHC spec].

FCS-CKM.1/GENKEY Cryptographic key generation SF_CRYPTO can generate the digital signature keys SCD/SVD for length specified by the standard [ALGO].

FCS-CKM.4 Cryptographic key destruction : By fulfilling the corresponding access conditions controlled by SF_ACCESS, it should be possible to destroy the cryptographic keys but no re-generation is possible during user phase (phase 7). During personalisation, SF_CARD_INIT have the ability to restart from initialisation phase, and so to destroy an old cryptographic key.

FCS_COP.1/HASH, FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/CSA, FCS_COP.1/ASYM_DEC, FCS_COP.1/SYM, FCS_COP.1/MAC Cryptographic operation : The cryptographic operations are managed by SF_CRYPTO using cryptographic algorithm and key length specified in 5.1.1.1.3 .

FCS_COP.1/CORRESP, FCS_COP.1/SIGNING Cryptographic operation The cryptographic operations (SCD/SVD correspondence prove, digital signature application) are managed by SF_CRYPTO using cryptographic algorithm and key length specified by [ALGO].

FCS_RND.1 Quality metric for random numbers : The mechanism to generate random is manage by SF_CRYPTO using AIS 20.

FDP_ACC Access control policy
This SFR requires that each identified access control SFP cover all operations on subjects and objects covered by that SFP. It further requires that all objects and operations with the TSC are covered by at least one identified access control SFP. Five access control SFPs have been identified in this TOE.
FDP_ACC.1/SVD TRANSFER SFP covers the SVD TRANSFER SFP that controls the export of the public key SVD is only possible in user mode (by trust center) and is covered by SF_ACCESS..
INITIALISATION SFP is covered by **FDP_ACC.1/INITIALISATION SFP** during phase 5b. **FDP_ACC.1/PERSONALISATION** covers the PERSONALISATION SFP that controls the creation of the transport PIN (D.RAD) by the administrator during the personalisation phase. Theses requirements are supported by

SF_CARD_INIT which ensures the administration of the card during initialisation the personalisation phases. The SIGNATURE-CREATION SFP controls the import of the DTBS and the signature of the DTBS during the user phase. **FDP_ACC.1/SIGNATURE-CREATION SFP** covers this SFP and is supported by SF_ACCESS that manages the access conditions during the user phase. The EEPROM SFP ensures the image loaded during initialisation phase is authentic and integer. **FDP_ACC.1/EEPROM SFP** covers this SFP and is supported by SF_CARDINIT.

FDP_ACC.2 Complete Access Control : SFP access rules are managed by SF_ACCESS.

FDP_ACF.1/ACCESS RULES Security attribute based access control : SFP access rules are managed by SF_ACCESS.

FDP_ACF Access control functions
This SFR defines the rules for the functions that implement the SFPs as identified in FDP_ACC.1.
The iterations of component FDP_ACC.1 listed below correspond to the access control SFPs identified in this TOE. They are supported by the same SFs which support the corresponding iteration of FDP_ACC.1.
(FDP_ACF.1/INITIALISATION SFP, FDP_ACF.1/SVD TRANSFER SFP, FDP_ACF.1/PERSONALISATION SFP, FDP_ACF.1/SIGNATURE-CREATION SFP, FDP_ACF.1//EEPROM SFP)

FDP_ETC Export to outside TSF control
This SFR requires the appropriate SFPs are enforced during export of user data without its associated security attributes. The SVD is exported in user mode (by trust center). **FDP_ETC/SVD TRANSFER** is managed by SF_ACCESS.

FDP_ITC Import from outside TSF control
This SFR requires that the security attributes are supplied separately and correctly represent the user data imported without security attributes. The import of the SCD without any security attributes **(FDP_ITC/SCD)** is managed by SF_CARD_INIT. For Signature_creation SF_CRYPTO imports the DTBS without security attributes **(FDP_ITC/DTBS)**.

FDP_RIP.1/HEALTH_OBJ Residual Information Protection : This SFR requires that the TSF ensure that any residual information content of a resource is made unavailable to objects upon allocation or deallocation of this resource to the objects. All temporarily copies are destroyed after usage by SF_CRYPTO or deleted by SF_AUTHENTICATION.

FDP_RIP.1/SSCD_OBJ Residual information protection
This SFR requires that the TSF ensure that any residual information content of a resource is made unavailable to objects upon allocation or deallocation of this resource to the objects.
All temporarily copies of the SCD are destroyed after usage by SF_CRYPTO. For the VAD and RAD the temporarily copies are deleted by SF_AUTHENTICATION.

FDP_SDI.2/Persistent, FDP_SDI.2/Volatile Stored Data Integrity : This SFR requires that the TSF monitors user data stored within the TSC for identified integrity errors.
In the case of an integrity error on all the user data persistently stored by the TOE, the use of the datas are prohibited by SF_TSF_PROTECTION **(FDP_SDI.2/Persistent).**.The integrity of DTBS is verified by SF_CRYPTO **(FDP_SDI.2/DBTS)**.

FDP_UCT.1 Basic data exchange confidentiality : SFP access rules are managed by SF_ACCESS.

FDP_UIT.1/ ACCESS RULES Data exchange integrity : This SFR that requires that the TSF ensures the detection of modification, insertion, replay and/or deletion of the user data during a transfer is covered by SF_ACCESS.

FDP_UIT.1/SVD TRANSFER, FDP_UIT.1/TOE DBTS Inter-TSF user data integrity transfer protection This SFR that requires that the TSF ensures the detection of modification, insertion and/or deletion of the user data during a transfer is covered by SF_ACCESS during the export of the SVD **(FDP_UIT.1/SVD TRANSFER)** and SF_ACCESS during the import of the DTBS **(FDP_UIT.1/TOE DTBS).**

FIA Identification and authentication : The SFRs from this class are managed by SF_AUTHENTICATION, SF_ACCESS and SF_CARD_INIT.
1/ The user is identified and authenticated following access rules **(FIA_ATD)**. In case of three consecutive failed authentication attempts of the user using PIN, the PIN is blocked **(FIA_AFL.1/PIN)**. In case of three failed or successful authentication attempt of the user using PUC, the PUC is blocked **(FIA_AFL.1/PUC)**
SF_ACCESS and SF_AUTHENTICATION control if an authentication is required before specific operations are allowed **(FIA_UID.1/ HEALTH, FIA_UAU.1/ HEALTH, FIA_UAU.4)**
2/ The user is identified and authenticated by presenting a PIN **(FIA_ATD.1/D.RAD)**. In case of ten consecutive failed authentication attempts of the user using PIN, the PIN is blocked **(FIA_AFL.1/D.RAD)**. In case of ten failed or successful authentication attempt of the user using PUK, the PUK is blocked **(FIA_AFL.1/PUK)**
SF_ACCESS (user) and SF_CARD_INIT (Administrator during the personalisation phases) control if an authentication is required before specific operations are allowed **(FIA_UAU.1)**

FMT_LIM Limited capabilities : SF_TSF_PROTECTION address the management of TSF and TSF data misuse of tests features of the TOE.

FMT_MOF.1 Management of function in the TSF This SFR requires to restrict the ability to enable the signature creation function by the signatory. SF_AUTHENTICATION and SF_ACCESS (only the signatory) manages this functionality : the signature creation function is validated when the Signatory replace the transport PIN by its own PIN.

FMT_MSA Management of security attributes SF_CARD_INIT allow the Administrator to manage the security attributes for INITIALISATION SFP **(FMT_MSA.1/Administrator)**. The attribute « SCD operational » is managed by SF_ACCESS and SF_AUTHENTICATION (Replace Transport PIN by signatory PIN) (**FMT_MSA.1/Signatory)** The management of secure values for security attributes is realized by SF_AUTHENTICATION for the PIN (6 digits long verification), SF_CARD_INIT for the SCD/SVD management and SF_ACCESS for others datas **(FMT_MSA.2),** restrictive default values are provided for the security attributes controlled by INITIALISATION SFP (SF_CARD_INIT) **(FMT_MSA.3),** EEPROM SFP (SF_CARD_INIT) (**FMT_MSA.3 EEPROM).**

FMT_MTD Management of TSF data The access to commands allowing card holder to modify PIN is controlled by SF_ACCESS and SF_AUTHENTICATION. The impossibility to modify the Public Key for Certification is controlled by SF_ACCESS. The possibility to write initialisation data for the TOE manufacturer or to personalisation data for the personalisation service provider is controlled by SF_ACCESS and SF_CARD_INIT. The restrict of the ability to download additional application to the Download service provider is addressed by SF_ACCESS
(FMT_MTD.1/ini, FMT_MTD.1/perso, FMT_MTD.1/CMS, FMT_MTD.1/PIN, FMT_MTD.1/KEY_MOD)
The access to commands allowing the signatory to modify PIN is controlled by SF_ACCESS and SF_AUTHENTICATION **(FMT_MTD.1/D.RAD**).

FMT_SMF.1/HEALTH Specification of Management Functions: The security management functions are managed by SF_ACCESS, SF_AUTHENTICATION (Modification of the PIN, Service card Management) and SF_CARD_INIT (Initialisation, Personalisation).

FMT_SMF.1/SSCD Specification of Management Functions The management functions to restrict the ability to enable the signature creation function by the signatory are controlled by SF_AUTHENTICATION and SF_ACCESS, to modify security attributes as SCD Import SFR, EEPROM SFP or INITIALISATION SFP are provided by SF_CARD_INIT, to modify Signature-Creation SFP or PIN are provided by SF_ACCESS and SF_AUTHENTICATION.

FMT_SMR.1/HEALTH Security roles: SF_AUTHENTICATION and SF_CARD_INIT maintains the roles card holder, download service provider, personalisation service provider and TOE manufacturer.

FMT_SMR.1/SSCD Security management roles SF_AUTHENTICATION and SF_CARD_INIT maintains the roles S.Admin and S.Signatory.

FPT_AMT Abstract machine testing The hardware security functionalities are tested during initial start-up and periodically by SF_TSF_PROTECTION, with the support of the IC security function SF6 (TSF self test), that manages the IC security features.

FPT_EMSEC TOE Emanation The counter-measures to avoid access via emanations using TOE interfaces are implemented by SF_AUTHENTICATION and SF_CRYPTO.

FPT_FLS.1 Failure with preservation of secure state :This SFR requires that the TSF preserve a secure state in the face of the following identified failures:
- FPT_TST.1 detects error: SF_TST_PROTECTION prevent information leakage by preserving a secure state
- Authentication data integrity failure: SF_TSF_PROTECTION prevents the use of RAD and informs the user.
- exposure to operating conditions due to external events and unexpected errors during execution of the TSF: SF_TSF_PROTECTION preserves a secure state by resetting security attributes to secure values and if necessary recovers the persistently stored data to a secure state.

FPT_PHP TSF Physical Protection
These SFRs, FPT_PHP.1 refer to restrictions on unauthorised physical access to the TSF, and to the deterrence of, and resistance to, unauthorised physical modification, or substitution of the TSF. They are supported by security functions provided by the IC which are SF1 (Operating state checking), SF6 (TSF self test), SF7 (Notification of physical attack) and SF_TSF_PROTECTION

.

FPT_PHP.3 Resistance to physical attack
These SFR, refer to restrictions on unauthorised physical access to the TSF, and to the deterrence of, and resistance to, unauthorised physical modification, or substitution of the TSF. This SFR is supported by SF1 (Operating state checking), SF6 (TSF self test), SF7 (Notification of physical attack).
FPT_TST.1 TSF testing : By doing software self test during initial start-up, integrity test for code patches (if any) and TSF data stored in EEPROM, and test of random numbers at the request of the operating system SF_TSF_PROTECTION supports this requirement.

FPT_RVM.1 Non-bypassability of the TSP and FPT_SEP.1 TSF domain separation: These SFR that require that the TSF prevents any bypass of the access rules, ensures that dealing with sensitive information or preventing information leakage can not be bypassed or corrupted, ensures that the detecting errors or insecure operational can not be bypassed or corrupted, ensures that the protection of TOE functions intended for the testing, the initialisation and the personalisation of the TOE can not by bypassed or corrupted is covered by SF_TSF_PROTECTION and SF_ACCESS.

FTP_ITC.1/ACCESS RULES Inter-TSF Trusted Channel: This SFR that requires that the TSF ensures communication via trusted channel as defines by SFP_acces_rules is covered by SF_ACCESS.Symmetric and asymmetric one-time cryptographic challenge-response protocols are able to establish a trusted channel or a trusted path. This trusted channel must be used for access to some eHC data, depending on the access conditions. It's covered by SF_AUTHENTICATION.

FTP_ITC.1/SVD TRANSFER, FTP_ITC/DTBS IMPORT Inter-TSF trusted channel This SFR requires that the TSF provide a trusted communication channel between itself and another trusted IT product. During user phase, SF_AUTHENTICATION by negotiating session keys and SF_ACCESS by providing secure-messaging functionality supports this requirement **(FTP_ITC/DTBS IMPORT, FTP_ITC.1/SVD TRANSFER)**.

FTP_TRP.1/TOE Trusted path This SFR requires that a trusted path between the TSF and a user be provided for user authentication. SF_AUTHENTICATION by negotiating session keys and SF_ACCESS by providing secure-messaging functionality supports this requirement.

8.3.2 TOE security functions dependencies

The following table gives the dependencies of the TOE ES security functions.

SF	Dependency	Which is
SF_TSF_PROTECTION	SF_CRYPTO	Included
SF_CRYPTO	SF_TSF_PROTECTION	Included
SF_AUTHENTICATION	SF_TSF_PROTECTION SF_CRYPTO	Included Included
SF_ACCESS	SF_TSF_PROTECTION SF_AUTHENTICATION SF_CRYPTO	Included Included Included
SF_CARD_INIT	SF_TSF_PROTECTION	Included

	SF_CRYPTO	Included

Table 26 – Security function dependencies

8.3.3 Assurance measures rationale

8.3.3.1 Assurance security requirements coverage

The following table shows how the assurance measures are appropriated to complete each security assurance requirements.

Security assurance requirement	Assurance measure	Rationale
ACM_AUT.1	AM_ACM	The assurance measure AM_ACM is about configuration management.
ACM_CAP.4	AM_ACM	The assurance measure AM_ACM is about configuration management, and confirms that the ACM_CAP.4 component is completed.
ACM_SCP.2	AM_ACM	The assurance measure AM_ACM is about configuration management, and confirms that the ACM_SCP.2 component is completed.
ADO_DEL.2	AM_ADO	The assurance measure AM_ADO gives the delivery procedures and confirms that the ADO_DEL.2 component is completed.
ADO_IGS.1	AM_ADO	The assurance measure AM_ADO gives the installation, generation and start-up procedures and confirms that the ADO_IGS.1 component is completed.
ADV_FSP.2	AM_ADV	The assurance measure AM_ADV gives the functional specification by describing the internal and external interfaces and confirms that the ADV_FSP.2 component is completed.
ADV_HLD.2	AM_ADV	The assurance measure AM_ADV gives the architectural design by system decomposition and confirms that the ADV_HLD.2 component is completed
ADV_IMP.2	AM_ADV	The assurance measure AM_ADV gives the implementation and confirms that the ADV_IMP.2 component is completed
ADV_LLD.1	AM_ADV	The assurance measure AM_ADV gives the architectural design by subsystem decomposition and confirms that the ADV_LLD.1 component is completed
ADV_RCR.1	AM_ADV	The assurance measure AM_ADV gives the correspondence demonstration and confirms that the ADV_RCR.1 component is completed
ADV_SPM.1	AM_ADV	The assurance measure AM_ADV gives the security policy model and confirms that the ADV_SPM.1 component is completed
AGD_ADM.1	AM_AGD	The assurance measure AM_AGD gives the administration documentation and confirms that the AGD_ADM.1 component is completed
AGD_USR.1	AM_AGD	The assurance measure AM_AGD gives the user documentation and confirms that the AGD_USR.1 component is completed
ALC_DVS.1	AM_ALC	The assurance measure AM_ALC gives the security measures and confirms that the ALC_DVS.1 component is completed
ALC_LCD.1	AM_ALC	The assurance measure AM_ALC gives the development process and confirms that the ALC_LCD.1 component is completed
ALC_TAT.1	AM_ALC	The assurance measure AM_ALC gives the development tools and confirms that the ALC_TAT.1

		component is completed
ATE_COV.2	AM_ATE	The assurance measure AM_ATE gives the test documentation and confirms that the ATE_COV.2 component is completed
ATE_DPT.1	AM_ATE	The assurance measure AM_ATE gives the test documentation and confirms that the ATE_DPT.1 component is completed
ATE_FUN.1	AM_ATE	The assurance measure AM_ATE gives the test documentation and confirms that the ATE_FUN.1 component is completed
ATE_IND.2	AM_ATE	The assurance measure AM_ATE gives the test documentation and confirms that the ATE_IND.2 component is completed
AVA_MSU.3	AM_AVA	The assurance measure AM_AVA gives the validation of analysis and confirms that the AVA_MSU.3 component is completed
AVA_SOF.1	AM_AVA	The assurance measure AM_AVA gives the SOF evaluation and confirms that the AVA_SOF.1 component is completed
AVA_VLA.4	AM_AVA	The assurance measure AM_VLA gives the covert channel analysis and confirms that the AVA_VLA.4 component is completed

Table 27 – Assurance measures coverage

8.3.3.2 Cross table correspondence

Security Assurance Requirements / Assurance Measure	AM_ACM	AM_ADO	AM_ADV	AM_AGD	AM_ALC	AM_ATE	AM_AVA
ACM_AUT.1	X						
ACM_CAP.4	X						
ACM_SCP.2	X						
ADO_DEL.2		X					
ADO_IGS.1		X					
ADV_FSP.2			X				
ADV_HLD.2			X				
ADV_IMP.2			X				
ADV_LLD.1			X				
ADV_RCR.1			X				
ADV_SPM .1			X				
AGD_ADM.1				X			
AGD_USR.1				X			
ALC_DVS.1					X		
ALC_LCD.1					X		
ALC_TAT.1					X		
ATE_COV.2						X	
ATE_DPT.2						X	
ATE_FUN.1						X	
ATE_IND.2						X	
AVA_MSU.3							X
AVA_SOF.1							X
AVA_VLA.4							X

Table 28 – Assurance measures cross table

8.3.4 Assurance measures dependencies

The following table gives the dependencies of the assurance measures.

AM	Dependency	Which is
AM_ACM	AM_ACM	Included
AM_ADO	AM_ACM AM_AGD	Included Included
AM_ADV	AM_ADV AM_ALC	Included Included
AM_AGD	AM_ADV	Included
AM_ALC	AM_ADV	Included
AM_ATE	AM_ADV AM_AGD	Included Included
AM_AVA	AM_ADV AM_AGD	Included Included

Table 29 – Assurance measure dependencies

8.3.5 Mutually supportive and internally consistent rationale

This part shows that the IT security functions are complete and internally consistent by demonstrating that they are mutually supportive and provide an 'integrated effective whole'.
The interactions between security functions are limited to the dependencies between these security functions.

It is the same for assurance measures.

8.4 PP CLAIMS RATIONALE

This security target presents threats, assumptions, objectives, assurance measures and functional requirements.
This security target is compliant to the Protection Profile [PP eHC].
In addition, it is based on the Protection Profile [PP SSCD3], but without claiming formal compliance to it.

The strength of function claimed is high, and the claimed level is EAL4 + as required by the based PPs. The IC security functions used by the platform also claim high level and the used IC is compliant to level EAL5+.

9. STATEMENT OF COMPATIBILITY BETWEEN COMPOSITE ST AND PLATFORM ST

9.1 SECURITY FUNCTIONS

The following table lists all security functions of the underlying Platform ST and shows the relevance for this Composite ST in the following terms:

- "**Transparent**": this SF is unconditionally provided by the platform, without any influence on or configuration by the ES. In effect this SF is simply present in the composite TOE, but because of its independence from the ES it is not considered elsewhere in the document.
- "**Signal**": this SF is implicitly provided by the platform without configuration by the ES, but giving a trigger signal for special ES reaction (usually an interrupt leading to ES halt).
- "**Utilized**": this SF is explicitly used by the ES as provided by the Platform, but without explicit configuration
- "**Configured**": This SF is explicitly used by the ES with special configuration.

The first column addresses specific security functionality of the underlying platform, which is assigned to Security Functions of the Composite ST in the second column. The last column provides additional information on the correspondence if necessary.

Platform TSF	Relevance for the Composite TOE	Reference / Remark
SEF1	Signal	
Operating State checking	SF1	Normally the hardware would fall into the so called "Security Reset". If, however, this feature is successfully attacked, the ES still reacts on the corresponding interrupt with a software halt.
SEF2	Transparent	
Phase management with test mode lock out	-	-
SEF3	Transparent	
Protection against snooping	-	-
SEF4	Transparent	
Data encryption and data disguising	-	-
SEF5	Configured	
Random number generation	SF_CRYPTO	The random number generation uses the hardware platform's TRNG according to the hardware guideline
SEF6	Utilized	
TSF self test	SF6	The ES frequently starts the test by calling a dedicate RMS routine.
SEF7	Configured	
Notification of physical attack	SF7	The ES fills and checks the shield pattern on a regular basis.
SEF8	Signal	
Memory management unit	SF_TSF_PROTECTION	The MMU is used for bank switching and restricting memory access during protocol operation (APDU transmission), but not for separation of memory areas or of system and user mode. Anyway, the ES reacts to a violation interrupt.
SEF9	Configured	
Cryptographic support	SF_CRYPTO	The ES uses the hardware accelerators for cryptographic computations. The library software provided by the hardware manufacturer is not used.

Table 30: Relevant Security Functions

9.2 Requirements

In the first column, the following table lists all relevant SFRs of the Platform ST.

Platform-SFR	Correspondence in Composite ST	Result
FPT_FLS.1	FPT_PHP.1 (SSCD application) FPT_PHP.3(SSCD application & eHC application)	Platform provides all appropriate means to manage case of abnormal environmental parameters and so an unambiguous detection of physical tampering
FPT_TST.2		
FPT_PHP.3		
FRU_FLT.2		
FDP_SDI.1		
FDP_SDI.2		
FDP_ACC.1		
FCS_RND.1	FCS_RND.1 (eHC application)	Platform provide TRNG evaluated as P2-class in [AIS31]
FCS_COP.1	FCS_COP.1(SSCD application & eHC application)	Platform provides hardware accelerators for cryptographic computations. But the TOE not used manufacturer library.
FDP_ACF.1 FMT_MSA.3 FMT_MSA.1 FMT_SMF.1	No correspondence	The MMU is not used not for separation of memory areas or of system and user mode. No contradiction to Composite-ST
FCS_CKM.1	No correspondence	The TOE not used manufacturer library. No contradiction to Composite-ST

9.3 Objectives

In the first column, the following table lists all relevant objectives for the TOE of the Platform ST. Corresponding objectives for the Composite TOE are assigned in the second column. The last column provides the result of the analysis for contradiction.

Platform-Objective	Corresponding Composite Objective	Result
TOE		
O.Phys-Manipulation	OT.Tamper_ID OT.Tamper_resistance OT.Prot_Phys_tamper OT.Prot_Inf_Leak	OT.Tamper-ID, OT_Tamper_resistance, OT.Prot_Phys_tamper and OT.Prot_Inf_Leak of the Composite TOE is supported by O.Phys-Manipulation of the HW by addressing the same objectives: protection against physical probing and tampering. No contradiction to Composite-ST.
O.Phys-Probing	OT.Tamper_ID OT.Tamper_resistance OT.Prot_Phys_tamper OT.Prot_Inf_Leak	OT.Tamper-ID, OT_Tamper_resistance, OT.Prot_Phys_tamper and OT.Prot_Inf_Leak of the Composite TOE is supported by O.Phys-Probing of the HW by addressing the same objectives: protection against physical probing and tampering. No contradiction to Composite-ST.
O.Malfunction	OT.Prot_Malfunction	OT.Prot_Malfunction of the Composite TOE is supported by O.Malfunction of the HW because they are nearly identical No contradiction to Composite-ST.
O.RND	OT.Cryptography	OT.Cryptography of the Composite TOE is supported by O.RND of the HW because OT.Cryptography include random generation No contradiction to Composite-ST.
O.Add-Functions	No correspondence	Platform provides the following specific security functionality to the Embedded Software: - *Area based Memory Access Control* - *Triple Data Encryption Standard (3DES),* - *Rivest-Shamir-Adleman (RSA)* But the ES not used these functionalities. No contradiction to Composite-ST.

9.4 Threat

In the first column, the following table lists all relevant threats of the Platform ST, those are all threats, that are traced to the relevant TOE security objectives. Corresponding threats are assigned in the second column. The last column provides the result of the analysis for contradiction.

Platform-Threat	Corresponding Composite Threats	Result
T.Phys-Manipulation	T.Hack_Phys T.Phys_Tamper T.Information_Leakage	T.Hack_Phys,T.Phys_Tamper and T.Information_Leakage of the Composite TOE address T.Phys-Manipulation No contradiction to Composite-ST.
T.Phys-Probing	T.Hack_Phys T.Phys_Tamper T.Information_Leakage	T.Hack_Phys,T.Phys_Tamper and T.Information_Leakage of the Composite TOE address T.Phys-Probing No contradiction to Composite-ST.
T.Malfunction	T.Malfunction	T.Malfunction of the Composite TOE nearly identical to T.Malfunction

Platform-Threat	Corresponding Composite Threats	Result
		No contradiction to Composite-ST.
T.RND	T.Forge_Internal_Data	T.Forge_Internal_Data of the Composite TOE addresses T.RND. No contradiction to Composite-ST.

9.5 Organisational Security Policies

In the first column, the following table lists relevant OSP of the Platform ST. Corresponding organisational policies is assigned in the second column. The last column provides the result of the analysis for contradiction.

Platform-OSP	Corresponding Composite Threats/OSPs	Result
P.Add-Functions	No correspondence	Platform provides the following specific security functionality to the Embedded Software: - *Area based Memory Access Control* - *Triple Data Encryption Standard (3DES),* - *Rivest-Shamir-Adleman (RSA)* But the ES not used these functionalities. No contradiction to Composite-ST.

9.6 Operational Environment

No assumption from the hardware-ST can be rated as “significant”.

10. ABBREVIATIONS

Name	Definition
AC	Access Conditions
ALR	Anomaly List Report
APC	Subsystem “APDU Container”
APDU	Application Protocol Data Unit
API	Application Programming Interface
APL	Acceptance Plan
ARGOS	Acceptance and Requirements for GEMALTO Organization System
ATM	Automatic Teller Machine
ATR	Answer To Reset
BLK	Module “Block”
CAR	Card Acceptance Report
CC	Common Criteria (referenced as CC)
CEPS	Common Electronic Purse Specifications
CGA	Certification generation application
CI	Configuration Item
CIS	Card Initialisation Specification
CLI	Command Line Interface
COS	Card Operating System
CM	Configuration Management
CMP	Configuration Mangement Plan
CMS	Configuration Management System
CSP	Certification-Service provider
CUD	Client User Document
DAR	DIL Acceptance Report
DESCRY	Module “DES-crypto”
DF	Dedicated File
DIL	Dual In Line
DTBS	Data to be signed
EAL	Evaluation Assurance Level
EC	Electronic Cash
EEPROM	Electrically Erasable and Programmable Read Only Memory
EF	Elementary File
eGK	elektronische Gesundheitskarte
eHC	electronic Health Card
EMV	Europay-Mastercard-Visa
ERR	Subsystem “Error Handling”
ES	Embedded Software
FRS	Functional Requirement Specifications
FS	Subsystem “File System”
HAL	Subsystem “Hardware Abstraction Layer”
HBCI	HomeBanking Computer Interface
HEC	Health Employee Card (technically a type of HPC)
HSH	Module “Hash”
HSM	Hardware Security Module
HPC	Health Professional Card
IC	Integrated circuit
ID	Identifier
IFD	Interface device
INS	Instruction code
I/O	Input/Output
IT	Information Technology
IUD	Internal User Documentation
LRC	Longitudinal Redundancy Checksum

MAC	Message Authentication Code
MAR	Mask Acceptance Report
MF	Master File
OS	Operating System
OSP	Operational Security Policy
OSP.***	Naming convention for organizational security policies in this PP, e. g. OSP.User_Information
OT.***	Naming convention for security objectives for the TOE in this PP, e. g. OT.Access_Rights
PIN	Personal Identification Number (authentication feature)
PKI	Public Key Infrastructure
PL	Project Leader
PP	Protection Profile
PROC	Subsystem “Process Handling”
PUC	PIN Unblocking Code
PUK	Pin Unblocked Key
PVCS	Product Version Control System
RAD	Reference Authentication Data
RAM	Random Access Memory
ROM	Read Only Memory
SAR	Security assurance requirements
RSA	Rivest Shamir Adleman (algorithm)
SCA	Signature-creation application
SCD	Signature-creation data
SCM	Software Configuration Management
SCMA	Software Configuration Management Administrator
SCU	Smart Card Utility
SDD	Software Design Description
SDD1	Preliminary Software Design Description
SDD2	Detailed Software Design Description
SDO	Signed Data Object
SF	Security Function
SFP	Security Function 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 and used by access control SFRs
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMS	Software Masking Specification
SOF	Strength Of Function
SSCD-PP	Secure Signature Creation Device Protection Profile
SK	Subsystem “Security Kernel”
SM	Module “secure messaging”
SMC	Security Module Card
ST	Security Target
SSCD	Secure signature-creation device
SVA	Software Validation Approval
TBX	Subsystem “Toolbox”
TDM	Technical Data Management
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
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UART	Universal Asynchronous Receiver Transmitter

UTP	Unitary Test Plan
UTR	Unitary Test Report
VAD	Verification authentication data
VCC	Voltage at the Common Collector
VLR	Validation Review
VTP	Validation Test Plan
VTP1	Preliminary Validation Test Plan
VTP2	Detailed Validation Test Plan
VTR	Validation Test Report
VTS	Validation Test Specification
X.509	A certificate format

Table 31 – Abbreviation table

11. GLOSSARY

The glossary elements for this development project are given in the table below:

Administrator means an user that performs TOE initialisation, TOE personalisation, or other TOE administrative functions.

Advanced electronic signature (defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control, and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Archive. PVCS or VSS file which contains the evolution history of a work file. PVCS or VSS is able to rebuild any revision of the work file. Historical information includes description of changes, who made them, and when they were made. The archive also contains information about the status and attributes of the archive and its associated work file

Authentication data is information used to verify the claimed identity of a user.

Branch. Separate line of development consisting of one or more revisions that diverge from a revision on the trunk or from another development branch

CEN workshop agreement (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN). This Protection Profile (PP) represents Annex A to the CWA that has been developed by the European Electronic Signature Standardization Initiative (EESSI) CEN/ISSS electronic signature (E-SIGN) workshop, Area F on secure signature-creation devices (SSCD).

Certificate means an electronic attestation which links the SVD to a person and confirms the identity of that person. (defined in the Directive [1], article 2.9)

Certification generation application (CGA) means a collection of application elements which requests the SVD from the SSCD for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair by the SSCD, if the requested SVD has not been generated by the SSCD yet. The CGA verifies the authenticity of the SVD by means of

(a) the SSCD proof of correspondence between SCD and SVD and
(b) Checking the sender and integrity of the received SVD.

Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. (defined in the Directive [1], article 2.11)

Check-In. Action of storing a new revision in an archive.

Check-Out. Action of getting a revision from an archive. Then the archive is locked, and can be modified to do another revision.

Component. The hardware component of the Operating System.

Data to be signed (DTBS) means the complete electronic data to be signed (including both user message and signature attributes).

Data to be signed representation (DTBS-representation) means the data sent by the SCA to the TOE for signing and is

a hash-value of the DTBS or
an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or
the DTBS.

The SCA indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.

Directive The Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] is also referred to as the 'Directive' in the remainder of the PP.

Evolution Index (VSS). Symbolic reference used to uniquely identify a preliminary software version.

Evolution Index (PVCS). This number (integer) is used to uniquely identify a software version. Take note that the EI is different from the revision number that is automatically generated by PVCS.

Filter. A set of bug fixes and adjustments of the ROM code, residing in EEPROM

Folder (VSS/PVCS). A folder enables to organise archives in the Version Manager MMI. It logically links some archives

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 an integrated circuit.

Label. Symbolic name assigned to a revision in one or more archives. Labels provide a convenient way to refer to several archives with different revisions by a single name

Mask. Software developed by GEMALTO to be implemented in the chip

Module. Subset of commands and/or mechanisms. A module groups several routines allowing a logical function. A module cannot be broken up. Most of the time, a module will contain only one source file in the OS referential while it may involve several tests in the Test referential. [examples of modules for the Administrative Kernel brick are Record, Authentication, Secure Messaging, ...]

Mutual Authentication. Type of those cryptographic protocols, were two entities mutually verify the authenticity of each other, for smart cards this is realized by suitable sequences of amt card commands and responses

Personalisation. The process by which personal data are brought into the TOE before it is handed to the card holder

Product. Set of modules that constitute a final mask or a final filter (final release)

Project. See VSS/PVCS project

Qualified certificate means a certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1]. (defined in the Directive [1], article 2.10)

Qualified electronic signature means an advanced signature which is based on a qualified certificate and which is created by a SSCD according to the Directive [1], article 5, and paragraph 1.

Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.

Referential. Set of software components which are used by several Teams such as the OS software or the Test environment. The Referential contains all the archives of a project

Revision. Particular iteration of a work file in an archive. Each time a work file is modified and checked back into the archive, VSS/PVCS creates a new revision and assigns it automatically a new revision number

Rule_*. Naming convention for access control rules in this PP, defined in SFP_access_rules.

Secure Channel. A connection between two devices, which is secured against interception or modification of the transmitted data. The TOE realizes a secure channel to other devices using secure messaging.

Secure signature-creation device (SSCD) means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive [1]. (SSCD is defined in the Directive [1], article 2.5 and 2.6).

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)

Signatory means a person who holds a SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. (defined in the Directive [1], article 2.3)

Signature attributes means additional information that is signed together with the user message.

Signature-creation application (SCA) means the application used to create an electronic signature, excluding the SSCD. I.e., the SCA is a collection of application elements 1. to perform the presentation of the DTBS to the signatory prior to the signature process according' to the signatory's decision, 2. to send a DTBS-representation to the TOE, if the signatory indicates by specific non-misinterpretable input or action the intend to sign, 3. to attach the qualified electronic signature generated by the TOE to the data or provides the qualified electronic signature as separate data.
Signature-creation data (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. (defined in the Directive [1], article 2.4)
Signature-creation system (SCS) means the overall system that creates an electronic signature. The signature-creation system consists of the SCA and the SSCD.
Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (defined in the Directive [1], article 2.7)
Signed data object (SDO) means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.
Sub-Referential. Consistent set of software components (Example: test scripts, specification documents,). A Sub-referential belongs to a Referential.
SSCD provision service means a service that prepares and provides a SSCD to subscribers.
Tip Revision. The latest revision of a line of development (the trunk or a branch)
TSF data. Data created by and for the TOE, that might affect the operation of the TOE
User means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data. Data created by and for the user, that does not affect the operation of the TSF
Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics.
VSS/PVCS Project. Logical set of folders and archives
Work File. Copy of an archive revision, usually for working with it on a local PC. If the archive is "checked out" this copy can be modified and "checked in" again as the new revision of the archive.
Work File Directory. Local folder to hold the archive copies generated by "Check Out" or "Get" actions (in German: "Auscheckordner"). A folder in VSS must be linked to a work file directory, so that "Get" actions can be performed.

Table 32 – Glossary table

12. REFERENCES

The documents and reference elements for this development project are given in the table below:

Reference	Title of document	Author
Common Criteria Documents		
CCPART1	Common Criteria for Information Technology Security Evaluation. Part 1: Introduction & general model, CCMB-2005-08-001. Version 2.3. August 2005.	Common Criteria Project Sponsoring Organizations
CCPART2	Common Criteria for Information Technology Security Evaluation. Part 2: Functional security requirements, CCMB-2005-08-001. Version 2.3. August 2005.	Common Criteria Project Sponsoring Organizations
CCPART3	Common Criteria for Information Technology Security Evaluation. Part 3: Assurance security requirements, CCMB-2005-08-001. Version 2.3. August 2005.	Common Criteria Project Sponsoring Organizations
CEM	Common Methodology for Information Technology Evaluation, CCMB-2005-08-004. Version 2.3. August 2005.	Common Criteria Project Sponsoring Organizations
AIS 34	Evaluation Methodology for CC Assurance Classes for EAL5+, Version 1.00 as of 01 June 2004	BSI
AIS 36	Composite product evaluation for Smart Cards and similar devices, Version 1, Rev 1, September 2007, CCDB-2007-09-001	Common Criteria
AAPSC	Application of Attack Potential to Smartcards, Version 2.7, February 2009	Common Criteria Project Sponsoring Organizations
AMSRP	Attack Methods for Smartcards and Similar Devices, Version 1.5, February 2009	Common Criteria Project Sponsoring Organizations
ETR_Lite Annex A	ETR-lite for composition: Annex A Composite smartcard evaluation : Recommended best practice, Version 1.2, March 2002	Common Criteria Project Sponsoring Organizations
PP SSCD1	Protection Profile Secure Signature-Creation Device CWA 14169:2002(E) Annex A, Version 1.05, April 02	ESIGN-Workshop Area F
PP SSCD2	Protection Profile Secure Signature-Creation Device CWA 14169:2002(E) Annex B, Version 1.05, April 02	ESIGN-Workshop Area F
PP SSCD3	Protection Profile Secure Signature-Creation Device CWA 14169:2002(E) Annex C, Version 1.05, April 02	ESIGN-Workshop Area F
PP eHC	**The Protection profile - "Electronic Health Card (eHC)" rev 2.60 29/07/2008**	BSI
EMV-CPS	EMV card personalisation specification, Version 1.0, June 2003.	EMV
Chip Documents		
ST IC	Security Target for SLE66CX680PE with RSA2048 /– Version 1.3– 22/03/2007	Infineon Technologies AG
CER IC	Certification report for SLE66CX680PE with RSA 2048– 27/05/2008 BSI-DSZ-CC-0437-2008	BSI
DB IC	SLE66CX680PE, Confidential Data Book 07.05	Infineon Technologies AG
ETR_Inf	EVALUATION TECHNICAL REPORT (ETR) Version: 1.3, Date: 26.07.2004,	TÜViT
RNG IC	SLE66CxxxPE / SLE66CxxxP , Testing the Random Number Generator – Application Note 09.00	Infineon Technologies AG
eHC Documents		
eHC spec part 1	The Specification of the German Electronic Health Card eHC Part 1 : Commands, Algorithms and Functions of the COS Platform Release 2.2.2, 16/09/2008	GEMATIK

eHC spec part 2	The Specification of the German Electronic Health Card eHC Part 2 : Applications and application related structures Release 2.2.1, 19/06/2008	GEMATIK
eHC spec part 3	The Specification of the German Electronic Health Card eHC Part 3 : Layout and physicam Properties Release 2.1.0, 20/12/2007	GEMATIK
SICCT	SICCT (28.2.2006): TeleTrusT, SICCT Secure Interoperable ChipCard Terminal, Version 1.0.0	
Reference	**Title of document**	**Author**
ISO Documents		
ISO C1	ISO 7816 – 3, Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics. 1997	
ISO C3	ISO 7816 - 3, Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols. 1997	ISO
ISO C4	ISO 7816 - 4, Identification cards - Integrated circuit(s) cards with contacts, Part 4: Inter-industry commands for interchange. 1995	ISO
ISO C4'	ISO 7816 - 4, Identification cards - Integrated circuit(s) cards with contacts, Part 4: Inter-industry commands for interchange, AMENDMENT 1: Impact of secure messaging on the structures of APDU messages. 1996	ISO
ISO C8	ISO 7816 - 8, Identification cards - Integrated circuit(s) cards with contacts, Part 8: Security related inter-industry commands. 1997	ISO
ISO C9	ISO 7816 - 9, Identification cards - Integrated circuit(s) cards with contacts	ISO
ISO HF3	ISO 10118 - 3, Information technology - Security techniques - Hash-functions, Part 3: Dedicated hash functions, 1998	ISO
DIN Documents		
DINSIG	Specification of chipcard interface with digital signature application/function acc. to SigG and SigV. DIN NI-17.4 Version 1.0 15.12.1998	DIN
DINSIG4	Chipcards with digital signature application/function according to SigG and SigV. Part 4: Basic Security Services. DIN V66291-4 Final Draft 07.06.2000	DIN
PKCS1	RSA Encryption Standard . Version 1.5 November 1, 1993	RSA Laboratories
Signature Ordinance Document		
ALGO	Notification in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance Published in Federal Gazette No 13, pp 346 of 27 January 2009 (in German)	Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway
ACT	Digital Signature Act of 16 May 2001, Federal Law Gazette IS. 876, 21 Mai2001	Federal Government
ORDI	Digital Signature Ordinance – SigV- 21 November 2001.	
European Directive Document		
DIRECTIVE	DIRECTIVE 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures.	EC

Nist Document		
FIPS	Federal Information Processing Standards Publication 46-3 (FIPS PUB 46-3) of U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology Data encryption standard (DES) – Reaffirmed 1999 October 25	NIST
Hash document		
RIPEMD	H. Dobbertin, A. Bosselaers, B. Preneel, RIPEMD-160: A strengthened version of RIPEMD, 1996	
Random generators		
AIS31	Functionality classes and evaluation methodology for true (physical) random number generators. Version 3.1, September 25, 2001. http://www.bsi.de/zertifiz/zert/interpr/trngk31e.pdf	

Table 33 – Reference table

<END OF DOCUMENT>