Document Administration

Recipient

Department	Name
secRnD_PAD	Secure e-Documents Research and Development, PADERBORN

For the attention of

Department	Name

Summary

The following document comprises the Security Target for a TOE evaluated according to Common Criteria Version 2.3. The TOE being subject of the evaluation is the smartcard product

MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0

from Sagem Orga GmbH. The IT product under consideration shall be evaluated according to CC EAL 4 augmented with a minimum strength level for the TOE security functions of SOF-high. The evaluation is based on the evaluation of the MICARDO V3.5 R1.0 eHC V1.0 without QES as listed under the certification ID BSI-DSZ-CC-0602 and BSI-DSZ-CC-0673.

Keywords

Electronic Health Card (EHC), Qualified Electronic Signature (QES),Target of Evaluation (TOE), Common Criteria, IC, Dedicated Software, Smartcard Embedded Software, Basic Software, Application Software, Security Objectives, Assumptions, Threats, TOE Security Function (TSF), TOE Security Enforcing Function (SEF), Level of Assurance, Strength of Functions (SOF), Security Functional Requirement (SFR), Security Assurance Requirement (SAR), Security Function Policy (SFP)

Responsibility for updating the document

Karsten Klohs karsten.klohs@morpho.com

Sagem ORGA GmbH (Morpho e-Documents)

MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0

ST-Lite

Document Id:	3MIC3EVAL.CSL.0010
Archive:	3
Product/project/subject:	MIC3EVAL (Micardo V3 Evaluierung)
Category of document:	CSL (ST-Lite)
Consecutive number:	0010
Version:	V1.00
Date:	26 May 2011
Author:	Karsten Klohs
Confidentiality:	

Checked report:	not applicable
Authorized (Date/Signature):	not applicable
Accepted (Date/Signature):	not applicable

Document Organisation

i Notation

None of the notations used in this document need extra explanation.

ii Official Documents and Standards

See Bibliography.

iii Revision History

Version	Type of change	Author / team
V1.00	Final sanitised version of the eHC v1.2+QESC v1.0 product conformant to Base Role-Out release 0.5.3 with updated reference to underyling IC/Crypto Library assurrance documents	Karsten Klohs

Table of Contents

1 ST Introduction

1.1 ST Identification

This Security Target refers to the smartcard product “MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0” (TOE) provided by Sagem Orga GmbH for a Common Criteria evaluation.

Title:	Security Target - MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0
Document Category:	Security Target for a CC Evaluation
Document ID:	Refer to Document Administration
Version:	Refer to Document Administration
Publisher:	Sagem Orga GmbH (Morpho e-Documents)
Confidentiality:	Refer to Document Administration
TOE:	“MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0” (Smartcard Product containing IC with Smartcard Embedded Software, including eHC Application and SIG Application, intended to be used within the German Health Care System)
Certification ID:	BSI-DSZ-CC-0604 (baseline)
IT Evaluation Scheme:	German CC Evaluation Scheme
Evaluation Body:	SRC Security Research & Consulting GmbH
Certification Body:	Bundesamt für Sicherheit in der Informationstechnik (BSI)

This Security Target has been built in conformance with Common Criteria V2.3.

1.2 ST Overview

Target of Evaluation (TOE) and subject of this Security Target (ST) is the smartcard product “MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0” developed by Sagem Orga GmbH.

The TOE is realised as Smartcard Integrated Circuit (IC with contacts) with Smartcard Embedded Software, consisting of the MICARDO Operating System platform and the dedicated electronic Health Card Application (eHC Application) and Signature Application (SIG Application) as intended to be used for the German Health Care System.

The TOE`s eHC Application and SIG Application are based on the MICARDO Operating System platform providing a wide range of functionality which can be employed for different applications. The MICARDO platform is designed as multifunctional platform for high security applications. The Operating System platform allows for an integration of a variety of applications, in particular in the following fields: Health Systems, ID Systems, Signature Applications with and without on-card signature key pair generation, Banking Systems, Loyalty Schemes.

In particular, the TOE´s platform and its technical functionality and inherently integrated security features are designed and developed under consideration of the following specifications, standards and requirements:

- Functional and security requirements defined in the specification /eHC1/ and /eHC2/ for the electronic Health Card (eHC) as employed within the German Health Care System.
- Functional and security requirements drawn from the EU Directive on electronic signatures /ECDir/, the German Signature Act /SigG01/, the German Signature Ordinance /SigV01/ and the catalogue of agreed cryptographic algorithms /ALGCAT/.
- Requirements from the Protection Profiles /BSI_PP_IC/, /PP_eHC/, /PP_SSCD_T3/
- Technical requirements defined in /ISO 7816/, Parts 1, 2, 3, 4, 8, 9, 15

The TOE is intended to be used as electronic Health Card (eHC) within the German Health Care System as specified in /eHC1/ and /eHC2/. MICARDO

Furthermore, the variante of the TOE described in this ST is intended to be used as Secure Signature-Creation Device (SSCD) for qualified electronic signatures in view of the European Directive 1999/93/EC on electronic signatures /ECDir/, the German Signature Act /SigG01/ and the German Signature Ordinance /SigV01/. The EU compliant SIG Application of the TOE is implemented according to the requirements in /eHC2/, chap. 8 and is explicitly designed for the generation of legally binding qualified electronic signatures as defined in /ECDir/, /SigG01/ and /SigV01/.

The functional and assurance requirements and components for SSCDs as defined in /ECDir/ Annex III, /SigG01/, and /SigV01/ are mapped to three different Protection Profiles, each of it corresponding to a dedicated type of SSCD. The Sagem Orga GmbH product is designed as SSCD of the so-called Type 3, i.e. as device with *oncard* - generation of the Signature-Creation Data / Signature-Verification Data (SCD/SVD key pair), the secure storage of the SCD/SVD key pair and the secure creation of electronic signatures by using the dedicated SCD key. Hence, the Security Target for the TOE resp. its SIG Application is based on the related Protection Profile /PP_SSCD_T3/.

Note: The TOE explicitly does not implement a Signature-Creation Application (SCA).

The CC evaluation and certification of the TOE against the present ST also serves for the security certificate as it is required for the confirmation of the TOE as SSCD according to /ECDir/ and /SigG01/ (in German: Bestätigung nach EU Direktive bzw. Signaturgesetz). Furthermore, the security certificate for the TOE contributes as necessary and essential part to the so-called prescribed licence of the TOE as technical component eHC for usage within the German Health Care System.

Under technical view, the TOE comprises the following components:

- Integrated Circuit (IC) with Crypto Library "NXP SmartMX P5CC080V0B Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software" provided by NXP Semiconductors GmbH
- Smartcard Embedded Software comprising the MICARDO V3.5 Operating System platform (designed as native implementation)
- the dedicated eHC Application
- and the dedicated SIG Application. The SIG Application in this product variant (QES komplettierbar) features a completion mechanism which can install the qualified certificate for the signature key pair *after* the personalisation phase. The TOE provides appropriate security functions to ensure that the signature application is not usable until the SIG Application has been completed by a trusted certification service provider.

1.3 CC Conformance

The CC evaluation of the TOE is based upon

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 2.3, August 2005 (/CC 2.3 Part1/)
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 2.3, August 2005 (/CC 2.3 Part2/)
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 2.3, August 2005 (/CC 2.3 Part3/)

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 2.3, August 2005 (/CEM 2.3/)

This Security Target is written in accordance with the above mentioned Common Criteria Version 2.3 and claims the following CC conformances:

- Part 2 extended
- Part 3 conformant
- conformant to the Protection Profile “electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK)” (/PP_eHC/)

Furthermore, the Security Target takes into account the contents of the Protection Profile /PP_SSCD_T3/.

The Security Target for the TOE covers all essential aspects and contents of /PP_SSCD_T3/. Only the following content related differences arise:

- Communication between the TOE and the external Signature-Creation Application (SCA):

  The establishment of a trusted channel resp. trusted path for the communication between the TOE and a SCA for a secure transmission of the data to be signed (DTBS) resp. of the verification authentication data (VAD) as required within /PP_SSCD_T3/ is now specified as optional. In the case that a trusted channel resp. trusted path is not used the cardholder resp. signatory is responsible for establishing a trusted environment for the communication between the TOE and the SCA.

  This extension is necessary as TOEs with mandatory use of trusted channels and trusted paths can only be used by SCAs resp. interface devices supporting trusted channels and trusted paths and would be in particular unusable for any other type of interface devices.

- Personalisation Phase of the TOE´s dedicated SIG Application:

  Related to the personalisation of the TOE´s SIG Application additional aspects concerning assets, assumptions, threats, security policies, security objectives and security functional requirements are appropriately added.

- Completion of the dedicated SIG Application:

  Related to the completion of the TOE's SIG Application additional aspects concerning assets, assumptions, threats, security policies, security objectives, and functional requirements are added.

The chosen level of assurance for the TOE is **EAL 4 augmented**. The augmentation includes the assurance components ADV_IMP.2, ATE_DPT.2, AVA_MSU.3 and AVA_VLA.4.

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

In order to avoid redundancy and to minimize the evaluation efforts, the evaluation of the TOE will be conducted as a delta evaluation of the CC-certified smartcard product "MICARDO V3.5 R1.0 eHC V1.0" from Sagem Orga GmbH (Certification ID BSI-DSZ-CC-0602).

Hint: The CC evaluation of the smartcard product "MICARDO V3.5 R1.0 eHC_v1.0" itself has been performed as a composite evaluation with re-usage of the evaluation results of the CC evaluation of the underlying semiconductor and related Crypto Library "NXP SmartMX P5CC080V0B Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software" provided by NXP Semiconductors GmbH. The IC incl. its IC Dedicated Software is evaluated according to Common Criteria EAL 5 augmented with a minimum strength level for its security functions of SOF-high and is covered by the certification reports /BSI_CC_IC/ (IC family) and /BSI_CC_ICCL/ (Crypto-Library). The evaluation of the IC is based on the Protection Profile /BSI_PP_IC/.

2 TOE Description

2.1 TOE Definition

2.1.1 Overview

The Target of Evaluation (TOE) is the smartcard product “MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0” (eHC for short in the following) intended to be used as electronic Health Card (eHC) in the German Health Care System.

In technical view the eHC is realised as a proprietary operating system with an Application Layer directly set-up on this operating system layer.

The eHC is based on the microcontroller with Crypto Library "NXP SmartMX P5CC080V0B Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software" provided by NXP Semiconductors GmbH. The IC incl. its Dedicated Software is evaluated according to Common Criteria EAL 5 augmented with a minimum strength level for its security functions of SOF-high (refer to /BSI_CC_IC/ and /BSI_CC_ICCL/).

Roughly spoken, the TOE is composed from the following parts:

- Integrated Circuit (IC) with its proprietary IC Dedicated Software (TOE-IC)
- Smartcard Embedded Software (TOE-ES) consisting of
  - Basic Software (TOE-ES/BS)
  - Application Software (TOE-ES/AS)

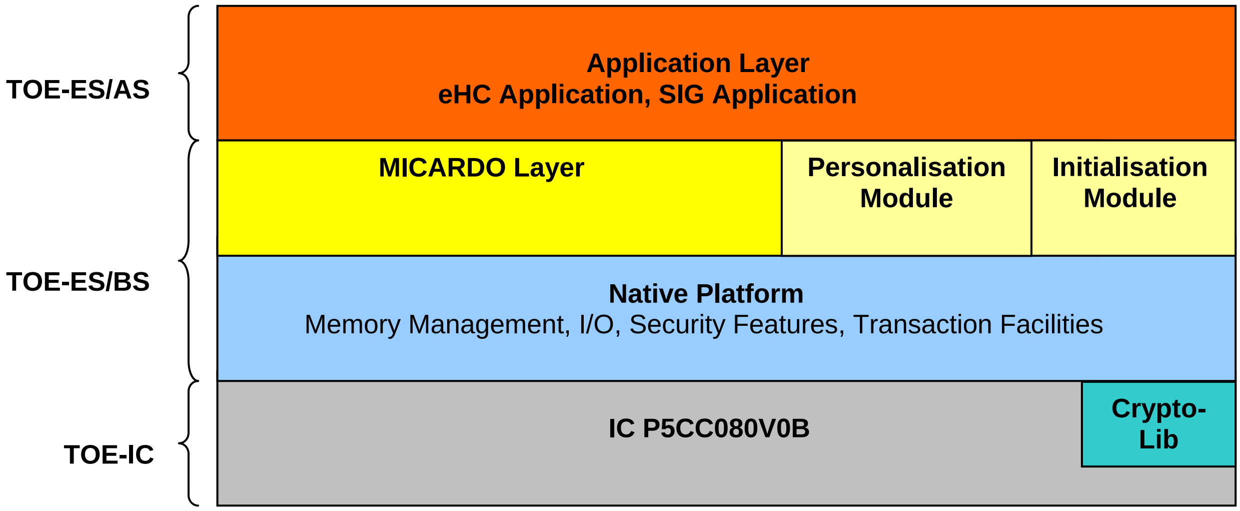
While the Basic Software consists of the MICARDO V3.5 Operating System platform of the TOE (realised as native implementation), the Application Software covers the Application Layer which is directly set-up on the MICARDO V3.5 Operating System platform and implements the specific eHC Application and SIG Application. The two pre-defined applications belonging to the TOE comprise own dedicated file and data systems with dedicated security structures, i.e. with application specific access rights for the access of subjects to objects and with application specific security mechanisms and PIN and key management. The design and implementation of the TOE´s dedicated eHC Application and SIG Application and their security structure follow the requirements in the specifications /eHC1/ and /eHC2/.

The eHC Application in the sense of this ST covers all elementary files at the MF-level, the DF.HCA, the DF.ESIGN, the DF.CIA.ESIGN as defined in /eHC2/ and further Sagem Orga specific files.

The SIG Application in the sense of this ST covers the DF.QES as defined in /eHC2/ and all elementary files at the MF-level which are accessed by the DF.QES as well as further Sagem Orga specific files.

Furthermore, the eHC itself offers the possibility to check its authenticity. For this purpose, the eHC contains the private part of a dedicated authentication key pair which depends on the configuration of the TOE and may be chosen customer specific (for more details see chap. 2.1.4.2).

The following figure shows the global architecture of the TOE and its components:



The different components of the TOE depicted in the figure above will be described more detailed in the following sections.

2.1.2 TOE Product Scope

The following table contains an overview of all deliverables associated to the TOE:

TOE component	Description / Additional Information	Type	Transfer Form
TOE-IC	NXP SmartMX P5CC080V0B Secure Smart Card Controller (incl. its IC Dedicated Software, covering in particular the Crypto Library)	HW / SW	Delivery of not-initialised / initialised modules or smart-cards Delivery of initialisation files in electronic form (if applicable)
TOE-ES/BS	Smartcard Embedded Software / Part Basic Software (implemented in ROM/EEPROM of the microcontroller)	SW	
TOE-ES/AS	Smartcard Embedded Software / Part Application Software (containing the eHC Application and SIG Application , implemented in the EEPROM of the microcontroller)	SW	
Note: The TOE will be delivered from Sagem Orga GmbH as not-initialised or initialised product (module / smartcard). To finalize the TOE as not-initialised product, the initialisation file developed by Sagem Orga GmbH must be loaded during the initialisation phase by the Initialiser (Sagem Orga GmbH or other initialisation facility).			
User Guide / User of the MICARDO platform	User guidance for the User of the MICARDO Operating System platform	DOC	Document in paper / electronic form
User Guide /	User guidance for the User of the eHC Card (in	DOC	Document in paper /

TOE component	Description / Additional Information	Type	Transfer Form
User of the eHC Card	particular, eHC Application and SIG Application)		electronic form
User Guide / Initialiser of the eHC Card	User guidance for the Initialiser of the eHC Card	DOC	Document in paper / electronic form
User Guide / Personaliser of the eHC Card	User guidance for the Personaliser of the eHC Card (in particular, eHC Application and SIG Application)	DOC	Document in paper / electronic form
Identification Data Sheet of the eHC Card	Data Sheet with information on the actual identification data and configuration of the eHC Card delivered to the customer	DOC	Document in paper / electronic form
Aut-Key of the eHC Card	Public part of the authentication key pair relevant for the authenticity of the eHC Card Note: The card´s authentication key pair is generated by Sagem Orga GmbH and depends on the TOE´s configuration delivered to the customer. Furthermore, the key pair may be chosen customer specific.	KEY	Document in paper form / electronic file
Pers-Key of the eHC Card	Personalisation key relevant for the personalisation of the eHC Card (pair of keys used for encryption and MAC respectively) Note: The card´s personalisation key pair is generated by Sagem Orga GmbH and depends on the TOE´s configuration delivered to the customer. Furthermore, the key may be chosen customer specific.	KEY	Document in paper form / electronic file

Note: Deliverables in paper form require a personal passing on or a procedure of at least the same security. For deliverables in electronic form an integrity and authenticity attribute will be attached.

2.1.3 Integrated Circuit (IC) with its Dedicated Software

Basis for the TOE´s Smartcard Embedded Software is the microcontroller with Crypto Library "NXP SmartMX P5CC080V0B Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software". The microcontroller and its Dedicated Software are developed and produced by NXP Semiconductors GmbH (within phase 2 and 3 of the smartcard product life-cycle, see chap. 2.2).

Detailed information on the IC Hardware, the IC Dedicated Software (in particular the Crypto Library) and the IC interfaces can be found in /ST_IC/ and /ST_IC_CL/.

2.1.4 Smartcard Embedded Software

The Smartcard Embedded Software of the TOE comprises the MICARDO V3.5 Operating System platform and applications running on this platform and is therefore divided into two parts with specific contents:

- Basic Software (MICARDO V3.5 Operating System platform)

- Application Software (Application Layer with dedicated eHC Application and SIG Application)

Each part of the Smartcard Embedded Software is designed and developed by Sagem Orga GmbH in phase 1 of the smartcard product life-cycle (see chap. 2.2). Embedding of the Smartcard Embedded Software into the TOE is performed in the later phases 3 and 5.

The main parts of the Basic Software are brought into the card by the IC manufacturer in form of the ROM mask and stored in the User-ROM of the IC (phase 3). The Application Software, and perhaps additional parts of the Basic Software, are located in the EEPROM area and are lateron loaded by specific initialisation routines of the TOE (phase 5). Hereby, the loading requires an encrypted and with a cryptographic checksum secured initialisation file. The necessary keys for securing the initialisation process are stored inside the IC during production time.

2.1.4.1 Basic Software

The Basic Software of the Smartcard Embedded Software comprises the MICARDO V3.5 Operating System platform of the TOE. Its main and security related parts are stored in the User-ROM of the underlying IC and are brought into the smartcard in form of the so-called ROM mask during the production process of the IC within phase 3 of the smartcard product life-cycle (see chap. 2.2).

The MICARDO V3.5 Operating System platform of the TOE is designed as proprietary software consisting of two layers. In detail, the integral parts of the TOE´s operating system consist of the MICARDO Layer and the Initialisation Module. Both are based on a Native Platform which serves as an abstraction layer towards the IC. On the other side, the MICARDO Layer and the Initialisation Module provide an interface between the operating system and the overlying Application Layer with the dedicated eHC Application and SIG Application.

The MICARDO Layer implements the executable code for the card commands and all general technical and security functionality of the MICARDO V3.5 Operating System platform as data objects and structures, file and object handling, security environments, security resp. cryptographic algorithms, key and PIN management, security states, access rules, secure messaging etc.

As mentioned, the Native Platform of the TOE´s operating system serves as an abstraction layer between the MICARDO Layer resp. the Initialisation Module and the IC. For this task, it provides essential operating system components and low level routines concerning memory management, I/O handling, transaction facilities, system management, security features and cryptographic mechanisms.

For the cryptographic features, the Native Platform makes use of a specific module, the Crypto Library, which supports and implements the TOE´s core cryptographic functionality. The Crypto Library is provided as IC Dedicated Support Software by the underlying IC. In view of the Smartcard Embedded Software, the Crypto Library is accessible only via the Native Platform.

For the initialisation process of the TOE conducted within phase 5 of the smartcard product life-cycle (see chap. 2.2) the operating system of the TOE puts dedicated initialisation routines at disposal which are solely accessible during the initialisation phase and which are realised within the Initialisation Module. After the initialisation has been successfully completed these commands are no longer available. Furthermore, the functionality of deleting the complete initialisation file after the initialisation (deletion of the whole EEPROM area) is disabled for the TOE.

The Initialisation Module puts the following features at disposal:

- specific initialisation routines
- specific test routines for the EEPROM area

Loading of an initialisation file is only possible by use of the TOE´s specific initialisation routines. Hereby, the initialisation file to be loaded has to be secured before with an encryption and a cryptographic checksum, both done with dedicated keys of the TOE.

The test routines for the EEPROM area can be used for a check of the correct functioning of the memory.

Furthermore, the Initialisation Module manages the specific states of the TOE´s operating system according to specified and unalterable rules.

In order to support the personalisation process the MICARDO V3.5 Operating System contains a personalisation module. This module provides a dedicated set of personalisation commands. These commands are only available after successful authentication with the personalisation key and are restricted to modify data intended for personalisation. Furthermore, the personalisation modules allows for the establishment of a trusted channel to secure the transfer of confidential data to the card. The personalisation commands are permanently disabled after successful personalisation.

2.1.4.2 Application Software

The Application Software part of the TOE´s Smartcard Embedded Software comprises the Application Layer and is directly set-up on the TOE´s Basic Software. It consists of the TOE´s dedicated eHC Application and SIG Application which are implemented according to the requirements in /eHC1/ and /eHC2/.

The Application Software will be brought into the smartcard in cryptographically secured form during the initialisation process within phase 5 of the smartcard product life-cycle (see chap. 2.2). The initialisation process uses the specific initialisation routines of the TOE´s operating system, and the Application Software will be stored in the EEPROM area of the IC.

The eHC offers the capability to check its authenticity. For this purpose, the TOE contains the private part of a dedicated RSA authentication key pair over which by an internal authentication procedure the authenticity of the eHC can be proven. The authentication key pair depends on the Initialisation File (containing the Application Software to be initialised) and its configuration and may be chosen customer specific. The corresponding public part of the authentication key pair is delivered through a trusted way to the external world.

Furthermore, the TOE contains a data area for storing identification data of the TOE and its configuration. The data area will be filled in the framework of the initialisation of the TOE with a specific operating system command and can be read out with a further specific operating system command. Once the identification data have been written, there is afterwards no change possible.

2.1.4.3 TOE´s SIG Application

The product variant which forms the TOE is a Secure Signature-Creation Device (SSCD Type 3) in view of the EU Directive /ECDir/ on electronic signatures.

The TOE as SSCD is configured software and hardware used to implement the Signature-Creation Data (SCD) and to guarantee for the secure usage of the SCD.

The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures:

1. Generation of the SCD and the correspondent Signature-Verification Data (SVD)
2. Creation of qualified electronic signatures
   a. after allowing for the data to be signed (DTBS) to be displayed correctly where the display function has to be provided by an appropriate environment
   b. using appropriate hash functions that are, according to /ALGCAT/, agreed as suitable for qualified electronic signatures
   c. after appropriate authentication of the signatory by the TOE
   d. using appropriate cryptographic signature functions that employ appropriate cryptographic parameters agreed as suitable according to /ALGCAT/.

The TOE includes an automatic preceding destruction of the old SCD prior to the generation of the new SCD/SVD pair.

The TOE implements all IT security functionality which is necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control. The user authenticates himself by supplying the verification authentication data (VAD) to the TOE which compares the VAD against the reference authentication data (RAD) securely stored inside the TOE. The TOE implements IT measures to support a trusted path to a trusted human interface device that can optionally be connected via a trusted channel with the TOE.

The TOE does not implement the Signature-Creation Application (SCA) which presents the data to be signed (DTBS) to the signatory and prepares the DTBS-representation the signatory wishes to sign for performing the cryptographic function of the signature. This ST assumes the SCA as environment of the TOE.

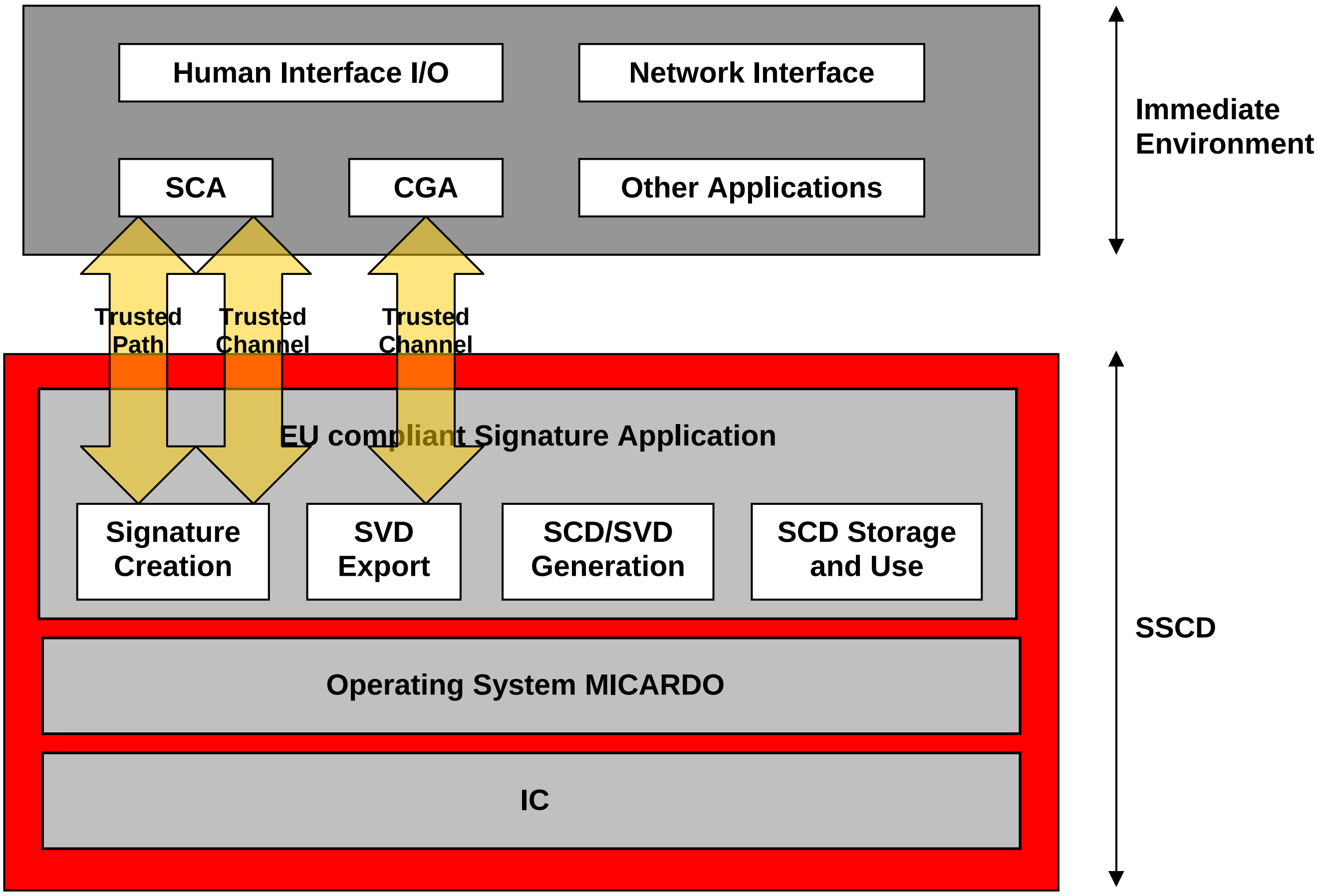
The TOE protects the SCD during the whole life-cycle as to be solely used in the signature-creation process by the legitimate signatory. The TOE as SSCD of Type 3 generates the signatory´s SCD oncard and serves for a secure storage of this data. The initialisation and personalisation of the TOE for the signatory´s use in the sense of the Protection Profile /PP_SSCD_T3/ include:

1. Generation of the SCD/SVD pair
2. Personalisation for the signatory by means of the signatory’s verification authentication data (VAD).

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the Certification-Service-Provider (CSP).

From the structural perspective, the TOE as SSCD comprises the underlying IC, the MICARDO V3.5 Operating System platform and the dedicated SIG Application with SCD/SVD generation, SCD storage and use, SVD export, and the signature-creation functionality. The SCA and the CGA (beside other applications within the German Health Care System) are part of the immediate environment of the TOE. They may communicate with the TOE over a trusted channel, a trusted path for the human interface provided by the SCA, respectively. In case a trusted channel or trusted path is not established with cryptographic means the TOE shall only be used within a Trusted Environment.

The following figure points the structural view of the TOE as SSCD and its integration into the external world out:



2.1.4.4 TOE’s SIG Application Completion Mechanism

The product variant “QES komplettierbar” differs from the product variant “QES” because the signature application is prepared only during the personalisation phase of the TOE but not operational – i.e. it is not possible to create qualified electronic signatures before completion of the SIG application. Therefore, we distinguish two different states of the SIG application

- the *transport state*, when the SIG application is prepared but not operational
- the *operational state*, when the SIG application is able to create qualified electronic signatures according to the requirements of /PP_SSCD_T3/ and in the sense of Section 2.1.4.3

The TOE provides a mechanism to complete the SIG Application after personalisation by the installation of a qualified certificate for the signature key pair which is already present on the card. Additionally, the completion mechanism ensures that the signature application will be under sole control of the signatory after completion. This is vital, to fulfil the requirements of the directive /ECDir/, the German signature act /SigG01/, and the German signature ordinance /SigV01/. Furthermore, the TOE provides means to protect the signature creation mechanism from being used ahead of time.
In detail, the completion procedure ensures that:

- the certification-service provider can prove the authenticity of the signature verification data (SVD) (the public key of the signature key pair) supplied by the TOE
- only a trusted certification-service provider can complete the SIG Application
- the SIG application is unusable until completion
- the signatory's reference authentication data (RAD) are initialised in a way which ensures that the SIG application is under sole control of the signatory.
- the intialisation of the signatory's verification authentication data is done in a confidential way

The specification /eHC2/ (chapter 7.2) defines several ways to implement a secure completion of the SIG application. There are three different kinds of options:

1. different ways to establish a trusted channel between the certification service provider and the TOE
2. different ways to ensure the authenticity of the SVD
3. different ways to ensure that the SIG application is under sole control of the signatory after completion.

The TOE described in this ST explicitly does not support all of the various variants, but restricts itself to the approaches which

1. establish the trusted channel between the certification service provider and the TOE based on asymetric mutual authentification
2. ensure the authenticity of the SVD by communication over the established trusted channel
3. supports technical means to enable the certification service provider to ensurethat the initialisation of the RAD has been performed by the signatory.

It is important to note, that the task of completion mechanism is to install the qualified certificate for the public signature key, to enforce the change of the RAD by the signatory, and to activate the SIG application after successful completion. It is *not* the task of the completion mechanism to generate or transmit the signature creation data. In fact the signature key pair is already generated during the personalisation phase of the TOE in *exactly the same way* than it is generated for the MICARDO V3.5 R1.0 eHC V1.0 (QES) variant of the product where the SIG application is activated during the personalisation phase already.

2.2 TOE Life-Cycle

The smartcard product life-cycle of the TOE is decomposed into seven phases. In each of these phases different authorities with specific responsibilities and tasks are involved:

Phase		Description
Phase 1	**Smartcard Embedded Software Development**	The **Smartcard Embedded Software Developer (Sagem Orga GmbH)** is in charge of • the development of the Smartcard Embedded Software (Basic Software, Application Software) and • the specification of the IC initialisation and pre-personalisation requirements (though the actual data for the IC initialisation and pre-personalisation come from Phase 4, 5 resp. 6). The purpose of the Smartcard Embedded Software designed during phase 1 is to control and protect the TOE during phases 4 to 7 (product usage).The global security requirements of the TOE are such that it is mandatory during the development phase to anticipate the security threats of the other phases.
Phase 2	**IC Development**	The **IC Designer (NXP Semiconductors GmbH)** • 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 (only Basic Software) from the developer through trusted delivery and verification procedures. From the IC design, IC Dedicated Software and Smartcard Embedded Software, the **IC Designer (NXP Semiconductors GmbH)** • constructs the smartcard IC database, necessary for the IC photomask fabrication.
Phase 3	**IC Manufacturing and Testing**	The **IC Manufacturer (NXP Semiconductors GmbH)** is responsible for • producing the IC through three main steps: - IC manufacturing, - IC testing, and - IC pre-personalisation. The **IC Mask Manufacturer (NXP Semiconductors GmbH)** • generates the masks for the IC manufacturing based upon an output from the smartcard IC database.
Phase 4	**IC Packaging and Testing**	The **IC Packaging Manufacturer (Sagem Orga GmbH)** is responsible for

		• the IC packaging (production of modules) and • testing.
Phase 5	**Smartcard Product Finishing Process**	The **Smartcard Product Manufacturer (Sagem Orga GmbH or other initialisation facility)** is responsible for • the initialisation of the TOE (in form of the initialisation of the modules of phase 4 or complete smartcards) and • its testing. The smartcard product finishing process comprises the embedding of the (initialised) modules for the TOE and the card production what is done alternatively by **Sagem Orga GmbH or by the customer.** Final card tests only aim at checking the quality of the card production, in particular concerning the bonding and implantation of the modules.
Phase 6	**Smartcard Personalisation**	The **Personaliser / Card Management System** is responsible for • the smartcard personalisation and • final tests. The personalisation of the smartcard includes the printing of the (card holder specific) visual readable data onto the physical smartcard, and the writing of (card holder specific) TOE User Data and TSF Data into the smartcard.
Phase 7	**Smartcard End-Usage**	The **Smartcard Issuer** is responsible for • the smartcard product delivery to the smartcard end-user (card holder), and the end of life process. The **authorized personalisation agents** (card management systems) are allowed • to add data for a new application, modify or delete an eHC application, but not to load additional executable code. Functions used for this are specifically secured functions for this usage phase (for example the require card-to-card authentication and secure messaging). This functionality doesn't imply that the card can be switched back to an earlier life cycle stage. An authorized certification service provider is allowed • to complete the SIG Application by the installation of a qualified certificate which connects the identity of the card holder to the public key of the signature generation key pair present on the smardcard. The TOE is used as eHC by the smart card holder in the operational use phase.

Appropriate procedures for a secure delivery process of the TOE or parts of the TOE under construction from one development resp. production site to another site within the smartcard product life-cycle are established. This concerns any kind of delivery performed from phase 1 to 5, including:

- intermediate delivery of the TOE or parts of the TOE under construction within a phase,
- delivery of the TOE or parts of the TOE under construction from one phase to the next.

In particular, the delivery of the Crypto Library from NXP Semiconductors GmbH to Sagem Orga GmbH follows the dedicated secured delivery process defined in /ST_IC_CL/. The delivery of the ROM mask and the EEPROM pre-personalisation data from Sagem Orga GmbH to NXP Semiconductors GmbH is done by using the dedicated secured delivery procedure specified by NXP Semiconductors GmbH following the so-called NXP Order Entry Form P5CC080V0B.

The IC manufacturer NXP Semiconductors GmbH delivers the IC with its IC Dedicated Software and the ROM mask supplied by Sagem Orga GmbH at the end of phase 3 in form of wafers according to /UG_IC/, chap. 2.1, Delivery Method 2, bullet point 1. The IC Dedicated Test Software stored in the Test-ROM is disabled before the delivery of the IC and cannot be used in the following phases.

The FabKey procedure described in /UG_IC/, chap. 2.1, Delivery Method 2, bullet point 2 is replaced by the following procedure which provides at least equivalent security: The TOE´s operating system puts in the non-initialised status the command “Verify ROM” at disposal, with which a SHA-1 hash value over the complete ROM and data freely chosen by the external world can be generated. Prior to the initialisation of the IC, the authenticity of the IC with its ROM mask will be proven by using the functionality “Verify ROM” and comparing the new generated hash value over the ROM data and the data freely chosen with a corresponding external reference value which is accessible only for Sagem Orga GmbH .

With regard to the smartcard product life-cycle of the TOE described above, the different development and production phases of the TOE with its IC incl. its IC Dedicated Software and with its Smartcard Embedded Software (Basic Software, Application Software) are part of the evaluation of the TOE. Different ways for the delivery of the TOE are established:

- Delivery as initialised product:
  - The TOE is delivered at the end of phase 5 in form of complete cards, i.e. after the initialisation process of the TOE has been successfully finished, final card tests have been successfully conducted and the card production has been fulfilled.
  - Alternatively, the TOE is delivered within phase 5 in form of initialised and tested modules. In this case, the smartcard finishing process (embedding of the delivered initialised modules, final (card) tests) is task of the customer.
- Delivery as not-initialised product:
  - The TOE is delivered within phase 5 in form of not-initialised cards, i.e. the initialisation of the product and final (card) tests have to be performed by the Initialiser.
  - Alternatively, the TOE is delivered at the end of phase 4 in form of not-initialised modules. In this case, the product´s initialisation and the smartcard finishing process (embedding of the modules, final (card) tests) are task of the customer.

The completion of the qualified electronic signature application is part of the operational phase of the TOE. The fact that the completion process itself satisfies all requirements of /ECDir/, /SigG01/, and /SigV01/ has to be considered during the approval of the completion process according to the German signature law. However, the TOE as an initilialised and personalised product has to supply security functions which support both the completion process and the final usage phase of the completed signature application. Therefore, this security target considers the requirements imposed by /PP_SSCD_T3/ and is extended by additional security requirements for the completion procedure. In particular, the signature application in its uncompleted form ensures that a certification service provider can extract the public part of the signature key pair for the generation of a qualified certificate in a secure way. Furthermore, the signature application in its uncompleted form supports the certification service provider to activate the signature application under sole control of the signatory.

The consideration of these security requirements ensures that both the completion process and the completed signature application are capable to fulfil the requirements for the generation of qualified electronic signatures.

2.3 TOE Environment

Considering the TOE and its life-cycle described above, four types of environments can be distinguished:

- development environment corresponding to phase 1 and 2,
- production environment corresponding to phase 3 to phase 5,
- personalisation environment corresponding to phase 6,
- end-user environment corresponding to phase 7.

2.3.1 Development Environment

Phase 1 - Smartcard Embedded Software Development

To assure security of the development process of the Smartcard Embedded Software, a secure development environment with appropriate personnel, organisational and technical security measures at Sagem Orga GmbH is established.

Only authorized and experienced personnel which understands the importance and the rigid implementation of the defined security procedures is involved in the development activities.

The development process comprises the specification, the design, the coding and the testing of the Smartcard Embedded Software. For design, implementation and test purposes secure computer systems preventing unauthorized access are used. For security reasons the coding and testing activities will be done independently of each other.

All sensitive documentation, data and material concerning the development process of the Smartcard Embedded Software are handled in an appropriately and sufficiently secure way. This concerns both the transfer as well as the storing of all related sensitive documents, data and material. Furthermore, all development activities run under a configuration control system which guarantees for an appropriate traceability and accountability.

The Smartcard Embedded Software of the developer, more precise the Basic Software part dedicated for the ROM of the IC, is delivered to the IC manufacturer through trusted delivery and verification procedures. The Application Software and additional parts of the Basic Software are delivered in form of a cryptographically secured initialisation file as well through trusted delivery and verification procedures to the initialisation centre.

Phase 2 – IC Development

During the design and layout process only people involved in the specific development project for the IC have access to sensitive data. Different people are responsible for the design data of the IC and for customer related data. The security measures installed at NXP Semiconductors GmbH ensure a secure computer system and provide appropriate equipment for the different development tasks.

2.3.2 Production Environment

Phase 3 - IC Manufacturing and Testing

The verified layout data are provided by the developers of NXP Semiconductors GmbH directly to the wafer fab. The wafer fab generates and forwards the layout data related to the relevant photomask to the IC mask manufacturer (NXP Semiconductors GmbH).

The photomask is generated off-site and verified against the design data of the development before usage. The accountability and traceability is ensured among the wafer fab and the photomask provider.

The production of the wafers includes two different steps regarding the production flow. In the first step the wafers are produced with the fixed mask independent of the customer. After that step the wafers are completed with the customer specific mask and the remaining mask. The computer tracking ensures the control of the complete process including the storage of the semifinished wafers.

The test process of every die is performed by a test centre of NXP Semiconductors GmbH.

Delivery processes between the involved NXP Semiconductors GmbH sites provide accountability and traceability of the produced wafers. The delivery of the ICs from NXP Semiconductors GmbH to Sagem Orga GmbH is made in form of wafers whereby non-functional ICs are marked on the wafer.

Phase 4 – IC Packaging and Testing

For security reasons the processes of IC packaging and testing at Sagem Orga GmbH are done in a secure environment with adequate personnel, organisational and technical security measures.

Only authorized and experienced personnel which understands the importance and the rigid implementation of the defined security procedures is involved in these activities.

All sensitive material and documentation concerning the production process of the TOE is handled in an appropriately and sufficiently secure way. This concerns both the transfer as well as the storing of all related sensitive material and documentation. All operations are done in such a way that appropriate traceability and accountability exist.

Phase 5 - Smartcard Product Finishing Process

To assure security of the initialisation process of the TOE, a secure environment with adequate personnel, organisational and technical security measures at the Initialiser is established.

Only authorized and experienced personnel which understands the importance and the rigid implementation of the defined security procedures is involved in the initialisation and test activities.

The initialisation process of the TOE comprises the loading of the TOE´s Application Software and the remaining EEPROM-parts of the TOE´s Basic Software which have been specified, coded, tested and cryptographically secured in phase 1 of the product life-cycle. The TOE allows only the initialisation of the intended initialisation file with its Application Software and its parts of the Basic Software. For security reasons, secure systems within a separate network and preventing unauthorized access are used for the initialisation process.

The smartcard finishing process comprises the embedding of the modules and final card tests.

All sensitive documentation, data and material concerning the production processes of the TOE at Sagem Orga GmbH within phase 5 are handled in an appropriately and sufficiently secure way. This concerns both the transfer as well as the storing of all related sensitive documents, data and material. Furthermore, all operations run under a control system which supplies appropriate traceability and accountability.

At the end of this phase, the TOE is complete as smartcard and can be supplied for delivery to the personalisation centre for personalisation.

2.3.3 Personalisation Environment

Note: The phases from the end of phase 5 up to phase 7 in the smartcard product life-cycle are not part of the TOE development and production process in the sense of this Security Target. Information about the phases 6 and 7 are just included to describe how the TOE is used after its development and production.

Phase 6 - Smartcard Personalisation

Central task for the personaliser is the personalisation of the initialised product, i.e the loading of card resp. card holder specific data into the dedicated eHC Application and SIG Application already existing on the initialised card.

The personalisation process and its security depend directly on the access rules which have been initialised and which are explicitly enforced by the personalisation commands. Furthermore, the use of these commands requires a mutual authentification between the card and the personalisation unit. Additionally, this authentification establishes a trusted channel for the secured transfer of confidential personalisation data.

However, the establishment of a secure environment for the personalisation process with adequate personnel, organisational and technical security measures is in the responsibility of the personalisation centre itself. In particular, the personaliser is responsible for the set-up of a secure personalisation process and for taking into account the requirements and recommendations given in the TOE´s user guidance for the personaliser. The secure key management and handling of the cryptographic keys for securing the data transfer within the personalisation process (if applicable) and the secure handling of the personalisation data itself is task of the personalisation centre.

2.3.4 End-User Environment

Phase 7 – Smartcard End-usage

In the end-usage phase, the TOE is under control of the card holder, and the eHC Application with its file systems, objects and data residing on the card are used in their intended way in the German Health Care System. However, according to the card structure and the access rules set for the different objects, further card management activities (as e.g. deleting or adding applications, inserting further personalisation data) may be possible for authorised users.
The product variant (QES komplettierbar) which forms the TOE of this security target contains the SIG Application in deactived form after production. The TOE supplies a SIG Application completion mechanism which supports the installation of a qualified certificate and the activation of the SIG Application by a trusted certification service provider. This security target covers the security functional requirements for both the completion process as well as the security requirements of the activated SIG Application after completion.

2.4 TOE Intended Usage

Introducing information on the intended usage of the TOE is given within chap. 1.2. The present chapter will provide additional and more detailed information on the Operating System platform and on the eHC Application and SIG Application residing on the card at delivery time point.

In general, the MICARDO V3.5 Operating System platform is designed as multifunctional platform for high security applications. Therefore, the TOE provides an Operating System platform with a wide range of technical functionality and an adequate set of inherently integrated security features.

The MICARDO V3.5 Operating System platform supports the following services:

- Oncard-generation of RSA key pairs of high quality (with appropriate key lengths)
- Different signature schemes (based on RSA with appropriate key lengths and padding schemes)
- Different encryption schemes (based on DES and RSA with appropriate key lengths and padding schemes)
- Key derivation schemes
- PIN based authentication scheme
- Different key based authentication schemes (based on DES and RSA, with / without session key agreement)
- Hash value calculation
- Random number generation of high quality
- Calculation and verification of cryptographic checksums
- Verification of CV certificates
- Protection of the communication between the TOE and the external world against disclosure and manipulation (Secure Messaging)
- Protection of files and data by access control functionality
- Life-cycle state information related to the Operating System itself as well as to all objects processed by the card
- Confidentiality of cryptographic keys, PINs and further security critical data
- Integrity of cryptographic keys, PINs and further security critical data
- Confidentiality of operating system code and its internal data
- Integrity of operating system code and its internal data (self test functionality)
- Resistance of crypto functionality against Side Channel Analysis (SPA, DPA, TA, DFA)
- Card management functionality
- Channel management (with separation of channel related objects)

To support the security of the above mentioned features of the TOE, the MICARDO V3.5 Operating System platform provides appropriate countermeasures for resistance especially against the following attacks:

- Cloning of the product
- Unauthorised disclosure of confidential data (during generation, storage and processing)
- Unauthorised manipulation of data (during generation, storage and processing)
- Identity usurpation
- Forgery of data to be processed
- Derivation of information on the private key from the related public part for oncard-generated RSA key pairs
- Side Channel Attacks

The resistance of the TOE against such attack scenarios is reached by usage of appropriate security features already integrated in the underlying IC as well as by implementing additional appropriate software countermeasures.

The specific eHC Application of the TOE comprises a file system with objects, access rules and data according to the requirements in /eHC1/ and /eHC2/. The eHC and its dedicated eHC Application provide the following main security services:

- Mutual Authentication between the eHC and a HPC or an SMC
- Mutual Authentication between the eHC and a security device (e. g. for online update of contract data in the card)
- Authentication of the card holder by use of one of two PINs, called PIN.CH and PIN.home

  (Note: Both of these PINs are used for general functions of the eHC. The electronic signature application (see below) requires a separate third PIN for its exclusive purposes.)
- Secure storage of contractual and medical data, with respect to confidentiality, integrity and authenticity of these data
- Authentication of the card using a private key and an X.509 certificate
- Document content key decipherment using a private key

Furthermore, the TOE is explicitly designed to to be used as Secure Signature-Creation Device (SSCD) for the generation of legally binding qualified electronic signatures in view of the European Directive 1999/93/EC on electronic signatures /ECDir/, the German Signature Act /SigG01/ and the German Signature Ordinance /SigV01/.

The Sagem Orga product is designed as SSCD of the so-called Type 3, i.e. as device with *oncard* - generation of the Signature-Creation Data / Signature-Verification Data (SCD/SVD key pair), the secure storage and use of the SCD and the secure creation of electronic signatures using the dedicated SCD key.

The TOE´s SIG Application provides the following services:

- Oncard-generation of the SCD/SVD pair
- Signature-creation using the dedicated SCD
- Confidentiality of cryptographic keys, PINs and further security critical data
- Integrity of cryptographic keys, PINs and further security critical data
- Confidentiality of operating system code and its internal data
- Integrity of operating system code and its internal data
- Authentication of the signatory, administrator and other users
- Protection of the communication between the TOE and the external world against disclosure and manipulation
- Protection of files and data by access control

Additional detailed information on the intended usage of the TOE and its functionality is given within the chapters 1.2 and 2.1.2.

2.5 Application Note: Scope of SSCD ST Application

This ST is intended to be used for a CC evaluation of a Secure Signature-Creation Device (SSCD) in view of the requirements specified in the European Directive 1999/93/EC on electronic signatures /ECDir/, Annex III as well as to the requirements from the German Signature Act /SigG01/ and the German Signature Ordinance /SigV01/.

For the TOE´s dedicated Signature Application, this ST refers to qualified certificates as electronic attestation of the SVD corresponding to the signatory's SCD that is implemented by the TOE.

While the main application scenario of the SSCD will assume a qualified certificate to be used in combination with the SSCD, there still is a large benefit in the security when such a SSCD is applied in other areas and such application is encouraged. The SSCD may as well be applied to environments where the certificates expressed as 'qualified certificates' in the ST do not fulfil the requirements laid down in Annex I and Annex II of the Directive /ECDir/.

With this respect the notion of qualified certificates in the ST refers to the fact that when an instance of the SSCD is used with a qualified certificate, such use is from the technical point of view eligible for an electronic signature as referred to in Directive /ECDir/, article 5, paragraph 1. As a consequence, the standard /ECDir/ does not prevent a device itself from being regarded as a SSCD, even when used together with a non-qualified certificate.

3 TOE Security Environment

3.1 Assets

Assets are security–relevant elements to be directly protected by the TOE whereby assets have to be protected in terms of confidentiality and integrity. Confidentiality of assets is always intended with respect to untrusted users of the TOE and its security-critical components, whereas the integrity of assets is relevant for the correct operation of the TOE and its security-critical components.

The confidentiality of the code of the TOE is included in this ST for several reasons. First, the confidentiality is needed for the protection of intellectual/industrial property on security or effectiveness mechanisms. Second, though protection shall not rely exclusively on code confidentiality, disclosure of the code may weaken the security of the involved application. For instance, knowledge about the implementation of the operating system or the applications running on the operaing system may benefit an attacker. This also applies to internal data of the TOE, which may similarly provide leaks for further attacks.

3.1.1 General Assets of the TOE

For a detailed description of the TOE´s assets related to the TOE´s dedicated eHC Application refer to /PP_eHC/, chap. 3.1.1.

3.1.2 Specific Assets of the TOE´s SIG Application

For a detailed description of the TOE´s assets related to the TOE´s dedicated SIG Application refer to /PP_SSCD_T3/, chap. 3.

Note: Biometric authentication is not supported by the TOE. Hence, “biometric data” and “biometric authentication references” are not applicable for the TOE.

The following asset concerning the personalisation of the TOE´s dedicated SIG Application is added:

SIG Application / Personalisation Data

Personalisation data related to the TOE´s dedicated SIG Application (integrity, authenticity and confidentiality of the personalisation data must be assured)

3.2 Assumptions

3.2.1 General Assumptions for the TOE

For a detailed description of the assumptions related to the TOE´s dedicated eHC Application refer to /PP_eHC/, chap. 3.4.

3.2.2 Specific Assumptions for the TOE´s SIG Application

For a detailed description of the specific assumptions related to the TOE´s dedicated SIG Application refer to /PP_SSCD_T3/, chap. 3.1.

The following specific assumption concerning the personalisation of the TOE´s dedicated SIG Application is added:

A.SIG_PERS Security of the Personalisation Process for the SIG Application

The originator of the personalisation data and the personalisation center responsible for the personalisation of the TOE´s dedicated SIG Application handle the personalisation data in an adequate secure manner. This concerns especially the security data to be personalised as secret cryptographic keys and PINs. The storage of the personalisation data at the originator and at the personalisation center as well as the transfer of these data between the different sites is conducted with respect to data integrity, authenticity and confidentiality.

Furthermore, the personalisation center treats the data for securing the personalisation process, i.e. the personalisation keys suitably secure.

It is in the responsibility of the originator of the personalisation data to garantuee for a sufficient quality of the personalisation data, especially of the cryptographic material to be personalised. The preparation and securing of the personalisation data appropriate to the card´s structure and according to the TOE´s personalisation requirements is as well in the responsibility of the external world and is done with care.

3.2.3 Specific Assumptions for the Completion Procedure of the TOE’s SIG Application

A.LEGITIMATE_ACTIVATION Activation for the legitimate signatory only

The certification service provider establishes and enforces a security policy which ensures that the signature application is activated under sole control of the signatory only.

3.3 Threats

The TOE is required to counter different type of attacks against its specific assets. A threat agent could try to threaten these assets either by functional attacks or by environmental manipulation, by specific hardware manipulation, by a combination of hardware and software manipulations or by any other type of attacks.

3.3.1 General Threats on the TOE

For a detailed description of the threats related to the TOE´s dedicated eHC Application refer to /PP_eHC/, chap. 3.3.

3.3.2 Specific Threats on the TOE´s SIG Application

For a detailed description of the specific threats related to the TOE´s dedicated SIG Application refer to /PP_SSCD_T3/, chap. 3.2.

The following specific threats concerning the personalisation of the TOE´s dedicated SIG Application are added:

T.SIG_ PERS_Aut Authentication for Personalisation Process of SIG Application

A successful storage of personalisation data for the TOE´s dedicated SIG Application without authorisation (of the external world) would be a threat to the security of the TOE.

T.SIG_PERS_Data Modification or Disclosure of Personalisation Data of SIG Application

A successful modification or disclosure of personalisation data for the TOE´s dedicated SIG Application during the data import would be a threat to the security of the TOE.

3.3.3 Specific Threats on the Completion Procedure of TOE’s SIG Application

There are no specific threats for the completion procedure of the TOE’s SIG Application other than the threats defined in /PP_SSCD_T3/. However, the completable SIG Application addresses some of the threats in a different way. See the security objectives rationale in Chapter 8 for details.

3.4 Organisational Security Policies

3.4.1 General Organisational Security Policies for the TOE

For a detailed description of the organisational security policies related to the TOE´s dedicated eHC Application refer to /PP_eHC/, chap. 3.2.

3.4.2 Specific Organisational Security Policies for the TOE´s SIG Application

For a detailed description of the organisational security policies related to the TOE´s dedicated SIG Application refer to /PP_SSCD_T3/, chap. 3.3.

3.4.3 Specific Organisational Security Policies for the Completion Procedure of the TOE’s SIG Application

There are no specific organisational security policies for the completion procedure of the TOE's SIG Application because the organisational security policies defined in /PP_SSCD_T3/ are sufficiently complete even for the completable variant.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE cover principally the following aspects:

- integrity and confidentiality of the TOE´s assets
- protection of the TOE and its associated documentation and environment during the development and production phases.

4.1.1 General Security Objectives for the TOE

For a detailed description of the security objectives related to the TOE´s dedicated eHC Application refer to /PP_eHC/, chap. 4.1.

4.1.2 Specific Security Objectives for the TOE´s SIG Application

For a detailed description of the specific security objectives related to the TOE´s dedicated SIG Application refer to /PP_SSCD_T3/, chap. 4.1. All security objectives have been overtaken, except OT.DTBS_Integrity_TOE which has been re-defined according to the extension of the Protection Profile concerning the establishment of trusted channels / paths for the communication between the TOE and a SCA. Furthermore, a specific security objective related to the personalisation of the TOE´s dedicated SIG Application is added.

OT.DTBS_Integrity_TOE Verification of the DTBS-Representation Integrity

In the case that a trusted channel between the TOE and the SCA by cryptographic means is established the TOE shall verify that the 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.

OT.SIG_PERS Security of the Personalisation Process for the SIG Application

The TOE shall only load and store personalisation data for the TOE´s dedicated SIG Application after the authentication of the external world. The TOE shall only load and store unaltered and authentic personalisation data.

The TOE shall detect flaws during the personalisation process, i.e. during the loading of the personalisation data.

The TOE must be able to support secure communication protocols and procedures between the TOE and the personalisation device ensuring data integrity, authenticity and confidentiality.

The TOE shall detect flaws during the personalisation process, i.e. during the loading of the personalisation data.

4.1.3 Specific Security Objectives for the Completion Procedure of the TOE’s SIG Application

The TOE has to meet additional security objectives to counter all the threats defined in /PP_SSCD_T3/ as long as the completion procedure of the SIG application is not successfully finished.

OT.QESC_TRSP_PROTECT Transport Protection of the SIG Application

The TOE shall enforce that the SIG Application is not usable until the completion process has been successfully finished.

Note: This security objective can be considered to be a variant of the security objective “OT.Sigy_SigF – Signature generation function for the legitimate signatory only” as specified in /PP_SSCD_T3/ Section 4.2. The goal of the definition of an additional security objective is to simplify the discussion for the security measures which apply to the transportation phase of the SIG application only.

OT.QESC_TRSP_RAD_Secrecy

The TOE shall protect the confidentiality of the the transport RAD – i.e. the RAD which has to be used by the signatory to set the initial operational RAD.

Note: This security objective applies only if the transport RAD is stored within the TOE.

4.2 Security Objectives for the Environment of the TOE

4.2.1 General Security Objectives for the Environment of the TOE

For a detailed description of the security objectives related to the environment of the TOE´s dedicated eHC Application refer to /PP_eHC/, chap. 4.2, 4.3.

4.2.2 Specific Security Objectives for the Environment of the TOE´s SIG Application

For a detailed description of the specific security objectives related to the environment of the TOE´s dedicated SIG Application refer to /PP_SSCD_T3/, chap. 4.2. All security objectives have been taken over, with the following exceptions: OE.HI_VAD has been re-defined and the new security objective OE.Trusted_Environment has been added according to the extension of the Protection Profile concerning the establishment of trusted channels / paths for the communication between the TOE and a SCA. Furthermore, a specific security objective related to the personalisation of the TOE´s dedicated SIG Application is added.

OE.HI_VAD Protection of the VAD

If an external device provides the human interface for user authentication, this device or its environment will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.

OE.Trusted_Environment Trusted Environment for SCA and TOE

In the case that a trusted channel resp. trusted path between the TOE and the SCA by cryptographic means is not established the environment for the TOE usage protects the confidentiality and integrity of the VAD as well as the integrity of the DTBS sent by the user via the SCA human interface to the TOE.

OE.SIG_PERS Security of the Personalisation Process for the SIG Application

The originator of the personalisation data and the personalisation center responsible for the personalisation of the TOE´s dedicated SIG Application handle the personalisation data in an adequate secure manner. This concerns especially the security data to be personalised as secret cryptographic keys and PINs. The storage of the personalisation data at the originator and at the personalisation center as well as the transfer of these data between the different sites is conducted with respect to data integrity, authenticity and confidentiality.

Furthermore, the personalisation center treats the data for securing the personalisation process, i.e. the personalisation keys suitably secure.

It is in the responsibility of the originator of the personalisation data to garantuee for a sufficient quality of the personalisation data, especially of the cryptographic material to be personalised. The preparation and securing of the personalisation data appropriate to the card´s structure and according to the TOE´s personalisation requirements is as well in the responsibility of the external world and is done with care.

4.2.3 Specific Security Objectives for the Environment of the Completion Procedure of the TOE’s SIG Application

The essential goal of the completion procedure for the TOE’s SIG application is to ensure that the SIG application is activated under sole control of the legitimate signatory. However, this goal cannot be ensured by the TOE alone but imposes some requirements on the environment of the TOE, too. Some of these requirements (namely OE.CGA_QCert, OE.SVD_Auth_CGA, and OE_HI_VAD) are already part of the protection profile of signature creation devices and have to be met by the completion process of a certification service provider as well.

However, the fact that the preparation of the QES application and the generation of the qualified certificate do no longer happen at the same time during the personalisation calls for some additional security objectives for the environment:

OE.QESC_CHECK_TRANSPORT_PROTECTION Check of the Transport Protection of the SIG Application

The certification service provider who conducts the completion has to check that the SIG transport protection of the SIG application is still active.

OE.QESC_CHECK_USER_LEGITIMACY Check the Legitimacy of the User

The certification server provider who conducts the completion has to check the legitimacy of the user.

OE.QESC_CHECK_SSCD Check that the Completion Procedure is Conducted on a SSCD

The certification service provider who conducts the completion has to check that the completion procedure is conducted on a secure signature creation device which fulfills the requirements of /SigG01/ and /SigV01/.

OE.QESC_SECURE_PIN_PUK_HANDLING Secure TransportPIN/PUK Handling

The security concept of the certification service provider who conducts the completion and the security concept of the certification service provider who is responsible for the personalisation of the card have to define and follow a coordinated approach for the secure handling of TransportPINs and TransportPUKs if this is required by the type of PINs/PUKs involved.

The intention of these objectives and how they relate to the security of the completion process are discussed in detail in the rationale (see Chapter 8).

5 IT Security Requirements

5.1 TOE Security Requirements

This section covers the subsections “TOE Security Functional Requirements” and ”TOE Security Assurance Requirements”.

5.1.1 TOE Security Functional Requirements

The TOE Security Functional Requirements (SFRs) define the functional requirements for the TOE using functional requirement components drawn directly from /CC 2.3 Part2/, functional requirement components of /CC 2.3 Part2/ with extension as well as self-defined functional requirement components. This chapter considers the SFRs concerning the IC (TOE-IC) as well as the SFRs concerning the Smartcard Embedded Software (TOE-ES).

Notes:

The SFRs for the TOE are listed in the following chapters within tables. Thereby, the tables contain in the left column the original definition of the respective SFR and its elements, dependencies, hierarchical information, management and audit functions. The right column supplies the iterations, selections, assignments and refinements chosen for the TOE.

Operations in the SFRs already carried out within the Protection Profiles are highlighted in bold face, further operations carried out in this ST are written in bold and italic face. Furthermore, extensions of the Protection Profile /PP_SSCD_T3/ are marked by underlining the new text (refer to chap. 5.1.1.2).

In general, the SFRs can be categorized as follows: cryptographic support, user data protection, identification and authentication, security management, protection of the TSF, trusted paths/channels.

5.1.1.1 General TOE Security Functional Requirements for the TOE

The following section gives a survey of the SFRs related to the TOE´s dedicated eHC Application as specified in the Protection Profile /PP_eHC/, chap. 5.1. The SFRs of the Protection Profile have been supplemented appropriately.

For the TOE´s dedicated eHC Application, the TOE maintains the SFP_access_rules as defined in /PP_eHC/, chap. 4.1.1.

FCS **Cryptographic Support**	
FCS_CKM **Cryptographic Key Management**	

FCS_CKM.1 **Cryptographic Key Generation**	PP eHC
FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. Hierarchical to: No other components Dependencies: - [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] - FCS_CKM.4 Cryptographic key destruction - FMT_MSA.2 Secure security attributes Management: a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption) Audit: a) Minimal: Success and failure of the activity b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)	**FCS_CKM.1/SM** **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 [**192bit (resp 168 bit, if parity bits are used)**] that meet the following: [- /eHC1/ (7.2)].
	FCS_CKM.1/RSA **FCS_CKM.1.1/RSA** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***RSA Key Generation***] and specified cryptographic key sizes [***2048 bit modulus length***] that meet the following: [/ALGCAT/***, chap. 1.3, 3.1, 4***].
FCS_CKM.4 **Cryptographic Key Destruction**	PP eHC
FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*]. Hierarchical to: No other components Dependencies:	**FCS_CKM.4** **FCS_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [***erasure of a 3DES session key***] that meets the following: [***physical erasure of the key***]. **Application Note** The TOE shall destroy the Triple-DES encryption session key and the Retail-MAC message authentication

- [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] - FMT_MSA.2 Secure security attributes <u>Management:</u> a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption) <u>Audit:</u> a) Minimal: Success and failure of the activity b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)	session keys for secure messaging after reset or termination of secure messaging session or reaching fail secure state according to FPT_FLS.1.
FCS_COP **Cryptographic Operation**	
FCS_COP.1 **Cryptographic Operation**	PP eHC
FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. <u>Hierarchical to:</u> No other components <u>Dependencies:</u> - [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] - FCS_CKM.4 Cryptographic key destruction - FMT_MSA.2 Secure security attributes <u>Management:</u> --- <u>Audit:</u> a) Minimal: Success and failure, and the type of cryptographic operation b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes	**FCS_COP.1/CSA** **FCS_COP.1.1/CSA** The TSF shall perform [**digital signature-creation**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [***of 2048 bit modulus length***] that meet the following: [- /PKCS1/].

	FCS_COP.1/CCA_SIGN **FCS_COP.1.1/CCA_SIGN** The TSF shall perform [**digital signature-creation**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [***2048 bit modulus length***] that meet the following: [- /ISO 9796-2/**(DS scheme 1)**].
	FCS_COP.1/ASYM_DEC **FCS_COP.1.1/ASYM_DEC** The TSF shall perform [**decryption**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [***of 2048 bit modulus length***] that meet the following: [- /PKCS1/].
	FCS_COP.1/CCA_VERIF **FCS_COP.1.1/ CCA_VERIF** The TSF shall perform [**digital signature-verification**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [***of 2048 bit modulus length***] that meet the following: [- /ISO 9796-2/ **(DS scheme 1)**].
	FCS_COP.1/SYM **FCS_COP.1.1/SYM** The TSF shall perform [**encryption and decryption**] in accordance with a specified cryptographic algorithm [**3DES in CBC mode**] and cryptographic key sizes [**168 bit**] that meet the following: [- /FIPS 46-3/].
	FCS_COP.1/MAC **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 sizes [**192 bit (resp 168 bit if parity bits are used)**] that meet the following: [- /ANSI X9.19/ **with DES**].
	FCS_COP.1/HASH

	FCS_COP.1.1/HASH The TSF shall perform [**hashing**] in accordance with the specified cryptographic algorithm [***SHA-256***] and cryptographic key sizes [**none**] that meet the following: [- /SHA/].
FCS_RND **Generation of Random Numbers**	
FCS_RND.1 **Quality Metric for Random Numbers**	PP eHC
FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric]. Hierarchical to: No other components Dependencies: No dependencies Management: --- Audit: ---	**FCS_RND.1** **FCS_RND.1.1** The TSF shall provide a mechanism to generate random numbers that meet [***deterministic RNG of quality class K4***].

FDP **User Data Protection**	
FDP_ACC **Access Control Policy**	
FDP_ACC.2 **Complete Access Control**	PP eHC
FDP_ACC.2.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and objects*] 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.	**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

Hierarchical to: FDP_ACC.1 Dependencies: - FDP_ACF.1 Security attribute based access control Management: --- Audit: ---	covered by an access control SFP.
FDP_ACF **Access Control Functions**	
FDP_ACF.1 **Security Attribute Based Access Control**	PP eHC
FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]. **FDP_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]. **FDP_ACF.1.3** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]. **FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]. Hierarchical to: No other components Dependencies: - FDP_ACC.1 Subset access control - FMT_MSA.3 Static attribute initialisation Management: a) Managing the attributes used to make explicit access or denial based decisions	**FDP_ACF.1** **FDP_ACF.1.1** 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** 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** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]. **FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the [**rules for all access methods and the access rules defined in SFP_access_rules**].

Audit: a) Minimal: Successful requests to perform an operation on an object covered by the SFP b) Basic: All requests to perform an operation on an object covered by the SFP c) Detailed: The specific security attributes used in making an access check	
FDP_RIP **Residual Information Protection**	
FDP_RIP.1 **Subset Residual Information Protection**	PP eHC
FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to*, *deallocation of the resource from*] the following objects: [assignment: *list of objects*]. Hierarchical to: No other components Dependencies: No dependencies Management: a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE Audit: ---	**FDP_RIP.1** **FDP_RIP.1.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***deallocation of the resource from***] the following objects: [***security relevant material (as secret and private cryptographic keys, PINs, PUCs, data in all files which are not freely accessible, ...)***].
FDP_SDI **Stored Data Integrity**	
FDP_SDI.2 **Stored Data Integrity Monitoring and Action**	PP eHC
FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*]. **FDP_SDI.2.2** Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*]. Hierarchical to: FDP_SDI.1 Dependencies: No dependencies	**FDP_SDI.2/Int-PersData** **FDP_SDI.2.1/Int-PersData** The TSF shall monitor user data ***and specific TSF data*** stored within the TSC for [**integrity errors**] on all objects, based on the following attributes: [***checksum secured persistently stored data***]. ***Application Note*** *The following data persistently stored by the TOE have the attribute „checksum secured persistently stored data":* - *User / application data (e.g. in files on the card)* - *Keys (incl. attributes)* - *PINs / PUCs (incl. attributes)*

Management: a) The actions to be taken upon the detection of an integrity error could be configurable Audit: a) Minimal: Successful attempts to check the integrity of user data, including an indication of the results of the check b) Basic: All attempts to check the integrity of user data, including an indication of the results of the check, if performed c) Detailed: The type of integrity error that occurred d) Detailed: The action taken upon detection of an integrity error	- *File and object management information (as e.g. access rules, object life cycle states)* - *Card life cycle status information* ***Refinement*** *The check for integrity errors shall be done before usage resp. processing of the data. The checksum securing shall concern the data objects as well as the data values themselves.* **FDP_SDI.2.2/Int-PersData** Upon detection of a data integrity error, the TSF shall [- **prohibit the use of the altered data** - **inform the connected entity about integrity error**].
	FDP_SDI.2/Int-TempData **FDP_SDI.2.1/Int-TempData** The TSF shall monitor user data ***and specific TSF data*** stored within the TSC for [**integrity errors**] on all objects, based on the following attributes: [***checksum secured temporarily stored data***]. ***Application Note*** *The following data temporarily stored by the TOE have the attribute „checksum secured temporarily stored data“:* - *User / application data (as hash values, ...)* - *Keys (incl. attributes)* - *Card Context including different Channel Contexts (actual Security Environment, status information as the actual security status for Key and PIN based authentication, information on the availability of session keys, ...)* - *Input data for electronic signatures* ***Refinement*** *The check for integrity errors shall be done before usage resp. processing of the data. The checksum securing shall concern the data objects as well as the data values themselves.* **FDP_SDI.2.2/Int-TempData** Upon detection of a data integrity error, the TSF shall [- **prohibit the use of the altered data** - **inform the connected entity about integrity error**].
FDP_UCT **Inter-TSF User Data Confidentiality Transfer Protection**	

FDP_UCT.1 **Basic Data Exchange Integrity**	PP eHC
FDP_UCT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to [selection*: transmit, receive*] objects in a manner protected from unauthorised disclosure. Hierarchical to: No other components Dependencies: - [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] - [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] Management: --- Audit: a) Minimal: The identity of any user or subject using the data exchange mechanisms b) Basic: The identity of any unauthorised user or subject attempting to use the data exchange mechanisms c) Basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This could include security attributes associated with the information	**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 unauthorised disclosure.
FDP_UIT **Inter-TSF User Data Integrity Transfer Protection**	
FDP_UIT.1 **Data Exchange Integrity**	PP eHC
FDP_UIT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to [selection*: transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors. **FDP_UIT.1.2** The TSF shall be able to determine on receipt of user data, whether [selection: *modification*, *deletion, insertion, replay*] has occurred. Hierarchical to: No other components Dependencies: - [FDP_ACC.1 Subset access control or	**FDP UIT.1** **FDP_UIT.1.1** 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** The TSF shall be able to determine on receipt of user data, whether [**modification, deletion, insertion and replay**] has occurred.

FDP_IFC.1 Subset information flow control] - [FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path] Management: --- Audit: a) Minimal: The identity of any user or subject using the data exchange mechanisms b) Basic: The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorised to do so c) Basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received; this could include security attributes associated with the user data d) Basic: Any identified attempts to block transmission of user data e) Detailed: The types and/or effects of any detected modifications of transmitted user data	

FIA **Identification and Authentication**	
FIA_AFL **Authentication Failures**	
FIA_AFL.1 **Authentication Failure Handling**	PP eHC
FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*], “*an administrator configurable positive integer within* [assignment: *range of acceptable values*]“] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*]. **FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*]. Hierarchical to: No other components Dependencies: - FIA_UAU.1 Timing of authentication Management: a) management of the threshold for unsuccessful authentication attempts	**FIA_AFL.1/PIN** **FIA_AFL.1.1/PIN** The TSF shall detect when [***3***] unsuccessful authentication attempts occur related to [**consecutive failed human user authentication for the health care application**]. **FIA_AFL.1.2/PIN** When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [- **block the PIN for authentication until successful unblock with resetting code**].

b) management of actions to be taken in the event of an authentication failure Audit: a) Minimal: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal)	
	FIA_AFL.1/PUC **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 [- ***warn the entity connected*** - ***not unblock the referenced blocked PIN*** - **block the PUC resp. the verification mechanism for this PUC such that any subsequent authentication attempt with this PUC will fail and an unblocking of all blocked PINs related to this PUC is no longer possible** - ***be able to indicate to subsequent users the reason for the blocking of the PUC***].
FIA_ATD **User Attribute Definition**	
FIA_ATD.1 **User Attribute Definition**	PP eHC
FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*]. Hierarchical to: No other components Dependencies: No dependencies Management: a) if so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users Audit: ---	**FIA_ATD.1** **FIA_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users: [**identity and role**].

FIA_UAU **User Authentication**	
FIA_UAU.1 **Timing of Authentication**	PP eHC
FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] 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. Hierarchical to: No other components Dependencies: - FIA_UID.1 Timing of identification Management: a) management of the authentication data by an administrator b) management of the authentication data by the associated user c) managing the list of actions that can be taken before the user is authenticated Audit: a) Minimal: Unsuccessful use of the authentication mechanism b) Basic: All use of the authentication mechanism c) Detailed: All TSF mediated actions performed before authentication of the user	**FIA_UAU.1** **FIA_UAU.1.1** The TSF shall allow [**reading the ATR, reading the Card Verifiable Authentication Certificate, reading the Certificate Service Provider self-signed Certificate, Identification by providing the users eHC-PIN, identification by providing the users certificate, *execution of commands allowed without preceding successful authentication due to the access rules set***] 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.
FIA_UAU.4 **Single-use Authentication Mechanisms**	PP eHC
FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: *identified authentication mechanism(*s)]. Hierarchical to: No other components Dependencies: No dependencies Management: --- Audit: a) Minimal: Attempts to reuse authentication data	**FIA_UAU.4** **FIA_UAU.4.1** The TSF shall prevent reuse of authentication data related to [**Card-to-Card Authentication Mechanism**].

FIA_UID **User Identification**	
FIA_UID.1 **Timing of Identification**	PP eHC
FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified. **FIA_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. Hierarchical to: No other components Dependencies: No dependencies Management: a) the management of the user identities b) if an authorised administrator can change the actions allowed before identification, the managing of the action lists Audit: a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided b) Basic: All use of the user identification mechanism, including the user identity provided	**FIA_UID.1** **FIA_UID.1.1** The TSF shall allow [**reading the ATR, reading the Card Verifiable Authentication Certificate, reading the Certificate Service Provider Certificate, *execution of commands allowed without preceding successful authentication due to the access rules set***] 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.

FMT **Security Management**	
FMT_LIM **Limited capabilities and availability**	
FMT_LIM.1 **Limited capabilities**	PP eHC
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*]. Hierarchical to: No other components	**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 manipu-**

Dependencies: - FMT_LIM.2 Limited availability Management: --- Audit: ---	**lated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks**].
FMT_LIM.2 **Limited availability**	PP eHC
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*]. Hierarchical to: No other components Dependencies: - FMT_LIM.1 Limited capability Management: --- Audit: ---	**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**].
FMT_MTD **Management of TSF Data**	
FMT_MTD.1 **Management of TSF Data**	PP eHC
FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*]. Hierarchical to: No other components Dependencies: - FMT_SMF.1 Specification of management functions - FMT_SMR.1 Security roles Management: a) managing the group of roles that can interact with the TSF data	**FMT_MTD.1/Ini** **FMT_MTD.1.1/Ini** The TSF shall restrict the ability to [**write**] the [**initialisation data**] to [**the TOE Manufacturer**].

Audit: a) Basic: All modifications to the values of TSF data	
	FMT_MTD.1/Pers **FMT_MTD.1.1/Pers** The TSF shall restrict the ability to [**write**] the [**personalisation data**] to [**the Personalisation Service Provider**].
	FMT_MTD.1/CMS **FMT_MTD.1.1/CMS** The TSF shall restrict the ability to [**write**] the [**file structures for additional applications, cryptographic keys for additional applications, PINs and other user authentication reference data for additional applications, access rights for additional applications**] to [**the Download Service Provider**].
	FMT_MTD.1/PIN **FMT_MTD.1.1/PIN** The TSF shall restrict the ability to [**modify, unblock**] the [**PIN**] to [**the Card Holder**].
	FMT_MTD.1/KEY_MOD **FMT_MTD.1.1/KEY_MOD** The TSF shall restrict the ability to [**modify**] the [**public key for CV certification verification**] to [**none**].
FMT_SMF **Specification of Management Functions**	
FMT_SMF.1 **Specification of Management Functions**	PP eHC
FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: *list of security management functions to be provided by the TSF*]. Hierarchical to: No other components Dependencies: No dependencies Management: --- Audit: a) Minimal: Use of the management functions.	**FMT_SMF.1** **FMT_SMF.1.1** The TSF shall be capable of performing the following security management functions: [**initialisation, personalisation, service card management, modification of the PIN**].

FMT_SMR **Security Management Roles**	
FMT_SMR.1 **Security Roles**	PP eHC
FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *the authorised identified roles*]. **FMT_SMR.1.2** The TSF shall be able to associate users with roles. Hierarchical to: No other components Dependencies: - FIA_UID.1 Timing of identification Management: a) managing the group of users that are part of a role Audit: a) Minimal: modifications to the group of users that are part of a role b) Detailed: every use of the rights of a role	**FMT_SMR.1** **FMT_SMR.1.1** The TSF shall maintain the roles [**Health Professional, Medical Assistant, Security Module Card (health care), Self Service Terminal, Health Insurance Agency Service Provider, Combined Services Provider, Card Holder, Download Service Provider, Personalisation Service Provider, TOE Manufacturer**]. **FMT_SMR.1.2** The TSF shall be able to associate users with roles.

FPT **Protection of the TSF**	
FPT_EMSEC **TOE Emanation**	
FPT_EMSEC.1 **TOE Emanation**	PP eHC
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]. Hierarchical to: No other components Dependencies: No dependencies	**FPT_EMSEC.1** **FPT_EMSEC.1.1** The TOE shall not emit [***information on IC power consumption, information on command execution time, information on electromagnetic emanations***] in excess of [***non useful information***] enabling access to [**PIN and PUC**] and [**Card Authentication Private Key, Client Server Authentication Private Key, Document Cipher Key Decipher Key, secure messaging keys**]. **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 [**PIN and PUC**] and [**Card Authentication Private Key, Client Server Authentication Private Key, Document Cipher Key Decipher Key,**

Management: --- Audit: ---	**secure messaging keys**]. **Application Note** The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The TOE has to provide a smart card interface with contacts according to ISO/IEC 7816-2 but the integrated circuit may have additional contacts or a contact less interface as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.
FPT_FLS **Fail Secure**	
FPT_FLS.1 **Failure with Preservation of Secure State**	PP eHC
FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*]. Hierarchical to: No other components Dependencies: - ADV_SPM.1 Informal TOE security policy model Management: --- Audit: a) Basic: Failure of the TSF	**FPT_FLS.1** **FPT_FLS.1.1** The TSF shall preserve a secure state when the following types of failures occur: [- **Exposure to operating conditions where therefore a malfunction could occur** - **Failure detected by TSF according to FPT_TST.1**].
FPT_PHP **Physical Protection**	
FPT_PHP.3 **Resistance to Physical Attack**	PP eHC
FPT_PHP.3.1 The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: *list of TSF devices / elements*] by responding automatically such that the TSP is not violated.	**FPT_PHP.3** **FPT_PHP.3.1** The TSF shall resist [**physical manipulation and physical probing**] to the [**TSF**] by responding automatically such that the TSP is not violated.

Hierarchical to: No other components Dependencies: No dependencies Management: a) management of the automatic responses to physical tampering Audit: ---	**Application Note** The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, “automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.
FPT_RVM **Reference Mediation**	
FPT_RVM.1 **Non-Bypassability of the TSP**	PP eHC
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. Hierarchical to: No other components Dependencies: No dependencies Management: --- Audit: ---	**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.
FPT_SEP **Domain Separation**	
FPT_SEP.1 **TSF Domain Separation**	PP eHC
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. Hierarchical to: No other components Dependencies: No dependencies	**FPT_SEP.1** **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.

Management: --- Audit: ---	
FPT_TST **TSF Self Test**	
FPT_TST.1 **TSF Testing**	PP eHC
FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*]. **FPT_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF data*], *TSF data*]. **FPT_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. Hierarchical to: No other components Dependencies: - FPT_AMT.1 Abstract machine testing Management: a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions b) management of the time interval if appropriate Audit: a) Basic: Execution of the TSF self tests and the results of the tests	**FPT_TST.1** **FPT_TST.1.1** The TSF shall run a suite of self tests [***during initial start-up, periodically during normal operation***] to demonstrate the correct operation of [***the TSF***]. ***Note*** *During initial start-up means before code execution.* ***Refinements*** *The TOE's self tests shall include the verification of the integrity of any software code (incl. patches) stored outside of the ROM. Upon detection of a self test error the TSF shall warn the entity connected. After OS testing is completed, all testing-specific commands and actions shall be disabled or removed. It shall not be possible to override these controls and restore them for use. Command associated exclusively with one life cycle state shall never be accessed during another state.* **FPT_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of [***TSF data***]. ***Refinement*** *In this framework, the OS (i.e. the Smartcard Embedded Software of the TOE (TOE-ES)) itself is understood as „authorised user“.* **FPT_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. ***Refinement*** *The integrity check over the executable code stored outside the ROM area is covered by FPT_TST.1.1 and the related refinement.* *The requirement for checking the integrity of the ROM-code shall concern only the production phase, more precise the initialisation phase of the TOE´s lifecycle. Prior to the initialisation of the TOE, the ROM-code of the TOE shall be verifiable by authorised us-*

	ers as the OS developer. The integrity of the ROM-code shall be provable only during the initialisation process.

FTP **Trusted Path/Channels**	
FTP_ITC **Inter-TSF Trusted Channel**	
FTP_ITC.1 **Inter-TSF Trusted Channel**	PP eHC
FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **FTP_ITC.1.2** The TSF shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel. **FTP_ITC.1.3** The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*]. Hierarchical to: No other components Dependencies: No dependencies Management: a) Configuring the actions that require trusted channel, if supported Audit: a) Minimal: Failure of the trusted channel functions b) Minimal: Identification of the initiator and target of failed trusted channel functions c) Basic: All attempted uses of the trusted channel functions d) Basic: Identification of the initiator and target of all trusted channel functions	**FTP_ITC.1** **FTP_ITC.1.1** The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **FTP_ITC.1.2** The TSF shall permit [**the remote trusted IT product**] to initiate communication via the trusted channel. **FTP_ITC.1.3** The TSF shall initiate communication via the trusted channel for [**all functions requiring a trusted channel as defined by SFP_access_rules**].

5.1.1.2 TOE Security Functional Requirements for the TOE´s SIG Application

The following section gives a survey of the SFRs related to the TOE´s dedicated SIG Application as specified in the Protection Profile /PP_SSCD_T3/, chap. 5.1. The SFRs of the Protection Profile have been supplemented appropriately.

For the TOE´s dedicated SIG Application, the TOE maintains an SFP as defined as follows:

SFP SIG Access Control

Subjects:

- User

Security attributes for subjects:

- General Attribute Role (Administrator, Signatory)
- Initialisation Attribute SCD/SVD Management (authorised, not authorised)

Objects:

- SCD
- DTBS

Security attributes for objects:

- For object SCD: SCD Operational (no, yes)
- For object DTBS: Sent by an authorised SCA (no, yes)

Operations (Access Modes):

- Signature key pair generation
- Export of SVD
- Creation and import of RAD
- Generation of electronic signatures

The SFP SIG Access Control is subdivided into four SFPs according to /PP_SSCD_T3/, chap. 5.1.2:

- SFP Initialisation (for the generation of SCD/SVD)
- SFP SVD Transfer (for the export of SVD)
- SFP Personalisation (for the creation and import of RAD)
- SFP Signature-Creation (for the generation of electronic signatures)

The related access rules for the TOE´s dedicated SIG Application are specified in detail within /PP_SSCD_T3/, chap. 5.1.2.

These rules are augmented for the SFP SVD Transfer, because also the authorised CSP shall be permitted to export the SVD, too. See the rationale for the adoptions of the /PP_SSCD_T3/ in Chapter 8 for further details.

For the personalisation of the TOE´s dedicated SIG Application in the sense of loading the personalisation data by usage of the applicable commands of the MICARDO V3.5 operating system platform, the TOE maintains an SFP as defined as follows:

<u>SFP SIG Personalisation</u>

Subjects:

- Card Management System (for personalisation of the SIG Application)

Security attributes for subjects:

- USER_GROUP (authorised user, non-authorised user)

Objects:

- Personalisation data

Security attributes for objects:

- Access Rules

Operations (Access Modes):

- Loading of personalisation data by usage of the MICARDO V3.5 operating system commands

The SIG Access Control SFP controls the access of subjects to objects on the basis of security attributes. The access rules for the personalisation of the TOE´s SIG Application are explicitly set in such a manner that personalisation requires a preceding mutual authentication between the TOE and the external world.

Hint: The export of SVD is part of the above defined SFP SVD Transfer. The generation and personalisation of RAD is part of the above defined SFP SIG Personalisation.

FCS **Cryptographic Support**	
FCS_CKM **Cryptographic Key Management**	
FCS_CKM.1 **Cryptographic Key Generation**	PP SSCD Type3

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. Hierarchical to: No other components Dependencies: - [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] - FCS_CKM.4 Cryptographic key destruction - FMT_MSA.2 Secure security attributes Management: a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption) Audit: a) Minimal: Success and failure of the activity b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)	**FCS_CKM.1** **FCS_CKM.1.1** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***RSA key pair generation with randomly generated resp. externally chosen public exponent (up to 64 bit) (command GENERATE ASYMMETRIC KEY PAIR)***] and specified cryptographic key sizes [***2048 bit modulus length***] that meet the following: [- /ALGCAT/***, chap. 1.3, 3.1, 4***].
FCS_CKM.4 **Cryptographic Key Destruction**	PP SSCD Type3
FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*]. Hierarchical to: No other components Dependencies: - [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] - FMT_MSA.2 Secure security attributes Management: a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period,	**FCS_CKM.4** **FCS_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [***erasure of a private RSA key***] that meets the following: [***physical erasure of the key***]. **Application Note** The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.

and use (e.g. digital signature, key encryption, key agreement, data encryption) Audit: a) Minimal: Success and failure of the activity b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)	
FCS_COP **Cryptographic Operation**	
FCS_COP.1 **Cryptographic Operation**	PP SSCD Type3
FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. Hierarchical to: No other components Dependencies: - [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] - FCS_CKM.4 Cryptographic key destruction - FMT_MSA.2 Secure security attributes Management: --- Audit: a) Minimal: Success and failure, and the type of cryptographic operation b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes	**FCS_COP.1/CORRESP** **FCS_COP.1.1/CORRESP** The TSF shall perform [**SCD/SVD correspondence verification**] in accordance with a specified cryptographic algorithm [***generation of an RSA digital signature***] and cryptographic key sizes [***2048 bit modulus length***] that meet the following: [- ***RSA signature scheme with appendix according to*** /PKCS1/***(based on SHA-2 (256 bit) as hash algorithm):*** /PKCS1/***, chap. 8.2.1 without hash value calculation inside step 1 of chap. 9.2;*** ***or alternatively*** - ***RSA signature scheme with appendix according to ISO/IEC 9796-2 with random number (based on SHA-2 (256, bit)as hash algorithm): /ISO 9796-2/ without hash value calculation;***]. ***Note*** *The SCD/SVD correspondence verification shall be realised by the generation of a digital signature using the SCD (to be done by the signatory resp. the TOE) followed by the verification of the supplied signature by the external world using the corresponding SVD.*
	FCS_COP.1/SIGNING-PKCS1: **FCS_COP.1.1/SIGNING-PKCS1** The TSF shall perform [**digital signature-generation *(command PSO COMPUTE DIGITAL SIGNATURE)***] in accordance with a specified cryptographic algorithm [***RSA***] and cryptographic key sizes [***2048 bit modulus length***] that meet the following: [- ***RSA signature scheme with appendix according to PKCS #1 (based on SHA-2 (256 bit) as hash algorithm)***

	].
	FCS_COP.1/SIGNING-ISO9796-2: **FCS_COP.1.1/SIGNING-ISO9796-2** The TSF shall perform [**digital signature-generation *(command PSO COMPUTE DIGITAL SIGNATURE)***] in accordance with a specified cryptographic algorithm [***RSA***] and cryptographic key sizes [***2048 bit modulus length***] that meet the following: [- ***RSA signature scheme with appendix according to ISO/IEC 9796-2 with random number (based on SHA-2 (256bit) as hash algorithm): /ISO 9796-2/ without hash value calculation;***].

FDP **User Data Protection**	
FDP_ACC **Access Control Policy**	
FDP_ACC.1 **Subset Access Control**	PP SSCD Type3
FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]. Hierarchical to: No other components Dependencies: - FDP_ACF.1 Security attribute based access control Management: --- Audit: ---	**FDP_ACC.1/SVD Transfer SFP** **FDP_ACC.1.1/SVD Transfer SFP** The TSF shall enforce the [**SVD Transfer SFP**] on [**export of SVD by User**].
	FDP_ACC.1/Initialisation SFP **FDP_ACC.1.1/Initialisation SFP** The TSF shall enforce the [**Initialisation SFP**] on [**generation of SCD/SVD pair by User**].
	FDP_ACC.1/Personalisation SFP

	FDP_ACC.1/Personalisation SFP The TSF shall enforce the [**Personalisation SFP**] on [**creation of RAD by Administrator**].
	FDP_ACC.1/Signature-Creation SFP **FDP_ACC.1/Signature-Creation SFP** The TSF shall enforce the [**Signature-Creation SFP**] on [**1. sending of DTBS-representation by SCA, 2. signing of DTBS-representation by Signatory**].
	FDP_ACC.1/SIG Personalisation SFP ***FDP_ACC.1.1/SIG Personalisation SFP*** *The TSF shall enforce the [**SIG Personalisation SFP**] on [**import of personalisation data by Administrator**].*
FDP_ACF **Access Control Functions**	
FDP_ACF.1 **Security Attribute Based Access Control**	PP SSCD Type3
FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]. **FDP_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]. **FDP_ACF.1.3** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]. **FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]. Hierarchical to: No other components Dependencies: - FDP_ACC.1 Subset access control - FMT_MSA.3 Static attribute initialisation	**FDP_ACF.1/SVD Transfer SFP** **FDP_ACF.1.1/SVD Transfer SFP** The TSF shall enforce the [**SVD Transfer SFP**] to objects based on the following: [**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: [**The user with the security attribute "role" set to "Administrator", "AuthorisedCSP", or to "Signatory" is allowed to export SVD**]. **FDP_ACF.1.3/SVD Transfer SFP** The TSF shall explicitly authorise 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 [**none**].

Management: a) Managing the attributes used to make explicit access or denial based decisions Audit: a) Minimal: Successful requests to perform an operation on an object covered by the SFP b) Basic: All requests to perform an operation on an object covered by the SFP c) Detailed: The specific security attributes used in making an access check	
	FDP_ACF.1/Initialisation SFP **FDP_ACF.1.1/Initialisation SFP** The TSF shall enforce the [**Initialisation SFP**] to objects based on the following: [**General attribute and Initialisation attribute**]. **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: [**The user with the security attribute “role” set to “Administrator” or set to “Signatory” and with the security attribute “SCD / SVD management” set to “ authorised” is allowed to generate SCD/SVD pair**]. **FDP_ACF.1.3/Initialisation SFP** The TSF shall explicitly authorise 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: The user with the security attribute “role” set to “Administrator” or set to “Signatory” and with the security attribute “SCD / SVD management” set to “not authorised” is not allowed to generate SCD/SVD pair**].
	FDP_ACF.1/Personalisation SFP **FDP_ACF.1.1/Personalisation SFP** The TSF shall enforce the [**Personalisation SFP**] to objects based on the following: [**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: [**User with the security attribute “role” set to “Administrator” is allowed to create the RAD**]. **FDP_ACF.1.3/Personalisation SFP** The TSF shall explicitly authorise 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 [**none**].
	FDP_ACF.1/Signature-Creation SFP **FDP_ACF.1.1/Signature-Creation SFP** The TSF shall enforce the [**Signature-creation SFP**] to objects based on the following: [**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: [**User with the security attribute “role” set to “Signatory” is allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “yes”**]. **FDP_ACF.1.3/Signature-Creation SFP** The TSF shall explicitly authorise 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) User with the security attribute “role” set to “Signatory” is not allowed to create electronic signatures for DTBS which is not sent by an authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “yes”; (b) User with the security attribute “role” set to “Signatory” is not allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “no”**]. **Application Note** A SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature. The Signatory controls wether a trusted channel to the SSCD by cryptographic means as required by FTP_ITC.1.3/SCA DTBS is established or a channel to the SSCD within a trusted environment is set-up.
	FDP_ACF.1/SIG Personalisation SFP ***FDP_ACF.1.1/SIG Personalisation SFP*** *The TSF shall enforce the [**SIG Application Personalisation SFP**] to objects based on the following: [**authentication status of user**].* ***FDP_ACF.1.2/SIG Personalisation SFP*** *The TSF shall enforce the following rules to determine*

	*if an operation among controlled subjects and controlled objects is allowed: [**The Card Management System is allowed to perform the smartcard personalisation process (loading of the personalisation data related to the TOE´s SIG Application)**].* ***FDP_ACF.1.3/SIG Personalisation SFP*** *The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].* ***FDP_ACF.1.4/SIG Personalisation SFP*** *The TSF shall explicitly deny access of subjects to objects based on the [**none**].*
FDP_ETC **Export to Outside TSF Control**	
FDP_ETC.1 **Export of User Data without Security Attributes**	PP SSCD Type3
FDP_ETC.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside of the TSC. **FDP_ETC.1.2** The TSF shall export the user data without the user data's associated security attributes. Hierarchical to: No other components Dependencies: - [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] Management: --- Audit: a) Minimal: Successful export of information b) Basic: All attempts to export information	**FDP_ETC.1/SVD Transfer** **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.
FDP_ITC **Import from Outside TSF Control**	
FDP_ITC.1 **Import of User Data without Security Attributes**	PP SSCD Type3
FDP_ITC.1.1 The TSF shall enforce the [assignment: *access control SFP and/or information flow control SFP*] when importing user data, controlled under the SFP, from	**FDP_ITC.1/DTBS** **FDP_ITC.1.1/DTBS** The TSF shall enforce the [**Signature-Creation SFP**]

outside of the TSC. **FDP_ITC.1.2** The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC. **FDP_ITC.1.3** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *additional importation control rules*]. Hierarchical to: No other components Dependencies: - [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] - FMT_MSA.3 Static attribute initialisation Management: a) The modification of the additional control rules used for import Audit: a) Minimal: Successful import of user data, including any security attributes b) Basic: All attempts to import user data, including any security attributes c) Detailed: The specification of security attributes for imported user data supplied by an authorised user	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: [**DTBS-representation shall be sent by an authorised SCA**]. **Application Note** A SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature. The Signatory controls wether a trusted channel to the SSCD by cryptographic means as required by FTP_ITC.1.3/SCA DTBS is established or a channel to the SSCD within a trusted environment is set-up.
FDP_RIP **Residual Information Protection**	
FDP_RIP.1 **Subset Residual Information Protection**	PP SSCD Type3
FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to*, *deallocation of the resource from*] the following objects: [assignment: *list of objects*]. Hierarchical to: No other components Dependencies: No dependencies Management: a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE	**FDP_RIP.1** **FDP_RIP.1.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**deallocation of the resource from**] the following objects: [**SCD, VAD, RAD**].

Audit: ---	
FDP_SDI **Stored Data Integrity**	
FDP_SDI.2 **Stored Data Integrity Monitoring and Action**	PP SSCD Type3
FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*]. **FDP_SDI.2.2** Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*]. Hierarchical to: FDP_SDI.1 Dependencies: No dependencies Management: a) The actions to be taken upon the detection of an integrity error could be configurable Audit: a) Minimal: Successful attempts to check the integrity of user data, including an indication of the results of the check b) Basic: All attempts to check the integrity of user data, including an indication of the results of the check, if performed c) Detailed: The type of integrity error that occurred d) Detailed: The action taken upon detection of an integrity error	**Note** The following data persistently stored by TOE have the user data attribute “integrity checked persistent stored data”: 1. SCD, 2. RAD, 3. SVD (if persistent stored by TOE). **FDP_SDI.2/Persistent** **FDP_SDI.2.1/Persistent** The TSF shall monitor user data stored within the TSC for [**integrity error**] on all objects, based on the following attributes: [**integrity checked persistent stored data**]. **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 Signatory about integrity error**].
	Note The DTBS-representation temporarily stored by TOE has the user data attribute “integrity checked stored data”. **FDP_SDI.2/DTBS** **FDP_SDI.2.1/DTBS** The TSF shall monitor user data stored within the TSC for [**integrity error**] 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 Signatory about integrity error**].

FDP_UIT **Inter-TSF User Data Integrity Transfer Protection**	
FDP_UIT.1 **Data Exchange Integrity**	PP SSCD Type3
FDP_UIT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to [selection*: transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors. **FDP_UIT.1.2** The TSF shall be able to determine on receipt of user data, whether [selection: *modification*, *deletion, insertion, replay*] has occurred. Hierarchical to: No other components Dependencies: - [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] - [FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path] Management: --- Audit: a) Minimal: The identity of any user or subject using the data exchange mechanisms b) Basic: The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorised to do so c) Basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received; this could include security attributes associated with the user data d) Basic: Any identified attempts to block transmission of user data e) Detailed: The types and/or effects of any detected modifications of transmitted user data	**FDP_UIT.1/SVD Transfer** **FDP_UIT.1.1/SVD Transfer** The TSF shall enforce the [**SVD Transfer SFP**] to be able to [**transmit**] user data 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/TOE DTBS **FDP_UIT.1.1/TOE DTBS** The TSF shall enforce the [**Signature-Creation SFP**] to be able to [**receive**] user data 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.

	Application Note Protection for FDP_UIT.1.1/TOE DTBS can either be assured by a trusted channel to the SSCD by cryptographic means or by a channel to the SSCD within a trusted environment.

FIA **Identification and Authentication**	
FIA_AFL **Authentication Failures**	
FIA_AFL.1 **Authentication Failure Handling**	PP SSCD Type3
FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*], "*an administrator configurable positive integer within* [assignment: *range of acceptable values*]"] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*]. **FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*]. Hierarchical to: No other components Dependencies: - FIA_UAU.1 Timing of authentication Management: a) management of the threshold for unsuccessful authentication attempts b) management of actions to be taken in the event of an authentication failure Audit: a) Minimal: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal)	**FIA_AFL.1** **FIA_AFL.1.1** The TSF shall detect when [***3***] unsuccessful authentication attempts occur related to [**consecutive failed authentication attempts**]. **FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**block RAD**].
FIA_ATD **User Attribute Definition**	
FIA_ATD.1 **User Attribute Definition**	PP SSCD Type3

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*]. Hierarchical to: No other components Dependencies: No dependencies Management: a) if so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users Audit: ---	**FIA_ATD.1** **FIA_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users: [**RAD**].
FIA_UAU **User Authentication**	
FIA_UAU.1 **Timing of Authentication**	PP SSCD Type3
FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] 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. Hierarchical to: No other components Dependencies: - FIA_UID.1 Timing of identification Management: a) management of the authentication data by an administrator b) management of the authentication data by the associated user c) managing the list of actions that can be taken before the user is authenticated Audit: a) Minimal: Unsuccessful use of the authentication mechanism b) Basic: All use of the authentication mechanism c) Detailed: All TSF mediated actions performed before authentication of the user	**FIA_UAU.1** **FIA_UAU.1.1** The TSF shall allow [**1. identification of the user by means of TSF required by 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. **Application Note** “Local user” mentioned in component FIA_UAU.1.1 is the user using the trusted path provided between the SCA in the TOE environment and the TOE as indicated by FTP_TRP.1/SCA and FTP_TRP.1/TOE.

FIA_UID **User Identification**	
FIA_UID.1 **Timing of Identification**	PP SSCD Type3
FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified. **FIA_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. Hierarchical to: No other components Dependencies: No dependencies Management: a) the management of the user identities b) if an authorised administrator can change the actions allowed before identification, the managing of the action lists Audit: a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided b) Basic: All use of the user identification mechanism, including the user identity provided	**FIA_UID.1** **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.

FMT **Security Management**	
FMT_MOF **Management of Functions in TSF**	
FMT_MOF.1 **Management of Security Functions Behaviour**	PP SSCD Type3
FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*]. Hierarchical to: No other components Dependencies: - FMT_SMF.1 Specification of management func-	**FMT_MOF.1** **FMT_MOF.1.1** The TSF shall restrict the ability to [**enable**] the functions [**signature-creation function**] to [**Signatory**].

tions - FMT_SMR.1 Security roles Management: a) managing the group of roles that can interact with the functions in the TSF Audit: a) Basic: All modifications in the behaviour of the functions in the TSF	
FMT_MSA **Management of Security Attributes**	
FMT_MSA.1 **Management of Security Attributes**	PP SSCD Type3
FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*]. Hierarchical to: No other components Dependencies: - [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] - FMT_SMF.1 Specification of management functions - FMT_SMR.1 Security roles Management: a) managing the group of roles that can interact with the security attributes Audit: a) Basic: All modifications of the values of security attributes	**FMT_MSA.1/Administrator** **FMT_MSA.1.1/Administrator** The TSF shall enforce the [**Initialisation SFP**] to restrict the ability to [**modify**] the security attributes [**SCD/SVD management**] to [**Administrator**].
	FMT_MSA.1/Signatory **FMT_MSA.1.1/Signatory** The TSF shall enforce the [**Signature-Creation SFP**] to restrict the ability to [**modify**] the security attributes [**SCD operational**] to [**Signatory**].
	FMT_MSA.1/SIG Personalisation ***FMT_MSA.1.1/SIG Personalisation*** *The TSF shall enforce the [**SIG Personalisation SFP**] to restrict the ability to [**modify**] the security attributes [**access rules**] to [**none**].*

FMT_MSA.2 **Secure Security Attributes**	PP SSCD Type3
FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes. Hierarchical to: No other components Dependencies: - ADV_SPM.1 Informal TOE security policy model - [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] - FMT_MSA.1 Management of security attributes - FMT_SMR.1 Security roles Management: --- Audit: a) Minimal: All offered and rejected values for a security attribute b) Detailed: All offered and accepted secure values for a security attribute	**FMT_MSA.2** **FMT_MSA.2.1** The TSF shall ensure that only secure values are accepted for security attributes.
FMT_MSA.3 **Static Attribute Initialisation**	PP SSCD Type3
FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection: *choose one of: restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP. **FMT_MSA.3.2** The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created. Hierarchical to: No other components Dependencies: - FMT_MSA.1 Management of security attributes - FMT_SMR.1 Security roles Management: a) managing the group of roles that can specify initial values b) managing the permissive or restrictive setting of default values for a given access control SFP Audit:	**FMT_MSA.3** **FMT_MSA.3.1** The TSF shall enforce the [**Initialisation SFP and Signature-Creation SFP**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP. **Refinement** The security attribute of the SCD “SCD operational” is set to “no” after generation of the SCD. **FMT_MSA.3.2** The TSF shall allow the [**Administrator**] to specify alternative initial values to override the default values when an object or information is created.

a) Basic: Modifications of the default setting of permissive or restrictive rules b) Basic: All modifications of the initial values of security attributes	
FMT_MTD **Management of TSF Data**	
FMT_MTD.1 **Management of TSF Data**	PP SSCD Type3
FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*]. Hierarchical to: No other components Dependencies: - FMT_SMF.1 Specification of management functions - FMT_SMR.1 Security roles Management: a) managing the group of roles that can interact with the TSF data Audit: a) Basic: All modifications to the values of TSF data	**FMT_MTD.1** **FMT_MTD.1.1** The TSF shall restrict the ability to [**modify**] the [**RAD**] to [**Signatory**].
FMT_SMF **Specification of Management Functions**	
FMT_SMF.1 **Specification of Management Functions**	PP SSCD Type3
FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: *list of security management functions to be provided by the TSF*]. Hierarchical to: No other components Dependencies: No dependencies Management: --- Audit: a) Minimal: Use of the management functions	***FMT_SMF.1*** ***FMT_SMF.1.1*** *The TSF shall be capable of performing the following security management functions: [**security function management, security attribute management, TSF data management**].* ***Note*** *This SFR has been added to the SFRs defined in the SSCD Protection Profile due to* /AIS32/*which implicitly makes the final interpretation 065 mandatory.*

FMT_SMR **Security Management Roles**	
FMT_SMR.1 **Security Roles**	PP SSCD Type3
FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *the authorised identified roles*]. **FMT_SMR.1.2** The TSF shall be able to associate users with roles. Hierarchical to: No other components Dependencies: - FIA_UID.1 Timing of identification Management: a) managing the group of users that are part of a role Audit: a) Minimal: modifications to the group of users that are part of a role b) Detailed: every use of the rights of a role	**FMT_SMR.1** **FMT_SMR.1.1** The TSF shall maintain the roles [**Administrator, Signatory, Card Management System, AuthorisedCSP**]. **FMT_SMR.1.2** The TSF shall be able to associate users with roles.

FPT **Protection of the TSF**	
FPT_AMT **Underlying Abstract Machine Test**	
FPT_AMT.1 **Abstract Machine Testing**	PP SSCD Type3
FPT_AMT.1.1 The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorised user, other conditions*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. Hierarchical to: No other components Dependencies: No dependencies Management: a) management of the conditions under which ab-	**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. ***Application Note*** *The test of the underlying abstract machine is performed in the framework of the self test functionality of the TOE (refer to SFR FPT_TST.1).*

stract machine test occurs, such as during initial start-up, regular interval, or under specified conditions b) management of the time interval if appropriate Audit: a) Basic: Execution of the tests of the underlying machine and the results ofthe tests	
FPT_EMSEC **TOE Emanation**	
FPT_EMSEC.1 **TOE Emanation**	PP SSCD Type3
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*]. Hierarchical to: No other components Dependencies: No dependencies Management: --- Audit: ---	**FPT_EMSEC.1** **FPT_EMSEC.1.1** The TOE shall not emit [***information on IC power consumption, information on command execution time, information on electromagnetic emanations***] in excess of [***non useful information***] enabling access to [**RAD**] and [**SCD**]. **FPT_EMSEC.1.2** The TSF shall ensure [***S.OFFCARD***] are unable to use the following interface [***IC contacts as Vcc, I/O and GND, IC surface***] to gain access to [**RAD**] and [**SCD**]. **Application Note** The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission. Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation**,** simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.
FPT_FLS **Fail Secure**	

FPT_FLS.1 **Failure with Preservation of Secure State**	PP SSCD Type3
FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*]. <u>Hierarchical to:</u> No other components <u>Dependencies:</u> - ADV_SPM.1 Informal TOE security policy model <u>Management:</u> --- <u>Audit:</u> a) Basic: Failure of the TSF	**FPT_FLS.1** **FPT_FLS.1.1** The TSF shall preserve a secure state when the following types of failures occur: [- ***HW and/or SW induced reset*** - ***Power supply cut-off or variations*** - ***Unexpected abortion of the execution of the TSF due to external or internal events (in particular, break of a transaction before completion)*** - ***System breakdown*** - ***Internal HW and/or SW failure*** - ***Manipulation of executable code*** - ***Corruption of status information (as e.g. card status information, object life cycle state, actual security state related to key and PIN based authentication, ...)*** - ***Environmental stress*** - ***Input of inconsistent or improper data*** - ***Tampering*** - ***Manipulation resp. insufficient quality of the HW-RNG resp. SW-RNG*** - ***Fault injection attacks*** - ***Exposure to operating conditions where therefore a malfunction could occur*** - ***Failure detected by TSF according to FPT_TST.1***]. ***Refinements*** *The TOE shall preserve a secure state during power supply cut-off or variations. If power is cut or if power variations occur from the TOE, or if a transaction is stopped before completion, or on any other reset conditions, the TOE shall be reset cleanly.*
FPT_PHP **Physical Protection**	
FPT_PHP.1 **Passive Detection of Physical Attack**	PP SSCD Type3
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. <u>Hierarchical to:</u> No other components	**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.

Dependencies: No dependencies Management: --- Audit: a) Minimal: if detection by IT means, detection of intrusion.	
FPT_PHP.3 **Resistance to Physical Attack**	PP SSCD Type3
FPT_PHP.3.1 The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: *list of TSF devices / elements*] by responding automatically such that the TSP is not violated. Hierarchical to: No other components Dependencies: No dependencies Management: a) management of the automatic responses to physical tampering Audit: ---	**FPT_PHP.3** **FPT_PHP.3.1** The TSF shall resist [***physical manipulation and physical probing (e.g. tampering of the specified physical and technical operating conditions of the IC as voltage supply, clock frequency and temperature out of the valid limits)***] to the [***TSF***] by responding automatically such that the TSP is not violated.
FPT_TST **TSF Self Test**	
FPT_TST.1 **TSF Testing**	PP SSCD Type3
FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*]. **FPT_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF data*], *TSF data*]. **FPT_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.	**FPT_TST.1** **FPT_TST.1.1** The TSF shall run a suite of self tests [***during initial start-up, periodically during normal operation***] to demonstrate the correct operation of [***the TSF***]. ***Note*** *During initial start-up means before code execution.* ***Refinements*** *The TOE's self tests shall include the verification of the integrity of any software code (incl. patches) stored outside of the ROM. Upon detection of a self test error the TSF shall warn the entity connected. After OS testing is completed, all testing-specific commands and actions shall be disabled or removed. It shall not be possible to override these controls and*

Hierarchical to: No other components Dependencies: - FPT_AMT.1 Abstract machine testing Management: a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions b) management of the time interval if appropriate Audit: a) Basic: Execution of the TSF self tests and the results of the tests	*restore them for use. Command associated exclusively with one life cycle state shall never be accessed during another state.* **FPT_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of [***TSF data***]. ***Refinement*** *In this framework, the OS (i.e. the Smartcard Embedded Software of the TOE (TOE-ES)) itself is understood as „authorised user“.* **FPT_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. ***Refinement*** *The integrity check over the executable code stored outside the ROM area is covered by FPT_TST.1.1 and the related refinement.* *The requirement for checking the integrity of the ROM-code shall concern only the production phase, more precise the initialisation phase of the TOE´s lifecycle. Prior to the initialisation of the TOE, the ROM-code of the TOE shall be verifiable by authorised users as the OS developer. The integrity of the ROM-code shall be provable only during the initialisation process.*

FTP **Trusted Path/Channels**	
FTP_ITC **Inter-TSF Trusted Channel**	
FTP_ITC.1 **Inter-TSF Trusted Channel**	PP SSCD Type3
FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **FTP_ITC.1.2** The TSF shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel. **FTP_ITC.1.3**	**FTP_ITC.1/SVD Transfer** **FTP_ITC.1.1/SVD Transfer** The TSF shall provide a communication channel between itself and a remote trusted IT product **CGA** 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 CSP, or CGA***] to initiate communication via the trusted channel.

The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*]. Hierarchical to: No other components Dependencies: No dependencies Management: a) Configuring the actions that require trusted channel, if supported Audit: a) Minimal: Failure of the trusted channel functions b) Minimal: Identification of the initiator and target of failed trusted channel functions c) Basic: All attempted uses of the trusted channel functions d) Basic: Identification of the initiator and target of all trusted channel functions	**FTP_ITC.1.3/SVD Transfer** The TSF**, CSP, or the CGA** shall initiate communication via the trusted channel for [**export SVD**].
	FTP_ITC.1/DTBS Import **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 SCA** shall initiate communication via the trusted channel for [**signing DTBS-representation**]. **Application Note** For the communication channel either a trusted channel to the SSCD by cryptographic means or a channel to the SSCD within a trusted environment can be used. In the latter case the TOE identifies the establishment of a trusted environment by a successful user authentication.
	FTP_ITC.1/SIG Personalisation ***FTP_ITC.1.1/ SIG Personalisation*** *The TSF shall provide a communication channel between itself and a remote trusted IT product* ***Card Management System*** *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/SIG Personalisation*** *The TSF shall permit [**the remote trusted IT product (Card Management System)**] to initiate communication via the trusted channel.* ***FTP_ITC.1.3/SIG Personalisation*** *The TSF **or the Card Management System** shall initiate communication via the trusted channel for [**import of personalisation data**].*
FTP_TRP **Trusted Path**	
FTP_TRP.1 **Trusted Path**	PP SSCD Type3
FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *remote, 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** The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communication via the trusted path. **FTP_TRP.1.3** The TSF shall require the use of the trusted path for [selection: *initial user authentication*, [assignment: *other services for which trusted path is required*]]. Hierarchical to: No other components Dependencies: No dependencies Management: a) Configuring the actions that require trusted path, if supported Audit: a) Minimal: Failures of the trusted path functions b) Minimal: Identification of the user associated with all trusted path failures, if available c) Basic: All attempted uses of the trusted path functions d) Basic: Identification of the user associated with all trusted path invocations, if available	**FTP_TRP.1/TOE** **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***] to initiate communication via the trusted path. **FTP_TRP.1.3/TOE** The TSF shall require the use of the trusted path for [***none***]. **Application Note** For the communication path either a trusted path to the SSCD by cryptographic means or a path to the SSCD within a trusted environment can be used. In the latter case the TOE identifies the establishment of a trusted environment by a successful user authentication.

5.1.1.3 TOE Security Functional Requirements for the Completion Procedure of the SIG application.

The TOE has to fulfill additional security functional requirements in order to ensure that the completion process meets both the security objectives defined in /PP_SSCD_T3/ as well as the additional security objectives defined in Section 4.1.3. The TOE maintains the following additional security function policies:

Completion Procedure Extensions to Attribute Groups:

Object the attribtue is associated with	Attribute	Status
General Attribute		
User	Role	Administrator, Signatory, *AuthorisedCSP,*
RAD	*Status*	*transport, operational*
SIGApplication	*Active*	*yes, no*

<u>SFP TRANSPORT PROTECTION APP</u>

Subjects:

- User

Security attributes for subjects:

- none

Objects:

- Signature Application

Security attributes for objects:

- SIGApplicatiom.Active

Operations (Access Modes):

- Signing of DTBS by user.

Application Note: The policy which enforces that only the signatory is able to sign the DTBS is already covered in the SFP Signature-Creation. Therefore, the dependency to the security attribute User.Role is not duplicated here.

SFP TRANSPORT PROTECTION RAD

Subjects:

- User

Security attributes for subjects:

- User.Role (Administrator, Signatory, AuthorisedCSP)

Objects:

- Signature Application, RAD

Security attributes for objects:

- SIGApplicatiom.Active, RAD.Status

Operations (Access Modes):

- Modification of RAD by Signatory and signing of DTBS-representation by singatory

Application Note: The SFP restricts the value range of the operational RADs to provide a mean to distinguish them form transports RADs. The fact that only the singatory is allowed to change the RAD is already covered by **FMT_MTD.1** in /BSI_PP_IC/.

SFP EXPORT_BVD

Subjects:

- User

Security attributes for subjects:

- User.Role (Administrator, Signatory, AuthorisedCSP)

Objects:

- BVD data

Security attributes for objects:

- none

Operations (Access Modes):

- export of BVD data

FDP **User Data Protection**	
FDP_ACC **Access Control Policy**	
FDP_ACC.1 **Subset Access Control**	PP SSCD Type3 augmentation
FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]. Hierarchical to: No other components Dependencies: - FDP_ACF.1 Security attribute based access control Management: --- Audit: ---	**FDP_ACC.1/TRANSPORT_PROTECTION_APP SFP** **FDP_ACC.1.1/TRANSPORT_PROTECTION_APP SFP** The TSF shall enforce the [**TRANSPORT_PROTECTION_APP SFP**] on [**signing of DTBS-representation by signatory**].
	FDP_ACC.1/TRANSPORT_PROTECTION_RAD SFP **FDP_ACC.1.1/TRANSPORT_PROTECTION_RAD SFP** The TSF shall enforce the [**TRANSPORT_PROTECTION_RAD SFP**] on [**modification of RAD by Signatory and signing of DTBS-representation by singatory.]**
	FDP_ACC.1/EXPORT_BVD SFP **FDP_ACC.1.1/EXPORT_BVD SFP** The TSF shall enforce the [**EXPORT_BVD SFP**] on [**export of BVD by User**].

FDP_ACF **Access Control Functions**	
FDP_ACF.1 **Security Attribute Based Access Control**	PP SSCD Type3 augmentation
FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant secu-*	**FDP_ACF.1/TRANSPORT_PROTECTION_APP SFP** **FDP_ACF.1.1/TRANSPORT_PROTECTION_APP SFP** The TSF shall enforce the [**TRANS-**

rity attributes, or named groups of SFP-relevant security attributes]. **FDP_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]. **FDP_ACF.1.3** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]. **FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]. Hierarchical to: No other components Dependencies: - FDP_ACC.1 Subset access control - FMT_MSA.3 Static attribute initialisation Management: a) Managing the attributes used to make explicit access or denial based decisions Audit: a) Minimal: Successful requests to perform an operation on an object covered by the SFP b) Basic: All requests to perform an operation on an object covered by the SFP c) Detailed: The specific security attributes used in making an access check	**PORT_PROTECTION_APP SFP**] to objects based on the following: [**User Attribute and SIGApplication attribute**]. **FDP_ACF.1.2/TRANSPORT_PROTECTION_APP SFP** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**Only if SIGApplication.Active is set to "yes", then the signature application shall be usable according to the requirements of the Signature-creation SFP defined in** /PP_SSCD_T3/**.**]. **FDP_ACF.1.3/TRANSPORT_PROTECTION_APP SFP** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]. **FDP_ACF.1.4/TRANSPORT_PROTECTION_APP SFP** The TSF shall explicitly deny access of subjects to objects based on the [**No user shall be able to use the signature application if SIGApplication.Active is set to "no"**].
	FDP_ACF.1/TRANSPORT_PROTECTION_RAD SFP **FDP_ACF.1.1/TRANSPORT_PROTECTION_RAD SFP** The TSF shall enforce the [**TRANSPORT_PROTECTION_RAD SFP**] to objects based on the following: [**User Attribute and RAD attribute**]. **FDP_ACF.1.2/TRANSPORT_PROTECTION_RAD SFP** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**The signature application shall be usable only if RAD.status is set to "operational.**]. **FDP_ACF.1.3/TRANSPORT_PROTECTION_RAD**

	SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]. **FDP_ACF.1.4/TRANSPORT_PROTECTION_RAD SFP** The TSF shall explicitly deny access of subjects to objects based on the [**a) No user shall be able to use the signature application if RAD.status is set to “transport”.** **b) A user with security attribute “role” set to “Signatory” and with RAD.Status set to “operational” or “transport” shall not be able to modify the RAD to a transport RAD**].
	FDP_ACF.1/Export BVD **FDP_ACF.1.1/Export BVD SFP** The TSF shall enforce the [**Export BVD SFP**] to objects based on the following: [**authorised CSP attribute**]. **FDP_ACF.1.2/Export BVD SFP** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**The user with the security attribute “role” set to “AuthorisedCSP” is allowed to export the “BVD (Benutzer Verifikations Daten)”**]. **FDP_ACF.1.3/Export BVD SFP** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]. **FDP_ACF.1.4/Export BVD SFP** The TSF shall explicitly deny access of subjects to objects based on the [**none**].

FMT_MSA **Management of Security Attributes**	
FMT_MSA.1 **Management of Security Attributes**	PP SSCD Type3 Augmentation
FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*]. Hierarchical to: No other components	**FMT_MSA.1/SIGAPPLICATION_ACTIVE** **FMT_MSA.1.1/SIGAPPLICATION_ACTIVE** The TSF shall enforce the [TRANSPORT_PROTECTION_APP SFP] to restrict the ability to [**set**] the [**SIGApplication.Active to “yes”**] to [**AuthorisedCSP**].

Dependencies: - [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] - FMT_SMF.1 Specification of management functions - FMT_SMR.1 Security roles Management: a) managing the group of roles that can interact with the security attributes Audit: a) Basic: All modifications of the values of security attributes	
	FMT_MSA.1/OPERATIONAL_RAD **FMT_MSA.1.1/OPERATIONAL_RAD** The TSF shall enforce the [TRANSPORT_PROTECTION_RAD SFP] to restrict the ability to [**set**] the [**RAD.Status to “operational”**] to [**Signatory**].

5.1.2 SOF Claim for TOE Security Functional Requirements

The required level for the Strength of Function of the TOE security functional requirements listed in the preceding chap. 5.1.1 is “SOF-high”. This correlates to the claimed assurance level with its augmentation by the assurance component AVA_VLA.4 (refer to the following chap. 5.1.3).

5.1.3 TOE Security Assurance Requirements

The TOE security assurance level is fixed as

EAL4 augmented by ADV_IMP.2, ATE_DPT.2, AVA_MSU.3 and AVA_VLA.4.

The assurance level with its augmentations is chosen in view of the requirements in the Protection Profiles /PP_eHC/

The following table lists the security assurance requirements (SARs) for the TOE:

SAR	
Class ACM **Configuration Management**	ACM_AUT.1 Partial CM Automation

	ACM_CAP.4 Generation Support and Acceptance Procedures
	ACM_SCP.2 Problem Tracking CM Coverage
Class ADO **Delivery and Operation**	ADO_DEL.2 Detection of Modification
	ADO_IGS.1 Installation, Generation, and Start-up Procedures
Class ADV **Development**	ADV_FSP.2 Fully Defined External Interfaces
	ADV_HLD.2 Security Enforcing High-Level Design
	ADV_IMP.**2** Implementation of the TSF
	ADV_LLD.1 Descriptive Low-Level Design
	ADV_RCR.1 Informal Correspondence Demonstration
	ADV_SPM.1 Informal TOE Security Policy Model
Class AGD **Guidance Documents**	AGD_ADM.1 Administrator Guidance
	AGD_USR.1 User Guidance
Class ALC **Life Cycle Support**	ALC_DVS.1 Identification of Security Measures
	ALC_LCD.1 Developer Defined Life-Cycle Model
	ALC_TAT.1 Well-defined Development Tools
Class ATE **Tests**	ATE_COV.2 Analysis of Coverage
	ATE_DPT.**2** Testing: Low-Level Design
	ATE_FUN.1 Functional Testing
	ATE_IND.2 Independent Testing – Sample

Class AVA **Vulnerability Assessment**	AVA_MSU.**3** Analysis and Testing for Insecure States
	AVA_SOF.1 Strength of TOE Security Function Evaluation
	AVA_VLA.**4** Highly Resistant

5.1.4 Refinements of the TOE Security Assurance Requirements

All assurance components given in the table of chap. 5.1.3 are used as defined in /CC 2.3 Part3/ and /CEM 2.3/.

5.2 Security Requirements for the Environment of the TOE

5.2.1 Security Requirements for the IT-Environment

The following sections cover the security requirements specified for the IT-environment of the TOE. Only the TOE´s dedicated SIG Application is affected.

5.2.1.1 Certification Generation Application (CGA)

For the Certification Generation Application (CGA), the following SFRs are defined according to /PP_SSCD_T3/, chap. 5.3.1:

FCS **Cryptographic Support**	
FCS_CKM **Cryptographic Key Management**	
FCS_CKM.2 **Cryptographic Key Distribution**	
FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*]. Hierarchical to: No other components Dependencies:	**FCS_CKM.2/CGA** **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: [**/ECDir/**].

- [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation] - FCS_CKM.4 Cryptographic key destruction - FMT_MSA.2 Secure security attributes Management: a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption) Audit: a) Minimal: Success and failure of the activity b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)	
FCS_CKM.3 **Cryptographic Key Access**	
FCS_CKM.3.1 The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*]. Hierarchical to: No other components Dependencies: - [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation] - FCS_CKM.4 Cryptographic key destruction - FMT_MSA.2 Secure security attributes Management: a) the management of changes to cryptographic key attributes; examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption) Audit: a) Minimal: Success and failure of the activity b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)	**FCS_CKM.3/CGA** **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: [**none**].

FDP **User Data Protection**	
FDP_UIT **Inter-TSF User Data Integrity Transfer Protection**	
FDP_UIT.1 **Data Exchange Integrity**	
FDP_UIT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to [selection*: transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors. **FDP_UIT.1.2** The TSF shall be able to determine on receipt of user data, whether [selection: *modification*, *deletion, insertion, replay*] has occurred. Hierarchical to: No other components Dependencies: - [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] - [FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path] Management: --- Audit: a) Minimal: The identity of any user or subject using the data exchange mechanisms b) Basic: The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorised to do so c) Basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received; this could include security attributes associated with the user data d) Basic: Any identified attempts to block transmission of user data e) Detailed: The types and/or effects of any detected modifications of transmitted user data	**FDP_UIT.1/SVD Import** **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.

FTP **Trusted Path/Channels**	

FTP_ITC **Inter-TSF Trusted Channel**	
FTP_ITC.1 **Inter-TSF Trusted Channel**	
FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **FTP_ITC.1.2** The TSF shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel. **FTP_ITC.1.3** The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*]. Hierarchical to: No other components Dependencies: No dependencies Management: a) Configuring the actions that require trusted channel, if supported Audit: a) Minimal: Failure of the trusted channel functions b) Minimal: Identification of the initiator and target of failed trusted channel functions c) Basic: All attempted uses of the trusted channel functions d) Basic: Identification of the initiator and target of all trusted channel functions	**FTP_ITC.1/SVD Import** **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 TSF**] to initiate communication via the trusted channel. **FTP_ITC.1.3/SVD Import** The TSF **or the TOE** shall initiate communication via the trusted channel for [**import SVD**].

5.2.1.2 Signature Creation Application (SCA)

For the Signature Creation Application (SCA), the following SFRs are defined according to /PP_SSCD_T3/, chap. 5.3.2:

FCS **Cryptographic Support**	
FCS_COP	

Cryptographic Operation	
FCS_COP.1 **Cryptographic Operation**	
FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. Hierarchical to: No other components Dependencies: - [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation] - FCS_CKM.4 Cryptographic key destruction - FMT_MSA.2 Secure security attributes Management: --- Audit: a) Minimal: Success and failure, and the type of cryptographic operation b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes	**FCS_COP.1/SCA Hash** **FCS_COP.1.1/SCA Hash** The TSF shall perform [**hashing the DTBS**] in accordance with a specified cryptographic algorithm [***SHA-2 (224, 256, 384 resp. 512 bit)*** **or RIPEMD-160**] and cryptographic key sizes [**none**] that meet the following: [/ALGCAT/**, chap. 2**].

FDP **User Data Protection**	
FDP_UIT **Inter-TSF User Data Integrity Transfer Protection**	
FDP_UIT.1 **Data Exchange Integrity**	
FDP_UIT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or* i*nformation flow control SFP(s)*] to be able to [selection*: transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors. **FDP_UIT.1.2** The TSF shall be able to determine on receipt of user data, whether [selection: *modification*, *deletion, insertion, replay*] has occurred.	**FDP_UIT.1/SCA DTBS** **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.

Hierarchical to: No other components Dependencies: - [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] - [FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path] Management: --- Audit: a) Minimal: The identity of any user or subject using the data exchange mechanisms b) Basic: The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorised to do so c) Basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received; this could include security attributes associated with the user data d) Basic: Any identified attempts to block transmission of user data e) Detailed: The types and/or effects of any detected modifications of transmitted user data	

FTP **Trusted Path/Channels**	
FTP_ITC **Inter-TSF Trusted Channel**	
FTP_ITC.1 **Inter-TSF Trusted Channel**	
FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **FTP_ITC.1.2** The TSF shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel. **FTP_ITC.1.3** The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a*	**FTP_ITC.1/SCA DTBS** **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 TOE** shall initiate communication via

trusted channel is required]. Hierarchical to: No other components Dependencies: No dependencies Management: a) Configuring the actions that require trusted channel, if supported Audit: a) Minimal: Failure of the trusted channel functions b) Minimal: Identification of the initiator and target of failed trusted channel functions c) Basic: All attempted uses of the trusted channel functions d) Basic: Identification of the initiator and target of all trusted channel functions	the trusted channel for [**signing DTBS-representation by means of the SSCD**].
FTP_TRP **Trusted Path**	
FTP_TRP.1 **Trusted Path**	
FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *remote, 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** The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communication via the trusted path. **FTP_TRP.1.3** The TSF shall require the use of the trusted path for [selection: *initial user authentication*, [assignment: *other services for which trusted path is required*]]. Hierarchical to: No other components Dependencies: No dependencies Management: a) Configuring the actions that require trusted path, if supported Audit: a) Minimal: Failures of the trusted path functions b) Minimal: Identification of the user associated with	**FTP_TRP.1/SCA** **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 [**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**].

all trusted path failures, if available c) Basic: All attempted uses of the trusted path functions d) Basic: Identification of the user associated with all trusted path invocations, if available	

5.2.2 Security Requirements for the Non-IT-Environment

The following section covers the security requirements specified for the Non-IT-environment of the TOE. Only the TOE´s dedicated SIG Application is affected.

The specific security requirements for the Non-IT-environment of the TOE are defined according to /PP_SSCD_T3/, chap. 5.4, with the following exception: the new security requirement R.Trusted_Environment has been added according to the extension of the Protection Profile concerning the establishment of trusted channels / paths for the communication between the TOE and a SCA. Furthermore, a specific security requirement related to the personalisation of the TOE´s dedicated SIG Application is added.

R.Trusted_Environment Trusted Environment for SCA and TOE

In the case that a trusted channel resp. trusted path between the TOE and the SCA by cryptographic means is not established the environment for the TOE usage shall be secured with the target to keep confidentiality and integrity of the VAD and integrity of the DTBS.

R.SIG_PERS Security of the Personalisation Process for the SIG Application

The originator of the personalisation data and the personalisation center responsible for the personalisation of the TOE´s dedicated SIG Application shall handle the personalisation data in an adequate secure manner. This concerns especially the security data to be personalised as secret cryptographic keys and PINs. The storage of the personalisation data at the originator and at the personalisation center as well as the transfer of these data between the different sites shall be conducted with respect to data integrity, authenticity and confidentiality.

Furthermore, the personalisation center shall treat the data for securing the personalisation process, i.e. the personalisation keys suitably secure.

It is in the responsibility of the originator of the personalisation data to garantuee for a sufficient quality of the personalisation data, especially of the cryptographic material to be personalised. The preparation and securing of the personalisation data appropriate to the card´s structure and according to the TOE´s personalisation requirements shall be as well in the responsibility of the external world and shall be done with care.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 TOE Security Functions / TOE-IC

For the definition of the TOE Security Functions (TSF) related to the TOE-IC refer to /ST_IC/, chap. 6.1.1.

The TSFs defined for the TOE-IC cover the following functions which are relevant for the TOE: F.RNG, F.HW_DES, F.OPC, F.PHY, F.LOG, F.COMP, F.MEM_ACC, F.SFR_ACC, F.DES, F.RSA_encrypt, F.RSA_sign, F.RSA_public, F.RSA_KeyGen, F.SHA, F.RNG_Access, F.Object_Reuse, F.COPY.

6.1.2 TOE Security Functions / TOE-ES

The following section gives a survey of the TSFs of the TOE´s Smartcard Embedded Software.

TOE Security Functions / TOE-ES	
Access Control	
F.ACS_SFP	**Security Attribute Based Access Control**
	The TSF enforces the SFPs SFP_access_rules, SIG Access Control and SIG Personalisation as defined in chap. 5.1.1.2 and 5.1.1.3. The TSF extends the TSF F.ACS of /ST-IC/, chap. 6.1.2. The TSF controls the access to data stored in the TOE and to functionality provided by the TOE. The access control is realised by usage of access rules as security attributes. Access to a DF, an EF, a key, a PIN or other user data is only possible if the related access rule is fulfilled. In particular, the TSF checks prior to command execution if the command specific requirements concerning user authentication and secure communication are satisfied. For SIG Access Control, the TSF covers especially the following functionality: • The TSF manages the following security attributes: - For subject User: General Attribute "Role" (Administrator, Signatory, AuthorisedCSP), Initialisation Attribute "SCD/SVD Management" (authorised, not authorised) - For object SCD: "SCD Operational" (no, yes) - For object DTBS: "Sent by an authorised SCA" (no, yes)

	- For object SIGApplication: "Active" (no, yes) • The user with the security attribute "Role" set to "Administrator", set to "AuthorisedCSP", or set to "Signatory" is allowed to export the SVD. Establishment and usage of a trusted channel for the export of the SVD is required. • The user with the security attribute "Role" set to "Administrator" or set to "Signatory" is allowed to generate the SCD/SVD pair if the security attribute "SCD / SVD management" is set to "authorised". • The user with the security attribute "Role" set to "Signatory" is allowed to create electronic signatures if the security attributes "Sent by an authorised SCA" and "SCD operational" are both set to "yes". This is only allowed during the end-usage phase of the TOE. • Establishment of a trusted path or trusted channel is allowed prior to identification and authentication of the user. Other TSF mediated actions explicitly require a preceding successful authentication. • The user with the security attribute "Role" set to "Signatory" is allowed to enable the signature-creation function. Required is a preceding authentication of the Signatory. • The user with the security attribute "Role" set to "Signatory" is allowed to modify the security attribute "SCD operational". • The user with the security attribute "Role" set to "Signatory" is allowed to modify RAD. • The user with the security attribute "Role" set to "Administrator" is allowed to modify the security attribute "SCD/SVD management". • The user with the security attribute "Role" set to "Administrator" is allowed to create the RAD. This is only allowed during the personalisation phase of the TOE. • The TSF provides an authentication mechanism for the Administrator. • The user with the security attribute "Role" set to "Administrator" is allowed to perform a secure modification of the security attributes "Role" and "SCD/SVD management". • The Security Attribute "SCD operational" is set to "no" after generation of the SCD. The user with the security attribute "Role" set to "Administrator" is allowed to specify an alternative value. • The SVD is exported without associated security attributes. • The user with security attribute "Role" set to "AuthorisedCSP" is allowed to export the BVD data • The user with security attribute "Role" set to "AuthorisedCSP" is allowed to perform a secure modification of the security attribute "SIGApplication.Active"
Identification and Authentication	
F.IA_AKEY	**Key Based User / TOE Authentication Based on Asymmetric Cryptography**
	The TSF provides the functionality of a key based external and internal authentication on the base of asymmetric cryptography. By an external authentication, users of the TOE can be authenticated with regard to the TOE. Vice versa, by an internal authentication, the TOE itself can be authenticated with regard to the external world. Both authentication mechanisms base on a challenge-response procedure using random numbers. The TSF enforces the following different internal and external authentication mecha-

	nisms: - Internal authentication without session key agreement according to /ISO 9796-2/, /eHC1/, chap. 7 and 15 - External authentication without session key agreement according to /ISO 9796-2/, /eHC1/, chap. 7 and 15 - Internal authentication including one step of session key and send sequence counter agreement according to /ISO 9796-2/, E.3, /eHC1/ chap. 7 and 15 - External authentication including one step of session key and send sequence counter agreement according to /ISO 9796-2/, /eHC1/, chap. 7 and 15. - Internal authentication according /eHC1/, chap. 7 and 15. Note: Each external authentication process requires a preceding Get Challenge – operation. The private and public keys necessary on the card´s side for authentication purposes are either generated on-card (with support by the TSF F.RSA_KEYGEN) or imported during the initialisation, personalisation or end-usage phase of the TOE. In particular, the import of public keys can be performed in the form of CV certificates what is connected with the verification of the respective CV certificate under usage of the TSF F.VER_DIGSIG. In each case, the keys involved on the card´s side in the authentication processes have to be explicitly referenced prior to their usage. The access to the keys necessary for the authentication processes is controlled by the specific SFP which is defined for the respective application using the authentication keys. The execution of the specific SFP is task of the TSF F.ACS_SFP for access control. In the case of a successful external authentication attempt the TSF sets a corresponding actual security state for key based user authentication. The TSF makes use of asymmetric cryptography with generation and verification of RSA digital signatures resp. RSA encryption and decryption and is therefore directly connected with the TSF F.CRYPTO. Depending on the type of authentication mechanism, the combination of a successful internal and external authentication process can include the generation of session keys (incl. send sequence counter). Depending on the type of authentication mechanism, the TSF stores the generated session keys volatile and on demand as well persistently on the card. The generated keys can be used for securing the following data exchange between the TOE and the external world (in the current or a later session) with the objective of data confidentiality and data integrity and authenticity (Secure Messaging). In addition, as well depending on the type of authentication mechanism, the generated keys can be used further on for authentication processes based on symmetric cryptography.
F.IA_SKEY	**Key Based User / TOE Authentication Based on Symmetric Cryptography**
	The TSF provides the functionality of a key based external and internal authentication on the base of symmetric cryptography. By an external authentication, users of the TOE can be authenticated with regard to the TOE. Vice versa, by an internal authentication, the TOE itself can be authenticated with regard to the external world. Both authentication mechanisms base on a challenge-response procedure using random numbers. The TSF enforces the following different internal and external authentication mechanisms:

	- Internal authentication with / without individual key derivation and without session key generation according /eHC1/, , /ISO 9796-2/ - External authentication with / without individual key derivation and without session key generation according to /eHC1/, /ISO 9796-2/ - Mutual authentication with / without individual key derivation and without session key generation according /eHC1/, /ISO 9796-2/ - Internal authentication with / without individual key derivation and including the first step of session key and send sequence counter generation according /eHC1/, , /ANSI X9.63/, /ISO 9796-2/ - External authentication with / without individual key derivation and including the last step of session key and send sequence counter generation according to /eHC1/, , /ANSI X9.63/, /ISO 9796-2/ - Mutual authentication with / without individual key derivation and including session key and send sequence counter generation according to /eHC1/ , /ANSI X9.63/, /ISO 9796-2/ Note: Each external authentication process requires a preceding Get Challenge – operation. The symmetric keys necessary on the card´s side for the authentication mechanisms can either be generated on-card by a derivation process for deriving individual keys before the main authentication process starts. This key derivation process is performed by the TSF F.CRYPTO. Alternatively, symmetric keys imported during the initialisation, personalisation or end-usage phase of the TOE or agreed within a preceding authentication process can be used. The access to the keys necessary for the authentication processes is controlled by the specific SFP which is defined for the respective application using the authentication keys. The execution of the specific SFP is task of the TSF F.ACS_SFP for access control. In the case of a successful external authentication attempt the TSF sets a corresponding actual security state for key based user authentication. The TSF makes use of symmetric cryptography with DES based encryption, decryption, MAC generation resp. MAC verification. Hence, the TSF F.IA_SKEY is directly connected with the TSF F.CRYPTO. Depending on the type of authentication mechanism, the combination of a successful internal and external authentication process can include the generation of session keys (incl. send sequence counter). Depending on the type of authentication mechanism, the TSF stores the generated session keys volatile and on demand as well persistently on the card. The generated keys can be used for securing the following data exchange between the TOE and the external world (in the current or a later session) with the objective of data confidentiality and data integrity and authenticity (Secure Messaging). In addition, as well depending on the type of authentication mechanism, the generated keys can be used further on for authentication processes based on symmetric cryptography.
F.IA_PWD	**Password Based User Authentication**
	Users of the TOE can be authenticated (towards the TOE) by means of a card holder authentication process. For the card holder authentication process, the TSF compares the card holder verification information, here a password (PIN), provided by a subject with a corresponding secret reference value stored permanently on the card. The TSF uses for the authentication process the password referenced by the external world. The access to the relevant password resp. its reference value is controlled by the specific SFP which

is defined for the respective application using the password. The execution of the specific SFP is task of the TSF F.ACS_SFP for access control.

The card holder authentication process can be performed by usage of the command Verify or Change Reference Data (whereat the latter command makes a password change possible).

Each password used for authentication purposes is connected with an own error usage counter and an own usage counter. Furthermore, each password is connected with an own resetting code (PUK) whereat the resetting code itself is connected with an own usage counter (but no error usage counter).

The number of applications of a password for authentication purposes with the command Verify is limited by its usage counter. The TSF allows at maximum for a number of authentication attempts with a password as restricted by its usage counter. The value for the usage counter can be predefined as infinite, i.e. the password can be used without any limit. A password with an expired usage counter cannot be longer used for authentication purposes with the command Verify (but with the command Change Reference Data).

In the case of a password with a finite usage counter, each authentication attempt with the command Verify decrements the usage counter of the password, independently whether the authentication attempt succeeds or fails. A successful authentication attempt with the command Change Reference Data re-initialises the usage counter to its predefined initial value.

The TSF detects for a password when a predefined number of consecutive unsuccessful authentication attempts occurs related to the card holder authentication process. Each consecutive unsuccessful comparison of the presented password with the reference value stored on the card is recorded by the TSF in order to limit the number of further authentication attempts with this password.

In the case of a successful authentication attempt a corresponding actual security state for the password is set and the error usage counter of the password is re-initialised to its predefined initial value.

If an authentication attempt with the password fails, the corresponding actual security state is reset and the error usage counter of the password is decreased. When the defined maximum number of unsuccessful authentication attempts has been met or surpassed, the TSF blocks the corresponding password for any further authentication attempt.

A password with an expired error usage counter can be unblocked by usage of the related resetting code, provided that the usage counters of the password and of the resetting code are not expired. Otherwise, there is no way to unblock the password so that this password is invalid for each further authentication attempt.

The unblocking of a blocked password can be performed by usage of the command Reset Retry Counter only. In the case of a successful authentication attempt with the resetting code related to the blocked password, the expired error usage counter is re-initialised to its initial value (as well as for the usage counter of the password) and hence, the password can be used further on for authentication attempts.

The number of applications of a resetting code for authentication purposes is limited by its usage counter. The TSF allows at maximum for a number of authentication attempts with the resetting code as restricted by its usage counter. Each unblocking attempt with the command Reset Retry Counter decrements the usage counter of the resetting code, independently whether the authentication attempt with the resetting code succeeds or fails. The unblocking process for a blocked password can be combined with a change of this password. However, even if the command Reset Retry Counter resp. the authentication

	with the resetting code succeeds, the actual security state for the password will not be set. For security reasons, a password shall be connected with an error usage counter with a sufficiently small value as initial value. Furthermore, the usage of the related resetting code itself shall be limited by an usage counter with a sufficiently small initial value. In general, a security state set due to a successful authentication attempt can be valid for several following TOE commands. However, as well, it is possible to restrict the validity of such an authentication state to one single following TOE command, i.e. after the next command has accessed this security state it will be reset by the TSF. The TSF does not check the quality of passwords or resetting codes used. The sufficient quality of passwords and resetting codes lies in the responsibility of the external world only. The transfer of passwords and resetting codes to the TOE can be executed in unsecured mode, i.e. without usage of Secure Messaging, or alternatively in secured mode, i.e. with usage of Secure Messaging. In the latter case, the TSFs F.EX_CONF and F.EX_INT are involved. For the TOE´s eHC Application and SIG Application, the concrete usage of PIN and PUK, in particular the definition of error usage counters and usage counters and their initial values, the (minimal) lengths of PIN and PUK and the access to the commands Verify, Change Reference Data and Reset Retry Counter is regulated by the specification /eHC2/. *Transport PIN Mechanism:* Additionally, the TSF differentiates two kinds of PIN. As long as the PIN is in the transport state, the PIN cannot be used for authentication purposes but only for changing the PIN into an operational PIN. Such a change of the PIN directly implies the change of the PIN status to the operational state. The TSF explicitly prohibits that the PIN is changed into a transport PIN. The TSF also enables the external world to query the state of the PIN. *Stack and Comfort PIN Mechanism:* The TSF supports stack and comfort PINs according to /TR_STACK_PIN/ resp. /TR_COMF_PIN/. Essentially, the TSF maintains an additional counter which enables the reuse of a single successful authentication for a fixed number of times. The TSF decrements counter each time a authentication is required for the operations protected by the corresponding PIN and enforces a new authentication if the counter is zero. The intention is to enable for example the generation of a fixed number of electronic signatures based on a single authentification to releave the signatory from the burden to enter the PIN for each single document if several documents have to be signed. The specification /eHC2/ limits the fixed number of subsequent operations that can be performed after a successful authentication to 1 for the PIN.QES. As a consequence, the stack and comfort PIN mechanism degenerates to a normal PIN which requires a successful authentication each time the card holder intends to use the signature application.
Integrity of Stored Data	
F.DATA_INT	**Stored Data Integrity Monitoring and Action**
	The TSF monitors data stored within the TOE for integrity errors. This concerns all - DFs

	- EFs - Passwords incl. related attributes - Cryptographic keys incl. related attributes - Security critical data stored within the card and channel context (session keys incl. attributes, status information as actual security states for key and password based authentication, hash values, further security relevant card and channel information) The monitoring is based on the following attributes: - Checksum (CRC) attached to the header of a file - Checksum (CRC) attached to the data body of a file - Checksums (CRC) attached to each secret (password, cryptographic key) and its related attributes stored in the EEPROM - Checksums (CRC) attached to card and channel context related security critical information Each access of the TOE to a DF, to an EF, to a secret (password or cryptographic key incl. its related attributes) or to security critical card resp. channel context data the TSF is secured with an integrity check on base of the mentioned attributes. Upon detection of a data integrity error, the TSF informs the user about this fault (output of a warning). If the checksum of the header of a file has been detected as corrupted, the data contained in the affected file are no longer accessible. If the data contained in a file are not of integrity, the affected data will be treated in the following way: - For the Read access, the affected data will be exported, but the data export will be connected with a warning. - For the Update access, the integrity error of the affected data will be ignored, and the data imported by the command will be stored and a new checksum will be computed. - For all remaining access modes, the affected data will not be used for data processing. If a secret (password, cryptographic key) and its related attributes are corrupted, the secret and its related data will not be processed. If security critical card or channel context data are not of integrity, the Smartcard Embedded Software immediately jumps into an endless-loop (re-activation by reset possible).
Data Exchange	
F.EX_CONF	**Confidentiality of Data Exchange**
	The TSF provides the capability to ensure that secret data which is exchanged between the TOE and the external world remains confidential during transmission. For this purpose, encryption based on symmetric cryptography is applied to the secret data. The TSF ensures that the user and the user data's access condition have indicated confidentiality for the data exchange. Securing the data transfer with regard to data confidentiality is done by Secure Messaging according to the standard ISO/IEC 7816-4.

	The cryptographic key used for securing the data transfer is either a symmetric session or static key. In case of a session key, the key is negotiated during a preceding mutual authentication process (based on a random challenge and response procedure) between the TOE and the external world (realised by the TSFs F.IA_SKEY, F.IA_AKEY, F.CRYPTO). For encryption and decryption, the TSF makes use of the TSF F.CRYPTO for DES functionality.
F.EX_INT	**Integrity and Authenticity of Data Exchange**
	The TSF provides the capability to ensure that data which is exchanged between the TOE and the external world remains integer and authentic during transmission. For this purpose, cryptographic checksums based on symmetric cryptography are applied to the data. The TSF ensures that the user and the user data's access condition have indicated integrity and authenticity for the data exchange. Securing the data transfer with regard to data integrity and authenticity is done by Secure Messaging according to the standard ISO/IEC 7816-4. The cryptographic key used for securing the data transfer is either a symmetric session or static key. In case of a session key, the key is negotiated during a preceding mutual authentication process (based on a random challenge and response procedure) between the TOE and the external world (realised by the TSFs F.IA_SKEY, F.IA_AKEY, F.CRYPTO). For checksum securing and verification, the TSF makes use of the TSF F.CRYPTO for DES functionality.
Object Reuse	
F.RIP	**Residual Information Protection**
	The TSF ensures that any previous information content of a resource is explicitly erased upon the deallocation of the resource used for any of the following components: - All volatile and non-volatile memory areas used for operations in which security relevant material (as e.g. cryptographic data, passwords or other security critical data) is involved. Explicit erasure is defined as physical erasure. The TSF is supported by the TSF F.Object_Reuse of the underlying IC and its Dedicated Support Software.
Protection	
F.FAIL_PROT	**Hardware and Software Failure Protection**
	The TSF preserves a secure operation state of the TOE when the following types of failures and attacks occur: - HW and/or SW induced reset - Power supply cut-off

	- Power supply variations - Unexpected abortion of the execution of the TSF due to external or internal events (in particular, break of a transaction before completion) - System breakdown - Internal HW and/or SW failure - Manipulation of executable code - Corruption of status information (as e.g. card status information, object life cycle state, actual security state related to key and password based authentication, ...) - Environmental stress - Input of inconsistent or improper data - Tampering - Manipulation resp. insufficient quality of the HW-RNG The TSF makes use of HW and SW based security features and corresponding mechanisms to monitor and detect induced HW and SW failures and tampering attacks. In particular, the TSF is supported by the IC specific TSFs F.OPC and F.PHY. Upon the detection of a failure of the above mentioned type the TSF reacts in such a way that the TSP is not violated. The TOE changes immediately to a locked state and cannot be used any longer within the actual session. Depending on the type of the detected attack to the underlying IC (incl. its Dedicated Software) or to the Smartcard Embedded Software code the TOE will be irreversible locked resp. can be reactivated by a reset.
F.SIDE_CHAN	**Side Channel Analysis Control**
	The TSF provides suitable HW and SW based mechanisms to prevent attacks by side channel analysis like Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and Timing analysis (TA). The TSF ensures that all countermeasures available are used in such a way that they support each other. In particular, the TSF is supported by the TSF F.LOG of the underlying IC and its Dedicated Support Software. The TSF acts in such a manner that all security critical operations of the TOE, in particular the TOE´s cryptographic operations, are suitably secured by these HW and SW countermeasures. The TSF guarantees that information on IC power consumption, information on command execution time and information on electromagnetic emanations do not lead to useful information on processed security critical data as secret cryptographic keys or passwords. In particular, the IC contacts as Vcc, I/O and GND or the IC surface do not make it possible for an attacker to gain access to security critical data as secret cryptographic keys or passwords. The TSF enforces the installation of a secure session before any cryptographic operation is started. In particular, the installation of a secure session does not only concern the core cryptographic operation itself. All preparing security relevant actions performed prior to the core cryptographic operation as e.g. the generation of session keys, the process of loading keys into the dedicated IC cryptographic modules and the data preparation as reformatting or padding are involved as well. Furthermore, the secure session covers all security relevant actions which follow the core cryptographic operation as e.g. the post-processing of the output data.

F.SELFTEST	**Self Test**
	The TSF covers different types of self tests whereat each self test consists of a check of a dedicated integrity attribute related to (parts of) the TOE´s code resp. data. The TSF integrates self tests with the following objectives: The TSF provides the capability of conducting a self test during initial start-up, i.e. after each reset, to demonstrate the correct operation of its TSFs. This self test is performed automatically by the TOE and consists of the verification of the integrity of any software code stored in the EEPROM area. Furthermore, the TSF provides authorised users - here the Smartcard Embedded Software of the TOE (TOE-ES) itself - with the capability to verify the integrity of TSF data during run-time. The self test is performed automatically by the TOE and is supported by the TSF F.DATA_INT. Additionally, the TSF provides authorised users with the capability to verify the integrity of stored TSF executable code. This concerns only the production phase, more precise the initialisation phase of the TOE (phase 5 of the product´s life cycle). Prior to the initialisation of the TOE, the ROM-code of the TOE can be verified on demand by the Smartcard Embedded Software developer. The integrity of the whole EEPROM-code is checked automatically by the TOE during the storage of the initialisation file in the framework of the TOE´s initialisation. These self tests are supported by the TSF F.CRYPTO (SHA-1 hash value calculation, MAC verification). The TSF supports all other TSFs defined for the Smartcard Embedded Software (TOE-ES).
Cryptographic Operations	
F.CRYPTO	**Cryptographic Support**
	The TSF provides cryptographic support for the other TSFs using cryptographic mechanisms. The TSF supports: DES/3DES algorithm according to the standard /FIPS 46-3/ resp. /ANSI X9.52/ with a key length of 168 bit (used for encryption, decryption, MAC generation and verification according to /FIPS 46-3/, /ANSI X9.52/, /ANSI X9.19/, /eHC1/ RSA core algorithm according to the standard /PKCS1/ with key lengths of 2048 bit modulus lengths (used for RSA encryption, decryption, signature generation and verification, see other TSFs related to RSA based mechanisms) Random number generation by a pseudo RNG. The generator is seeded by the hardware random number generator (see /UG_CL/, /UG-CL-RND/) SHA-256 hash value calculation according to /ALGCAT/, chap. 2 Negotiation of 3DES session keys The resistance of the TSF against SPA, DPA, DFA and TA is part of the TSF F.SIDE_CHAN. The random number generation is in particular used for RSA and DES key generation and authentication mechanisms. The mechanism for the generation of session keys is directly connected with the TSFs F.IA_AKEY and F.IA_SKEY which realise internal and external authentication processes.

	Furthermore, the generation of random numbers of high quality, and depending on the authentication type, the SHA-256 hash value calculation of TSF F.CRYPTO are involved. The TSF is directly supported by the TSFs of the underlying IC and its Cryptographic Library which supply cryptographic functionality. In particular, the TSFs F.RNG, F.HW_DES, F.DES, F.RSA_encrypt, F.RSA_sign, F.RSA_public, F.RSA_KeyGen, F.SHA and F.RNG_Access are involved.
F.RSA_KEYGEN	**RSA Key Pair Generation**
	The TSF generates RSA key pairs with key lengths of 2048 bit modulus length for asymmetric cryptography which can be used later on e.g. for digital signatures or authentication purposes. The TSF enforces the key pair generation process and the related key material to meet the following requirements: - The RSA key pair generation process follows a well-designed key generation algorithm of sufficient quality; in particular, the requirements for RSA keys and their generation in /ALGCAT/ , chap. 3.1 and 4 as well as in the corresponding European algorithm paper, chap. 4.5.2, 4.6, Annex C.2 and C.3 are taken into account. - Random numbers used in the key pair generation process for the generation of the primes are of high quality to ensure that the new key pair is unpredictable and unique with a high probability. - The generation of the random numbers necessary for the primes is performed by usage of a deterministic RNG running on the TOE. - Prime numbers produced in the key pair generation process are unique with a high probability and satisfy the requirements in/ALGCAT/, chap. 3.1 and 4. In particular, the so-called epsilon-condition is considered. - The primes are independently generated. - Sufficiently good primality tests with convincing limits are implemented to guarantee with a high probability for the property of the generated prime candidates to be prime. In particular, the actual version of the significance limit for primality tests is considered. - In the key pair generation process, for the public exponent given by the external world the corresponding private exponent is calculated and converted into its CRT parameters. - For each key length, the generated key pairs show a “good” distribution within the key range; in particular, the generated new key pair is unique with a high probability. - Only cryptographically strong key pairs with the intended key length are generated. In particular, for any generated key pair, the private key cannot be derived from the corresponding public key. - The key pair generation process includes a dedicated check if the generated private and public key match; only valid key pairs are issued. - During the key pair generation process, it is not possible to gain information about the chosen random numbers, about the calculated primes, about other secret values which will be used for the key pair to be generated or about the generated key pair and its parts itself. - During the key pair generation process, it is not possible to gain information about the design of the routines realising the key pair generation. - The key pair generation process includes a physical destruction of the old private

	key part before the new key pair is generated. The resistance of the TSF against SPA, DPA, DFA and TA is part of the TSF F.SIDE_CHAN. The TSF makes use of the TSF F.CRYPTO for random number generation and RSA signature generation and verification. The public part of the generated key pair can be exported with an authentication attribute which either can be a MAC (generation supported by the TSF F.CRYPTO) or a digital signature (generation supported by the TSF F.GEN_DIGSIG) over the public key data.
F.GEN_DIGSIG	**RSA Generation of Digital Signatures**
	The TSF provides a digital signature functionality based on asymmetric cryptography, particularly based on the RSA algorithm with key lengths of 2048 bit modulus length. The TSF digital signature function will be used for several purposes with different formats for the digital signature input: - Explicit generation of digital signatures using the signature scheme with appendix according to the standard /PKCS1/, chap. 8.2.1 and with hash algorithm SHA-2 (256 bit), see /eHC1/, chap. 7 - Explicit generation of digital signatures using the signature scheme with appendix according to the standard /PKCS1/ with random number based on the hash algorithm SHA-2 (224, 256, 384 resp. 512 bit) resp. RIPEMD160 (external hash value calculation), see /eHC1/, chap. **7** - Implicit generation of digital signatures within authentication mechanisms for the creation of authentication tokens using the signature scheme with message recovery according to the standard /PKCS1/ based on the hash algorithm SHA-256, see /eHC1/, chap. 7 and 16 - Implicit generation of digital signatures within authentication mechanisms for the creation of authentication tokens using the signature scheme with message recovery according to the standard /ALGCAT/, chap. 8.2.1 without hash and OID, but with an additional limitation of the length of the input message, see /eHC1/, chap. 7 and 16 The TSF function for generation of a digital signature uses the private key which has been referenced before. The random numbers necessary for the padding of the data within the signature process are generated by using the TSF F.CRYPTO for random number generation. Furthermore, for the signature calculation itself, the TSF makes use of the TSF F.CRYPTO, and the computation of hash values is as well based on the TSF F.CRYPTO. Each private key used for the signature generation function is either generated on-card by usage of the TSF F.RSA_KEYGEN or is generated by the external world and loaded onto the card during the initialisation, personalisation or end-usage phase of the TOE. In the latter case, it is in the responsibility of the external world to guarantee for a sufficient cryptographic strength of the private key and to handle the private key outside the card in a sufficient secure manner. The resistance of the TSF against SPA, DPA, DFA and TA is part of the TSFs F.Log and F.SIDE_CHAN. For each private key - generated on-card or imported with the assumption that the external world meets the requirements on the key handling as defined before - the TSF digital signature function works in such a manner that the private key cannot be

	derived from the signature and the signature cannot be generated by other individuals not possessing that secret. Furthermore, the TSF digital signature function works in such a manner that no information about the private key can be disclosed during the generation of the digital signature.
F.VER_DIGSIG	**RSA Verification of Digital Signatures**
	The TSF provides a functionality to verify digital signatures based on asymmetric cryptography, particularly based on the RSA algorithm with key lengths of 2048 bit modulus length. The TSF function to verify a digital signature will be used for several purposes with different formats for the digital signature input: - Implicit verification of digital signatures within authentication mechanisms for the verification of authentication tokens using the signature scheme with message recovery according to the standard /PKCS1/ a hash algorithm provided by F.CRYPTO - Implicit verification of digital signatures within the verification and unwrapping of imported CV certificates using the signature scheme with message recovery according to the standard /ISO 9796-2/ based a the hash algorithm provided by F.CRYPTO The TSF function to verify a digital signature uses the public key which has been referenced before. For the verification mechanism itself, the TSF makes directly use of the TSF F.CRYPTO, and the computation of hash values is as well based on the TSF F.CRYPTO. Each public key used for the function to verify a digital signature is either generated on-card by usage of the TSF F.RSA_KEYGEN or is generated by the external world and loaded onto the card during the initialisation, personalisation or end-usage phase of the TOE. In particular, loading via a CV certificate by a suitable preceding operation is possible. Due to the requirements of the specification /eHC1/, Chapters 7 and 8, the verification of digital signatures for the eHC product is restricted to: - RSA_ISO9796_2_DSS1 with hashing function SHA-256 according to /ISO 9796-2/
F.RSA_ENC	**RSA Encryption**
	The TSF provides a functionality to encrypt data based on asymmetric cryptography, particularly based on the RSA algorithm with key lengths of 2048 bit modulus length. The TSF encryption function will be used for several purposes with different formats for the encryption input: - Explicit encryption of a plain text using the “encryption scheme” with formatted plain message according to the standard /PKCS1/, chap. 7.2.1 and with hash algorithm SHA-256, see /eHC1/, chap. 7 - Implicit encryption within authentication mechanisms for the generation of authentication tokens using the “encryption primitive” according to the standard /PKCS1/, chap. 5.1.1 The TSF encryption function uses the public key which has been referenced before. For the encryption mechanism itself, the TSF makes directly use of the TSF F.CRYPTO. Each public key used for the encryption function is either generated on-card by usage of

	the TSF F.RSA_KEYGEN or is generated by the external world and loaded onto the card during the initialisation, personalisation or end-usage phase of the TOE. In particular, loading via a CV certificate by a suitable preceding operation is possible.
F.RSA_DEC	**RSA Decryption**
	The TSF provides a functionality to decrypt data based on asymmetric cryptography, particularly based on the RSA algorithm with key lengths of 2048 bit modulus length. The TSF decryption function will be used for several purposes with different formats for the data supplied within the cryptogram: - Explicit decryption of a cryptogram using the “decryption scheme” with formatted input according to the standard /PKCS1/, chap. 7.2.2 and with hash algorithm SHA-256, see /eHC1/, chap. 7 - Implicit decryption within authentication mechanisms for the verification of authentication tokens using the “decryption primitive” according to the standard /PKCS1/, chap. 5.1.2 The TSF decryption function uses the private key which has been referenced before. For the decryption mechanism itself, the TSF makes directly use of the TSF F.CRYPTO. Each private key used for the decryption function is either generated on-card by usage of the TSF F.RSA_KEYGEN or is generated by the external world and loaded onto the card during the initialisation, personalisation or end-usage phase of the TOE. In the latter case, it is in the responsibility of the external world to guarantee for a sufficient cryptographic strength of the private key and to handle the private key outside the card in a sufficient secure manner. The resistance of the TSF against SPA, DPA, DFA and TA is part of the TSFs F.Log and F.SIDE_CHAN. For each private key - generated on-card or imported with the assumption that the external world meets the requirements on the key handling as defined before - the TSF decryption function works in such a manner that the private key cannot be derived from the cryptogram and the cryptogram cannot be deciphered by other individuals not possessing that secret. Furthermore, the TSF decryption function works in such a manner that no information about the private key may be disclosed during the decipherment of the cryptogram.

6.2 SOF Claim for TOE Security Functions

According to Common Criteria, /CC 2.3 Part1/ and /CC 2.3 Part3/, all TOE Security Functions (TSF) which are relevant for the assurance requirement AVA_SOF.1 are identified in this section.

For the TSFs explicitly defined for the underlying IC, information on the SOF claim can be found in /ST_IC/ and /ST_IC_CL/.

The TSFs related to the complete product using mechanisms which can be analysed for their permutational or probabilistic properties and which contribute to AVA_SOF.1 are the following:

TOE Security Function	SOF Claim	Description / Explanation
F.ACS_SFP	Not applicable	The TSF is not realised by permutational or probabilistic mechanisms.
F.IA_AKEY	SOF high	The TSF implements under usage of the TSFs F.CRYPTO, parts for RSA operations, hash value calculation and random number generation, and of the TSFs F.GEN_DIGSIG, F.VER_DIGSIG, F.ENC and F.DEC cryptographic mechanisms for authentication. The TSF is realised by permutational and probabilistic mechanisms.
F.IA_SKEY	SOF-high	The TSF implements under usage of the TSFs F.CRYPTO, parts for DES operations and random number generation, cryptographic mechanisms for authentication. The TSF is realised by permutational and probabilistic mechanisms.
F.IA_PWD	SOF high	The TSF includes a probabilistic password mechanism for the authentication of the user.
F.DATA_INT	Not applicable	In general, the mechanisms for generating and checking CRC-checksums can be analysed with permutational or probabilistic methods. But these mechanisms are not relevant for AVA_SOF.1 as the securing of data areas by CRC-checksums is only intended to secure against *accidental* data modification.
F.EX_CONF	Not applicable	The TSF includes cryptographic mechanisms using DES functionality from the TSF F.CRYPTO. Refer to the explanations for F.CRYPTO concerning the SOF claim resp. valuation of DES based encryption / decryption functions.
F.EX_INT	Not applicable	The TSF includes cryptographic mechanisms using DES functionality from the TSF F.CRYPTO. Refer to the explanations for F.CRYPTO concerning the SOF claim resp. valuation of DES based MAC generation / MAC verification functions.
F.RIP	Not applicable	The TSF is not realised by permutational or probabilistic mechanisms.
F.FAIL_PROT	Not applicable	The TSF is not realised by permutational or probabilistic mechanisms.
F.SIDE_CHAN	Not applicable	The TSF is not realised by permutational or probabilistic mechanisms.
F.SELFTEST	Not applicable	The TSF is not realised by permutational or probabilistic mechanisms, except for the functionality supported by the TSFs F.DATA_INT and F.CRYPTO (→ refer to the SOF claim for these TSFs).
F.CRYPTO	SOF high	The TSF includes cryptographic algorithms SHA-256, RSA with key lengths 2048 bit modulus length as well as random number generation by usage of a deterministic RNG of quality class K4. These algorithms and key lengths defined for the TSF comply

		with the requirements in /ALGCAT/, chap. 2, 3.1, 4 for qualified electronic signatures and fulfill therefore the requirements for SOF high. The TSF part concerning DES functionality (used for encryption, decryption, MAC generation and MAC verification) are as well assigned to the SOF claim as permutational and probabilistic mechanisms are involved. The negotiation of session keys and the derivation of individual keys is not considered to part for the SOF analysis.
F.RSA_KEYGEN	SOF high	The TSF includes permutational and probabilistic mechanisms for the key generation process itself as well as for the integrated random number generation and key check. In particular, functionality from the TSF F.CRYPTO (random number generation, RSA signature generation and verification) is used by this TSF.
F.GEN_DIGSIG	SOF high	The TSF implements under usage of the TSF F.CRYPTO, parts for RSA operations and random number generation, cryptographic mechanisms for signature generation. The TSF is realised by permutational and probabilistic mechanisms, in particular the quality of the implemented security mechanisms against leakage can be analysed using permutational or probabilistic methods.
F.VER_DIGSIG	Not applicable	The implementation of the TSF uses only public keys and needs not to be considered with regard to high attack potential so that securing of the implementations against Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and Timing Attacks (TA) is not necessary. Because of this fact, the TSF – although it can be analysed with permutational or probabilistic methods - is not relevant for AVA_SOF.1. Nevertheless, this TSF is secured by appropriate hardware security features.
F.RSA_ENC	Not applicable	The implementation of the TSF uses only public keys and needs not to be considered with regard to high attack potential so that securing of the implementations against Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and Timing Attacks (TA) is not necessary. Because of this fact, the TSF – although it can be analysed with permutational or probabilistic methods - is not relevant for AVA_SOF.1. Nevertheless, this TSF is secured by appropriate hardware security features.
F.RSA_DEC	SOF high	The TSF implements under usage of the TSF F.CRYPTO, part for RSA operations, cryptographic mechanisms for decryption. The TSF is realised by permutational and probabilistic mechanisms, in particular the quality of the implemented security mechanisms against leakage can be analysed using permutational or probabilistic methods.

For each of the TOE Security Functions given in the preceding list an explicit claim of “SOF-high” is made.

The TOE´s cryptographic algorithms themselves can also be analysed with permutational or probabilistic methods but this is not in the scope of CC evaluations.

6.3 Assurance Measures

Appropriate assurance measures will be employed by the developer of the TOE to satisfy the security assurance requirements defined in chap. 5.1.3. For the evaluation of the TOE, the developer will provide appropriate documents describing these measures and containing further information supporting the check of the conformance of these measures against the claimed assurance requirements.

For the Smartcard Embedded Software part of the TOE (TOE-ES), the following table gives a mapping between the assurance requirements and the documents containing the relevant information for the respective requirement. All these documents concerning the TOE-ES are provided by the developer of the TOE-ES. The table below contains only the directly related documents, references to further documentation can be taken from the mentioned documents.

Overview of Developer´s TOE-ES related Documents		
Assurance Class	**Family**	**Document containing the relevant information**
ACM Configuration Management	ACM_AUT	- Document Configuration Control System
	ACM_CAP	- Document Life-Cycle Model - Document Configuration Control System
	ACM_SCP	- Document Configuration Control System - Document Life-Cycle Model
ADO Delivery and Operation	ADO_DEL	- Document Life-Cycle Model
	ADO_IGS	- Document Installation, Generation and Start-Up Procedures
ADV Development	ADV_FSP	- Document Functional Specification
	ADV_HLD	- Document High-Level Design - Detailed development documents as system specifications, design specifications, etc.
	ADV_LLD	- Document Low-Level Design - Detailed development documents as system specifications, design specifications, etc.
	ADV_IMP	- Source Code - Detailed development documents as system specifications, design specifications, etc.

	ADV_RCR	- Document Functional Specification - Document High-Level Design - Document Low-Level Design
	ADV_SPM	- Document TOE Security Policy Model
AGD Guidance Documents	AGD_ADM, AGD_USR	- User Guidance for the Initialiser of the TOE - User Guidance for the Personaliser of the TOE - User Guidance for the User of the TOE´s MICARDO OS platform - User Guidance for the User of the TOE´s eHC and SIG Application
ALC Life Cycle Support	ALC_DVS	- Document Security of the Development Environment
	ALC_LCD	- Document Life-Cycle Model
	ALC_TAT	- Configuration List
ATE Tests	ATE_COV	- Document Test Documentation - Detailed test documentation as system test specifications, test protocols, etc.
	ATE_DPT	- Document Test Documentation - Detailed test documentation as system test specifications, test protocols, etc.
	ATE_FUN	- Document Test Documentation - Detailed test documentation as system test specifications, test protocols, etc.
	ATE_IND	- Samples of the TOE - Source Code
AVA Vulnerability Assessment	AVA_MSU	- Document Analysis of the Guidance Documents
	AVA_SOF	- Document TOE Security Function Evaluation
	AVA_VLA	- Document Vulnerability Analysis

As mentioned, the evaluation of the TOE will re-use evaluation results of the CC evaluation of the underlying IC with Crypto Library "NXP SmartMX P5CC080V0B Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software" provided by NXP Semiconductors GmbH. Therefore, for the TOE-IC the following documents will be at least provided by the IC developer:

Overview of Developer´s TOE-IC related Documents	
Class	**Documents**
Security Target	Security Target of the IC evaluation, /ST-IC/

	Security Target of the IC evaluation incl. Crypto Library, /ST-IC+CL/
User Guidances	User Guidance for the IC, /UG_IC/
	Data Sheet for the IC, /DS_IC/
	User Guidances for the Crypto Library, /UG_CL/, /UG-CL-DES/, /UG_CL_RSA/, /UG-CL-RND/, /UG_CL_SHA/, /UG_CL_RSAKeyGen/, /UG-CL-Util/

7 PP Claims

The Security Target claims conformance to the Protection Profile /PP_eHC/. Furthermore, as outlined in chap. 1.3 the Security Target takes into account the contents of the Protection Profile /PP_SSCD_T3/. More detailed information on the differences to the mentioned Protection Profiles can be found in the following chapters 7.1 (for /PP_eHC/) resp. 7.2 (for /PP_SSCD_T3/).

7.1 TOE´s eHC Application

7.1.1 PP References

The Security Target for the TOE and its eHC Application is based on the Protection Profile /PP_eHC/.

Only the following substantial differences to the Protection Profile /PP_eHC/ exist:

- Hash algorithms:

  The TOE provides in addition the hash algorithm SHA-256.

For the impact of these changes on assets, assumptions, threats, security policies, security objectives, security requirements and security functional requirements for the TOE and its environment defined in /PP_eHC/ refer to the following section.

7.1.2 PP Changes and Supplements

All assets, assumptions, threats, security policies, security objectives, security requirements and security functional requirements for the TOE and its environment as defined in the Protection Profile /PP_eHC/ are taken over without any change, except the following changes and supplements:

PP Changes and Supplements		
Name	**Reference in this ST**	**Description**
FCS_COP.1/HASH	Chap. 5.1.1.2	Change of SFR (Supplement of SHA-256)

7.2 TOE´s SIG Application

7.2.1 PP References

The Security Target for the TOE and its SIG Application is based on the Protection Profile /PP_SSCD_T3/ for SSCDs of Type 3, i.e. for devices with oncard - generation of the SCD/SVD key pair, secure storage and usage of the SCD and secure creation of electronic signatures using the dedicated SCD key.

Only the following substantial differences to the Protection Profile /PP_SSCD_T3/ exist:

- Communication between the TOE and the external SCA:

  The establishment of a trusted channel resp. trusted path for the communication between the TOE and the SCA as required within /PP_SSCD_T3/ is now specified as optional. In the case that a trusted channel resp. trusted path is not used the cardholder resp. signatory is responsible for establishing a trusted environment for the communication between the TOE and the SCA.

For the impact of these extensions on assets, assumptions, threats, security policies, security objectives, security requirements and security functional requirements for the TOE and its environment defined resp. not-defined in /PP_SSCD_T3/ refer to the following section.

7.2.2 PP Changes and Supplements

All assets, assumptions, threats, security policies, security objectives, security requirements and security functional requirements for the TOE and its environment as defined in the Protection Profile /PP_SSCD_T3/ for SSCDs of Type 3 are taken over without any change, except the following changes and supplements:

PP Changes and Supplements		
Name	**Reference in this ST**	**Description**
SIG Application / Personalisation Data	Chap. 3.1.3	New asset for the TOE´s personalisation phase
A.SIG_PERS	Chap. 3.2.3	New assumption for the TOE´s personalisation phase
T.SIG_PERS_Aut	Chap. 3.3.3	New threat for the TOE´s personalisation phase
T.SIG_PERS_Data	Chap. 3.3.3	New threat for the TOE´s personalisation phase
OT.DTBS_Integrity_TOE	Chap. 4.1.3	Changed objective due to extension of PP regards trusted channel/path
OT.SIG_PERS	Chap. 4.1.3	New security objective for the TOE´s personalisation phase
OE.HI_VAD	Chap. 4.2.3	Changed objective due to extension of PP regards trusted channel/path
OE.Trusted_Environment	Chap. 4.2.3	New objective due to extension of PP regards trusted channel/path
OE.SIG_PERS	Chap. 4.2.3	New security objective for the TOE´s personalisation phase

FDP_ACC.1 / SIG Personalisation SFP	Chap. 5.1.1.3	New SFR for the TOE´s personalisation phase
FDP_ACF.1 / Signature-Creation SFP	Chap. 5.1.1.3	New Application Note due to extension of PP regards trusted channel/path
FDP_ACF.1 / SIG Personalisation SFP	Chap. 5.1.1.3	New SFR for the TOE´s personalisation phase
FDP_ITC.1 / DTBS	Chap. 5.1.1.3	Changed Application Note due to extension of PP regards trusted channel/path
FDP_UIT.1 / TOE DTBS	Chap. 5.1.1.3	New Application Note due to extension of PP regards trusted channel/path
FMT_MSA.1 / SIG Personalisation	Chap. 5.1.1.3	New SFR for the TOE´s personalisation phase
FTP_ITC.1 / DTBS Import	Chap. 5.1.1.3	New Application Note due to extension of PP regards trusted channel/path
FTP_TRP.1 / TOE	Chap. 5.1.1.3	New Application Note
FPT_AMT.1	Chap. 5.1.1.3	New Application Note
FPT_FLS.1	Chap. 5.1.1.3	New Refinement
FPT_TST.1	Chap. 5.1.1.3	New Application Note and Refinements
FMT_SMF.1	Chap. 5.1.1.3	New SFR due to /AIS 32/
FTP_ITC.1 / SIG Personalisation	Chap. 5.1.1.3	New SFR for the TOE´s personalisation phase
R.Trusted_Environment	Chap. 5.2.2	New requirement due to extension of PP regards trusted channel/path
R.SIG_PERS	Chap. 5.2.2	New requirement for the TOE´s personalisation phase

PP Changes and Supplements for the Completion Process		
Name	**Reference in this ST**	**Description**
A.LEGITIMATE_ACTIVATION	Sec. 3.2.3	New assumption which highlights the special responsibilities of the CSP in the completion process
OT.QESC_TRSP_PROTECT	Sec. 4.1.3	New objective for the protection of the uncompleted SIG application
OT.QESC_RAD_SECRECY	Sec. 4.1.3	New objective for the protection of the initial RAD if stored on the card
OE.QESC_CHECK_TRANSPORT_PROTECTION	Sec. 4.2.3	New objective to enforce that the environment checks the transport protection
OE.QESC_CHECK_USER_LEGITIMACY	Sec. 4.2.3	New objective to enforce that the CSP checks the identity of the user
OE.QESC_CHECK_SSCD	Sec. 4.2.3	New objective to enforce that the environment checks that the smartcard is a certified SSCD

OE.QESC_SECURE_PIN_PUK_HANDLING	Sec. 4.2.3	New objective to enforce that the PIN and PUKs are treated adequately secure.
FDP_ACF 1.2/SVD_TRANSFER_SFP **FMT_SMR 1.1** **FTP_ITC 1.2/SVD_TRANSFER** **FTP_ITC 1.3/SVD_TRANSFER**	Sec. 5.1.1.2	The SVD Transfer SFP has been augemented with the new role „AuthorisedCSP" to emphasise that also the CSP who is responsible for the completion procedure shall be able to export the SVD.
SFP_TRANSPORT_PROTECTION_APP **SFP_TRANSPORT_PROTECTION_RAD** **SFP_EXPORT_BVD** **(and corresponding FDP_ACC, FDP_ACF, and FMT_MSA definitions)**	Sec. 5.1.1.3	New security function policies which enforce the transport protection of the application and the RAD as well as the secured export of the BVD (if stored on the card)

8 Rationale

The following chapters cover the security objectives rationale, the security requirements rationale and the TOE summary specification rationale. Furthermore, the chapter contains a statement of compatibility between the platform security target and this composite security target.

The chapter is not disclosed in the ST-Lite.

Reference

I Bibliography

/CC 2.3 Part1/

Title:	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model
Identification:	CCIMB-2005-08-001
Version:	Version 2.3
Date:	August 2005
Author:	CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CC 2.3 Part2/

Title:	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements
Identification:	CCIMB-2005-08-002
Version:	Version 2.3
Date:	August 2005
Author:	CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CC 2.3 Part3/

Title:	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements
Identification:	CCIMB-2005-08-003
Version:	Version 2.3
Date:	August 2005
Author:	CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CEM 2.3/

Title:	Common Methodology for Information Technology Security Evaluation
Identification:	CCIMB-2005-08-004
Version:	Version 2.3
Date:	August 2005
Author:	CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/AIS32/

Title:	Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema
Identification:	AIS 32, Version 1
Date:	02.07.2001
Publisher:	Bundesamt für Sicherheit in der Informationstechnik

/AIS36/
Title: Kompositionsevaluierung
Identification: AIS 36, Version 2
Date: 12.11.2007
Publisher: Bundesamt für Sicherheit in der Informationstechnik

/BSI_PP_IC/
Title: Smartcard IC Platform Protection Profile
Identification: Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002
Version: Version 1.0
Date: July 2001
Author: Atmel Smart Card ICs, Hitachi Europe Ltd, Infineon Technologies AG, Philips Semiconductors

/BSI_CC_IC/
Title: Certification Report for NXP Secure Smart Card Controller P5CD080V0B, P5CC080V0B, P5CN080V0B and P5CC073V0B each with specific IC Dedicated Software
Identification: BSI-DSZ-CC-0680-2010
Author: Bundesamt für Sicherheit in der Informationstechnik (BSI)
Publisher: Bundesamt für Sicherheit in der Informationstechnik (BSI)

/BSI_CC_ICCL/
Title: Assurance Continuity Maintainance Report: NXP Smart Card Controller P5CD080V0B with IC dedicated software - Secured Crypto Library Release 2.1
Identification: BSI-DSZ-CC-0417-2010-MA-02
Author: Bundesamt für Sicherheit in der Informationstechnik (BSI)
Publisher: Bundesamt für Sicherheit in der Informationstechnik (BSI)

/DS_IC/
Title: Product Data Sheet: P5Cx02x/040/073/080/144 family – Secure dual interface and contact PKI smart card controller
Version: Revision 3.7
Date: 04st June 2010
Publisher: NXP Semiconductors GmbH

/UG_IC/
Title: Guidance, Delivery and Operation Manual for the P5Cx012/02x/040/073/080/144 V0B family
Version: Revision 1.8
Date: 15th Feb. 2010
Publisher: NXP Semiconductors GmbH

/UG_CL/

Title:	Secured Crypto Library on the P5Cx02x/040/080/144 Family, User guidance manual: Overview
Version:	Revision 3.9
Date:	06th May 2010
Publisher:	NXP Semiconductors GmbH

/UG-CL-DES/

Title:	Secured Crypto Library on the SmartMX, User guidance manual: DES Library
Version:	Revision 3.0
Date:	24th Aug. 2007
Publisher:	NXP Semiconductors GmbH

/UG_CL_RSA/

Title:	Secured Crypto Library on the SmartMX, User guidance manual: RSA Library
Version:	Revision 4.4
Date:	30th March 2010
Publisher:	NXP Semiconductors GmbH

/UG-CL-RND/

Title:	Secured Crypto Library on the SmartMX, User guidance manual: Random Number Generator
Version:	Revision 5.0
Date:	24nd Aug. 2007
Publisher:	NXP Semiconductors GmbH

/UG_CL_SHA/

Title:	Secured Crypto Library on the SmartMX, User guidance manual: SHA-1, SHA-224 and SHA-256 Lib
Version:	Revision 4.1
Date:	24th Aug. 2007
Publisher:	NXP Semiconductors GmbH

/UG_CL_RSAKeyGen/

Title:	Secured Crypto Library on the SmartMX, User guidance manual: RSA Key Generation
Version:	Revision 4.3
Date:	30th March 2010
Publisher:	NXP Semiconductors GmbH

/UG-CL-Util/

Title:	Secured Crypto Library on the SmartMX, User guidance manual: Utility Library
Version:	Revision 1.0

Date: 24th Aug. 2007
Publisher: NXP Semiconductors GmbH
Publisher: NXP Semiconductors GmbH

/ST_IC/
Title: Security Target Lite – P5CC080V0B
Identification: BSI-DSZ-CC-0680-2010
Version: Revision 1.9
Date: 14th Jul 2010
Publisher: NXP Semiconductors GmbH

/ST_IC_CL/
Title: Security Target Lite – Secured Crypto Library on the P5CC080V0B
Identification: BSI-DSZ-CC-0417-2010-MA-02
Version: Revision 1.3.2
Date: 10th May 2010
Publisher: NXP Semiconductors GmbH

/ISO 9796-2/
Title: Information Technology – Security Techniques – Digital Signature Schemes Giving Message Recovery – Part 2: Integer Factorization Based Mechanisms
Identification: ISO/IEC 9796-2
Version: Second Edition
Date: 2002
Publisher: ISO / IEC

/ISO 9798-3/
Title: Information Technology – Security Techniques – Entity Authentication Mechanisms – Part 3: Entity Authentication Using a public key algorithm
Identification: ISO/IEC 9798-3
Version: Second Edition
Date: 1998
Publisher: ISO / IEC

/ISO 7816-4/
Title: Integrated circuit(s) cards with contacts. Part 4: Interindustry commands for interchange
Identification: ISO/IEC 7816-4
Version: First edition
Date: September 1.1995
Publisher: International Organization for Standardization/International Electrotechnical Commission

/ISO 7816-8/
Title: Integrated circuit(s) cards with contacts. Part 8: Interindustry commands for interchange
Identification: ISO/IEC FDIS 7816-8

Date: June 1998
Publisher: International Organization for Standardization/International Electrotechnical Commission

/ISO 7816-9/
Title: Integrated circuit(s) cards with contacts. Part 9: Enhanced inter-industry commands
Identification: ISO/IEC 7816-9
Version: First Edition
Date: Sept. 2000
Publisher: International Organization for Standardization/International Electrotechnical Commission

/SHA/
Title: Secure Hash Standard (SHS)
Identification: FIPS Publication 180-2
Date: August 2002
Publisher: National Institute of Standards and Technology (NIST)

/FIPS 46-3/
Title: Data Encryption Standard (DES)
Identification: FIPS Publication 46-3
Date: October 1999
Publisher: National Institute of Standards and Technology (NIST)

/ANSI X9.52/
Title: Triple Data Encryption Algorithm Modes of Operation
Identification: ANSI X9.52
Date: 1998
Publisher: American National Standards Institute (ANSI)

/PKCS1/
Title: PKCS #1 v2.1: RSA Cryptography Standard
Date: June 2002
Publisher: RSA Laboratories

/ISO 11770-3/
Title: Information Technology – Security Techniques – Key Management – Part 3: Mechanisms Using Asymmetric Techniques
Identification: ISO/IEC 11770-3
Date: 1996
Publisher: ISO/IEC

/ANSI X9.19/

Title: Financial Institution Retail Message Authentication
Identification: ANSI X9.19
Date: 1996
Publisher: American National Standards Institute (ANSI)

/ANSI X9.63/
Title: Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography
Identification: ANSI X9.63
Date: 2001
Publisher: American National Standards Institute (ANSI)

/eHC1/
Title: Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle
Version: as specified in the Base Roll-Out Release 0.5.3 (including SRQ supplements)
Publisher: gematik mbH

/TR_COMF_PIN/
Title: Komfortsignatur mit dem Heilberufeausweis
Identification: BSI TR-03115
Version: 2.0
Date: 19.10.2007
Publisher: Bundesamt für Sicherheit in der Informationstechnik (BSI)

/TR_STACK_PIN/
Title: Stapelsignatur mit dem Heilberufeausweis
Identification: BSI TR-03114
Version: 2.0
Date: 22.10.2007
Publisher: Bundesamt für Sicherheit in der Informationstechnik (BSI)

/eHC2/
Title: Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen (früher: Anwendungen und anwendungsspezifische Strukturen)
Version: as specified in the Base Roll-Out Release 0.5.3 (including SRQ supplements)
Publisher: gematik mbH

/SigG01/
Title: Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften
Identification: Bundesgesetzblatt Nr. 22, S. 876
Date: 16.05.2001

Publisher: Dtsch. Bundestag

/SigV01/
Title: Verordnung zur elektronischen Signatur
Identification: Bundesgesetzblatt Nr. 509, S. 3074
Date: 16.11.2001
Publisher: Dtsch. Bundestag

/ECDir/
Title: Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen Identification: Bundesgesetzblatt Nr. 509, S. 3074
Identification: Amtblatt der Europäischen Gemeinschaften, L13/12-L13/20
Date: 19.01.2001
Publisher: Europäisches Parlament und Rat der Europäischen Union

/ALGCAT/
Title: Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs.1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Anschnitt I Nr. 2 SigV vom 22. Nov. 2001
Identification: Bundesanzeiger (to be published)
Date: 22.12.2010
Publisher: Bundesnetzagentur

/PP_eHC/
Title: Protection Profile – electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK)
Identification: BSI-CC-PP-0020-V2-2007-MA-03
Version: 2.61
Date: 19th April 2011
Publisher: Bundesamt für Sicherheit in der Informationstechnik (BSI)

/PP_SSCD_T3/
Title: Protection Profile – Secure Signature-Creation Device Type 3
Identification: BSI-PP-0006-2002
Version: 1.05
Date: 25.07.2001
Publisher: CEN/ISSS – Information Society Standardization System, Workshop on Electronic Signatures

II Summary of abbreviations

A.x	Assumption
AC	Access Condition
AID	Application Identifier
ALW	Always
AM	Access Mode
AR	Access Rule
AS	Application Software
ATR	Answer To Reset
AUT	Key Based Authentication
BS	Basic Software
CC	Common Criteria
CGA	Certification Generation Application
CH	Card Holder
CHV	Cardholder Verification
CSP	Certification Service Provider
DES	Data Encryption Standard
DF	Dedicated File
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DTBS	Data to be signed
EAL	Evaluation Assurance Level
EF	Elementary File
EHC	Electronic Health Card
ES	Embedded Software
HPC	Health Professional Card
IC	Integrated Circuit
IFD	Interface Device
MAC	Message Authentication Code
MF	Master File
O.x	Security Objective
OS	Operating System
PAR	Partial Access Rule
P.x	Organisational Security Policy
PIN	Personal Identification Number
PP	Protection Profile
PUC	PIN Unblocking Code
PW	Password
PWD	Password Based Authentication
RAD	Reference Authentication Data
RSA	Rivest-Shamir-Adleman Algorithm
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCD	Signature Creation Data
SCS	Signature Creation System
SDO	Signed Data Object
SFP	Security Function Policy
SFR	Security Functional Requirement
SM	Secure Messaging
SMC	Security Module Card
SOF	Strength of Functions
SPA	Simple Power Analysis

SPM	TOE Security Policy Model
SSC	Send Sequence Counter
SSCD	Secure Signature Creation Device
ST	Security Target
SVD	Signature Verification Data
TA	Timing Analysis
T.x	Threat
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VAD	Verification Authentication Data

III Glossary

For explanation of technical terms refer to the following documents:

/BSI_PP_IC/ Chap. 8.7

Appendix

Mapping SigG / SigV – TOE Sicherheitsfunktionen

#	Anforderungen aus SigG / SigV	Referenz	Relevante TSFs des EVG
1	(1) Für die Speicherung von Signaturschlüsseln sowie für die Erzeugung qualifizierter elektronischer Signaturen sind sichere Signaturerstellungseinheiten einzusetzen, die Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung der Signaturschlüssel schützen. Werden die Signaturschlüssel auf einer sicheren Signaturerstellungseinheit selbst erzeugt, so gilt Absatz 3 Nr. 1 entsprechend.	/SigG01/, §17 „Produkte für qualifizierte elektronische Signaturen“, (1)	Eine Nutzung des Signaturschlüssels der Signaturapplikation der sicheren Signaturerstellungseinheit „MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0“ ist nur nach erfolgreicher PIN-basierter Authentisierung des Nutzers möglich (Identifikation durch Besitz und Wissen). Die Sicherung des Signaturschlüssels und seiner Nutzung ist Gegenstand von TSF F.ACS_SFP (Zugriffskontrolle) und F.IA_PWD (Prozesse der PIN-basierten Authentisierung). Pro PIN-Verifikation ist alternativ entweder nur eine Signaturerzeugung möglich oder aber beliebig viele Signaturen können erzeugt werden. Die Auswahl der Variante erfolgt im Rahmen der Personalisierung des Produktes. Solange sich die Signaturanwendung im Transportzustand befindet verhindert die Sicherheitsfunktion F.IA_PWD, dass die TransportPIN für die PIN-basierte Authentisierung verwendet werden kann. Insbesondere erzwingt die Sicherheitsfunktion auch, dass eine einmal gesetzte operationale PIN niemals in den Transportzustand zurückgesetzt werden kann. Die Sicherheitsfunktion F.ACS_SFP (Zugriffskontrolle) ermöglicht nicht nur das authentische und integre Auslesen des Signaturprüfschlüssels sondern auch den das Auslesen von Kartenmerkalen über einen sicheren Kanal. Auf diese Weise kann sich der Nachlade ZDA vor Erstellung des qualifizierten Zertifikats davon überzeugen, dass noch keine Signaturen mit der Signaturerstellungseinheit erzeugt worden sind. Zu diesem Test ist der Nachlade-ZDA gemäß OE.CHECK_TRANSPORT_PROTECTION verpflichtet. Insgesamt ist als sichergestellt, dass die Signaturanwendung nur komplettiert wird, wenn vorher keine Signaturen erzeugt wurden. Die Generierung des Signaturschlüsselpaares der Signaturapplikation der sicheren Signaturerstellungseinheit „MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0“ erfolgt ausschließlich on-card. Die Anforderungen

			an die Qualität des Generierungsprozesses werden in TSF F.RSA_KEYGEN, F.SIDE_CHAN, F.CRYPTO und F.RIP umgesetzt. Die Schlüsselgenerierung findet ausschließlich im Rahmen der Personalisierung des Produktes (unter den in der User Guidance für den Personalisierer angegebenen Auflagen) statt. Insbesondere ist aufgrund der gesetzten Zugriffsregeln keine erneute Schlüsselgenerierung im Wirkbetrieb des Produktes möglich (TSF F.ACS_SFP). Die Sicherheit des Prozesses der Signaturerzeugung, insbesondere bzgl. der Gewinnung von Informationen über den benutzten Signaturschlüssel, wird über TSF F.GEN_DIGSIG, F.CRYPTO, F.SIDE_CHAN und F.RIP sichergestellt. Insbesondere sorgen die genannten TSF dafür, dass Fälschungen von Signaturen und Verfälschungen signierter Daten erkennbar gemacht werden.
2	(3) Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um 1. bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen, ...	/SigG01/, §17 „Produkte für qualifizierte elektronische Signaturen“, (3), Satz 1	Siehe Erklärungen zu Tabellenzeile 1.
3	(1) Sichere Signaturerstellungseinheiten nach § 17 Abs. 1 Satz 1 des Signaturgesetzes müssen gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder [...] angewendet werden kann. Der Signaturschlüssel darf nicht preisgegeben werden. [...] Die zur Erzeugung und Übertragung von Signaturschlüsseln erforderlichen technischen Komponenten nach § 17 Abs. 1 Satz 2 oder Abs. 3 Nr. 1 des Signaturgesetzes müssen gewährleisten, dass aus einem Signaturprüfschlüssel oder einer Signatur nicht der Signaturschlüssel errechnet werden kann und die Signaturschlüssel nicht dupliziert werden können.	/SigV01/, §15 „Anforderungen an Produkte für qualifizierte elektronische Signaturen“, (1)	Eine Nutzung des Signaturschlüssels der Signaturapplikation der sicheren Signaturerstellungseinheit „MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0“ ist ausschließlich nach erfolgreicher PIN-basierter Authentisierung des Nutzers möglich (Identifikation durch Besitz und Wissen). Die Nutzung biometrischer Merkmale zur Authentisierung des Nutzers ist nicht implementiert. Die Sicherung des Signaturschlüssels und seiner Nutzung ist Gegenstand von TSF F.ACS_SFP (Zugriffskontrolle) und F.IA_PWD (Prozesse der PIN-basierten Authentisierung). Ein direktes Auslesen des Signaturschlüssels über die regulären Betriebssystem-Kommandos ist aufgrund der gesetzten Zugriffsregeln ebenfalls nicht möglich (TSF F.ACS_SFP).

			Die Generierung des Signaturschlüsselpaares der Signaturapplikation der sicheren Signaturerstellungseinheit „MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0“ erfolgt ausschließlich on-card. Die Anforderungen an die Qualität des Generierungsprozesses werden in TSF F.RSA_KEYGEN, F.SIDE_CHAN, F.CRYPTO und F.RIP umgesetzt. Die Schlüsselgenerierung findet ausschließlich im Rahmen der Personalisierung des Produktes (unter den in der User Guidance für den Personalisierer angegebenen Auflagen) statt. Insbesondere ist aufgrund der gesetzten Zugriffsregeln keine erneute Schlüsselgenerierung im Wirkbetrieb des Produktes möglich (TSF F.ACS_SFP). Die Sicherheit des Prozesses der Signaturerzeugung, insbesondere bzgl. der Gewinnung von Informationen über den benutzten Signaturschlüssel, wird über TSF F.GEN_DIGSIG, F.CRYPTO, F.SIDE_CHAN und F.RIP sichergestellt.
4	(4) Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.	/SigV01/, §15 „Anforderungen an Produkte für qualifizierte elektronische Signaturen“, (4)	Die sichere Signaturerstellungseinheit „MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0“ beinhaltet geeignete Sicherungsmechanismen, die einen sicheren Betriebszustand des Produktes garantieren und dem Nutzer (direkt oder indirekt, je nach Fehlerfall) Information hierüber geben. Die Sicherungsmechanismen werden in TSF F.FAIL_PROT, F.SELFTEST und F.SIDE_CHAN realisiert.
5	Restriktionen zur PIN-/PUK-Funktionalität	---	Die Signaturapplikation der sicheren Signaturerstellungseinheit „MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0“ sieht folgende Restriktionen für die dem Signaturschlüssel zugeordnete Signatur-PIN (PIN.QES) vor: - Initialwert für den Fehlbedienungszähler: 3 - Mindestlänge der PIN: 6 Ziffern - Nutzung des Transport-PIN Verfahrens (Länge der Transport-PIN: 5 Ziffern, Wechsel der Transport-PIN über das Kommando CHANGE REFERENCE DATA notwendig vor erster Nutzung des Signaturschlüssels, d.h. vor erster erfolgreicher PIN-Verifikation über das Kommando VERIFY) - Verwendung einer PUK (Resetting Code) zum Freischalten einer gesperr-

			ten Signatur-PIN Für die der Signatur-PIN zugeordnete PUK sieht die Signaturapplikation folgende Restriktionen vor: - Keine Verwendung eines Fehlbedienungszählers - Initialwert für den Bedienungszähler: 10 - Länge der PUK: 8 Ziffern - Jeder Zugriff auf die PUK dekrementiert den zugehörigen Bedienungszähler. - Variante für RESET RETRY COUNTER: ohne Wechsel der Signatur-PIN, kein Setzen des Sicherheitszustandes der Signatur-PIN
6	Restriktionen zur Nutzung der Display-Message	---	Die Signaturapplikation der sicheren Signaturerstellungseinheit „MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0“ verwendet ein Datenfeld für die Display-Message. Eine Änderung der Display-Message erfordert aufgrund der gesetzten Zugriffsregeln die erfolgreiche PIN Verifikation mit der PIN PIN.CH der eHC Karte. Die PIN PIN.CH ist ein von der Signatur-PIN PIN.QES zur Sicherung des Signaturschlüssels verschiedenes Objekt.
7	(5) ... Bei der Prüfung und Bestätigung der Sicherheit von Produkten nach § 17 Abs. 1 und 3 Nr. 1 des Signaturgesetzes sind die Vorgaben des Abschnitts II der Anlage 1 zu dieser Verordnung zu beachten.	/SigV01/, §15 „Anforderungen an Produkte für qualifizierte elektronische Signaturen“, (5)	Siehe Erklärungen in den folgenden Tabellenzeilen 8 - 10.

8	Die Prüfung der Produkte für qualifizierte elektronische Signaturen nach Maßgabe des § 15 Abs. 7 und des § 17 Abs. 4 des Signaturgesetzes hat nach den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ (Common Criteria for Information Technology Security Evaluation, BAnz. 1999 S. 1945, – ISO/IEC 15408) oder nach den „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“ (ITSEC – GMBl vom 8. August 1992, S. 545) in der jeweils geltenden Fassung zu erfolgen. Die Prüfung muss ... b) bei sicheren Signaturerstellungseinheiten nach § 2 Nr. 10 des Signaturgesetzes mindestens die Prüftiefe EAL 4 oder E 3 umfassen, ...	/SigV01/, Anlage 1, I, 1.1 „Anforderungen an Prüftiefen“	Die sichere Signaturerstellungseinheit „MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0“ unterliegt einer Evaluierung und Zertifizierung nach dem Standard Common Criteria Version 2.3 mit dem Evaluierungslevel EAL 4+ (mit den Augmentierungen ADV_IMP.2, ATE_DPT.2, AVA_MSU.3 und AVA_VLA.4) und SOF Hoch.
9	Bei den Prüfstufen „EAL 4“ und bei „EAL 3“ gemäß Abschnitt I Nr. 1.1 Buchstabe a bis c i) und Buchstabe d ist ergänzend zu den bei dieser Prüfstufe vorgeschriebenen Maßnahmen gegen ein hohes Angriffspotenzial zu prüfen und eine vollständige Missbrauchsanalyse durchzuführen. ...	/SigV01/, Anlage 1, I, 1.2 „Anforderungen an Schwachstellenbewertung / Mechanismenstärke“	Die sichere Signaturerstellungseinheit „MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0“ unterliegt einer Evaluierung und Zertifizierung nach dem Standard Common Criteria Version 2.3 mit dem Evaluierungslevel EAL 4+ (mit den Augmentierungen ADV_IMP.2, ATE_DPT.2, AVA_MSU.3 und AVA_VLA.4) und SOF Hoch.
10	Die Algorithmen und zugehörigen Parameter müssen nach Abschnitt I Nr. 1.2 dieser Anlage als geeignet beurteilt sein.	/SigV01/, Anlage 1, I, 1.3 „Anforderungen an Algorithmen“	Die sichere Signaturerstellungseinheit „MICARDO V3.5 R1.0 eHC V1.2 QESC V1.0“ berücksichtigt für die Signaturerzeugung, Hashwert-Berechnung, Zufallszahlengenerierung und Schlüsselgenerierung Algorithmen und Parameter, die dem aktuellen Algorithmenkatalog /ALGCAT/ entsprechen. Vergleiche hierzu die TSFs F.GEN_DIGSIG, F.RSA_KEYGEN und F.CRYPTO.