Document Administration

Recipient

Department	Name

For the attention of

Department	Name

Summary

The following document comprises the Security Target Lite for a TOE evaluated according to Common Criteria Version 2.2. The TOE being subject of the evaluation is the smartcard product

ZKA SECCOS Sig v1.5.2

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.

Keywords

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

Dr. Susanne Pingel

Sagem ORGA

ZKA SECCOS Sig v1.5.2

ST-Lite

Document Id:	3SECCOS.CSL.0001
Archive:	3
Product/project/subject:	SECCOS (SECCOS - Secure Chip Card Operating System)
Category of document:	CSL (ST-Lite)
Consecutive number:	0001
Version:	V1.00
Date:	25 April 2006
Author:	Dr. Susanne Pingel
Confidentiality:	

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

OdsDok V2.00

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
X1.00.1 / V1.00	First edition	Dr. Susanne Pingel

Table of Contents

1 ST Introduction

1.1 ST Identification

This Security Target Lite refers to the smartcard product "ZKA SECCOS Sig v1.5.2" (TOE) provided by Sagem ORGA GmbH for a Common Criteria evaluation.

Title:	ZKA SECCOS Sig v1.5.2 - ST-Lite
Document Category:	Security Target for a CC Evaluation (Public Version)
Document ID:	3SECCOS.CSL.0001
Version:	Refer to Document Administration
Publisher:	Sagem ORGA GmbH
Confidentiality:	confidential
TOE:	"ZKA SECCOS Sig v1.5.2": Smartcard product on the base of the SECCOS operating system intended to be used as Secure Signature-Creation Device (SSCD) for qualified electronic signatures in accordance with the European Directive 1999/93/EC on electronic signatures /ECDir/, the German Signature Act /SigG01/ and the German Signature Ordinance /SigV01/
Certification ID:	BSI-DSZ-CC-0341
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 Lite has been built in conformance with Common Criteria V2.2 resp. Common Criteria V2.1 (ISO 15408) under consideration of all relevant finally agreed RIs (refer to /AIS32/).

Note: The new version Common Criteria V2.2 is based on the older version V2.1 and integrates as single difference all RIs finally agreed up to the end of 2003.

1.2 ST Overview

Target of Evaluation (TOE) and subject of this Security Target Lite (ST-Lite) is the smartcard product "ZKA SECCOS Sig v1.5.2" developed by Sagem ORGA GmbH.

The TOE is realised as Smartcard Integrated Circuit (IC with contacts) with Cryptographic Library, Smartcard Embedded Software and the EEPROM part containing a dedicated Signature Application.

The Smartcard Embedded Software comprises the so-called SECCOS operating system. This platform provides a fully interoperable ISO 7816 compliant multi-application platform which can be used for smartcards with high security applications. The wide range of the various technical, functional and security features of the SECCOS operating system platform as integrated in the Sagem ORGA product allows in particular beside the dedicated Signature Application of the TOE for further different kinds of (banking) applications as GeldKarte Application (/SECCOS GK/), EMV Application (/SECCOS EMV/), electronic cash Application (/SECCOS EC/), etc.

The TOE is intended to be used as Secure Signature-Creation Device (SSCD) for qualified electronic signatures in accordance with the European Directive 1999/93/EC on electronic signatures /ECDir/, the German Signature Act /SigG01/ and the German Signature Ordinance /SigV01/. The EU compliant Signature Application of the TOE (named ZKA-SigG-Q in the following) is explicitly designed for the generation of legally binding qualified electronic signatures as defined in /ECDir/, /SigG01/ and /SigV01/.

The TOE´s dedicated Signature Application provides asymmetric cryptography based on RSA for key generation and signature-creation with key lengths between 1024 bit and 1984 bit. Digital signature schemes are either PKCS#1 with the hash algorithm SHA-1 (/PKCS1/) or ISO/IEC 9796-2 with random numbers with the hash algorithm RIPEMD-160 (/ISO 9796-2/, /ISO 10118-3/).

The TOE´s dedicated Signature Application allows configuration in different aspects:

First, according to /SECCOS Sig/, the Signature Application can be layout for the following types of signature cards: “Pure Signature Card”, “GeldKarte / Debit Card with Signature Application” or “Credit Card with Signature Application”.

Furthermore, the Signature Application contains according to /SECCOS Sig/ several configurable and optional elements. In particular, this concerns attributes of keys (as e.g. availability of keys, key lengths, maximum number of signature-creation processes with the signature-creation data (SCD)), of the signature PIN (as e.g. minimal length, error usage counter) and of resetting codes (as e.g. availability of such codes, minimal length, error usage counter, usage counter). In addition, different data fields (e.g. for certificates) are marked as optional, and the download of certificates or the insertion of certificate references in a batch procedure can be allowed or denied. The configuration of these elements underlies specific restrictions which are specified in detail in /SECCOS Sig/.

Furthermore, the choice of a secure or insecure variant of the key pair generation functionality for the TOE´s initialisation phase is possible. The insecure variant of the TOE´s key pair generation functionality is only applicable for the initialisation phase of the TOE´s life-cycle (refer to chap. 2.2). Under guarantee of sufficient security of the initialisation environment this variant can be chosen due to customer wish with the target to accelerate the key pair generation process and therefore to reduce production time.

For simplicity, no differentiation between the different configurations of the TOE´s Signature Application will be made in the following, and therefore the term “TOE´s *dedicated* Signature Application” will be used.

The configuration of the TOE´s dedicated Signature Application will be done during the development phase of the TOE´s life-cycle (refer to chap. 2.2) by Sagem ORGA GmbH and in particular prior to delivery of the product to the customer. Afterwards, no change of the configuration chosen for the TOE´s dedicated Signature Application is possible.

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

The TOE 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 /SECCOS/ for the SECCOS operating system
- Functional and security requirements defined in the specification /SECCOS Sig/ for the Signature Application of the TOE (ZKA-SigG-Q Application)
- Functional and security requirements defined in the specification /SECCOS GK/ for the GeldKarte Application
- Functional and security requirements defined in the specification /SECCOS EMV/ for the EMV Application
- Functional and security requirements defined in the specification /SECCOS EC/ for the electronic cash Application
- Functional and security requirements defined in the specification /SECCOS Perso/ and /SECCOS Perso Sig/ for the initialisation and personalisation of SECCOS-based smartcards resp. of the TOE´s Signature Application (ZKA-SigG-Q Application)
- 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 drawn from the Protection Profile /PP SSCD Type 3/
- Technical requirements defined in /ISO 7816/, Parts 1, 2, 3, 4, 8, 9, 15

Note: In the following, under the name “SECCOS operating system” all standard operating system commands defined in the specification /SECCOS/, all application commands defined in the specifications /SECCOS GK/, /SECCOS EMV/ and /SECCOS EC/ as well as all additional production commands for the smartcard initialisation and personalisation defined in the specifications /SECCOS Perso/ and /SECCOS Perso Sig/ are summarised. The Signature Application ZKA-SigG-Q of the TOE makes only use of the standard and production commands. The remaining application commands are only necessary for the optional additional banking applications.

Under technical view, the TOE comprises the following components:

- Integrated Circuit (IC) AE55C1 (HD65255C1), Version 02 with related Advanced Cryptographic Library, Version 1.43 (ACL) provided by Renesas Technology Corp.
- Smartcard Embedded Software comprising the SECCOS operating system platform provided by Sagem ORGA GmbH
- EEPROM Initialisation Tables with the dedicated Signature Application provided by Sagem ORGA GmbH (possibly including additional (banking) applications)

The pre-defined Signature Application (ZKA-SigG-Q Application) belonging to the TOE is set-up on the SECCOS operating system platform of the TOE and comprises an own dedicated file and data system 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 Signature Application makes only use of the data structures, security architecture and standard and production commands as specified in /SECCOS/ and /SECCOS Perso/. A detailed description of the TOE´s Signature Application and its security structure can be found in /SECCOS Sig/.

The TOE´s EEPROM part resp. the Initialisation Tables may contain optional additional (banking) applications as GeldKarte Application, EMV Application, electronic cash Application, etc. These additional applications are completely separated from the TOE´s Signature Application and handle their own file and data system with own security structures and an own PIN and key management.

The TOE will be delivered from Sagem ORGA GmbH in the following variants:

- Delivery as *not-initialised* module or smartcard:

  The delivery of the modules resp. smartcards will be combined with the delivery of the customer specific Initialisation Table (in particular containing the evaluated Signature Application) developed by Sagem ORGA GmbH to the involved Verlag der Kreditwirtschaft. To finalize the TOE, the following processes have to be performed on customer side: The supplied Initialisation Table has to run through a further post-processing at the Verlag der Kreditwirtschaft for insertion of additional verification data. Afterwards, the finalised Initialisation Table has to be sent from the Verlag der Kreditwirtschaft (by a secured transfer way) to the Initialiser for loading the EEPROM initialisation data into the TOE during its initialisation phase whereat the production requirements defined in the Guidance for the Initialiser (as well delivered by Sagem ORGA) have to be considered.

  In the case of the delivery of modules, the last part of the smartcard finishing process, i.e. the embedding of the delivered modules and final tests, is task of the customer.

- Delivery as *initialised* module or smartcard:

  The initialisation of the modules resp. smartcards will be performed by Sagem ORGA GmbH. Prior to the initialisation, the customer specific Initialisation Table (in particular containing the evaluated Signature Application) developed by Sagem ORGA GmbH will be sent to the involved Verlag der Kreditwirtschaft. The supplied Initialisation Table runs through a further post-processing at the Verlag der Kreditwirtschaft (insertion of additional verification data) and the finalised Initialisation Table is sent back from the Verlag der Kreditwirtschaft (by a secured transfer way) to Sagem ORGA GmbH as Initialiser for loading the EEPROM initialisation data into the TOE during its initialisation phase.

  In the case of the delivery of modules, the last part of the smartcard finishing process, i.e. the embedding of the delivered modules and final tests, is task of the customer.

The form of the delivery of the TOE does not influence the security features of the TOE in any way. However, in the case of the delivery of the product in initialised form, the initialisation process at Sagem ORGA GmbH will be considered in the framework of the TOE´s CC evaluation.

The functional and assurance requirements and components for SSCDs as defined in /ECDir/, Annex III are mapped to three different Protection Profiles, each of it corresponding to a dedicated type of SSCD. 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 of the SCD/SVD key pair and the secure creation of electronic signatures by using the dedicated SCD key. Hence, the Security Target Lite for the TOE is based on the related Protection Profile /PP SSCD Type 3/.

The Security Target Lite for the TOE covers all essential aspects and contents of /PP SSCD Type 3/. 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 Type 3/ 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.

- Initialisation and Personalisation Phase of the TOE:

  The phases initialisation and personalisation of the TOE´s life-cycle model are considered as part of the operational phase (refer to chap. 2.2 and 2.3). Therefore, additional aspects concerning assets, assumptions, threats, security policies, security objectives and security functional requirements have to be appropriately added.

The CC evaluation and certification of the TOE against the present ST-Lite 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). The CC evaluation and certification of the TOE implies the proof for compliance of the Signature Application ZKA-SigG-Q with the corresponding specifications /SECCOS/ and /SECCOS Sig/ and their requirements.

In order to be compliant with the requirements from the EU Directive on electronic signatures /ECDir/, the German Signature Act /SigG01/ and the German Signature Ordinance /SigV01/ the TOE will be evaluated according to CC EAL 4 augmented with a minimum strength level for the TOE security functions of SOF high.

The evaluation and certification process for the TOE covers the Smartcard IC with its Advanced Cryptographic Library, the Smartcard Embedded Software (SECCOS operating system) and the Initialisation Tables representing the EEPROM part of the TOE and including the TOE´s dedicated Signature Application (and possibly further additional (banking) applications).

The evaluation and certification process will be carried out as so-called composite evaluation, i.e. the software of the TOE will be evaluated in combination with the underlying IC and the related Cryptographic Library whereat the evaluation and certification results of the hardware part (IC incl. ACL) will be re-used.

The main objectives of this ST-Lite are

- to describe the TOE as a smartcard product particularly intended to be used as SSCD of Type 3 for qualified electronic signatures
- to define the limits of the TOE
- to describe the assumptions, threats and security objectives for the TOE and its environment
- to describe the security requirements for the TOE and its environment
- to define the TOE´s security functions

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 2.2, January 2004 (/CC 2.2 Part1/)
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 2.2, January 2004 (/CC 2.2 Part2/)
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 2.2, January 2004 (/CC 2.2 Part3/)

resp.

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 2.1, August 1999 (/CC 2.1 Part1/)
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 2.1, August 1999 (/CC 2.1 Part2/)
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 2.1, August 1999 (/CC 2.1 Part3/)

under consideration of all relevant RIs agreed up to the end of 2003 (refer to /AIS32/).

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 1.0, August 1999 (/CEM 2.2 Part2/)

resp.

- Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 1.0, August 1999 (/CEM 1.0 Part2/)

under consideration of all relevant RIs agreed up to the end of 2003 (refer to /AIS32/).

This Security Target Lite is written in accordance with the above mentioned Common Criteria Versions V2.1 resp. V2.2 and claims the following CC conformances:

- Part 2 extended
- Part 3 conformant

The Security Target Lite is based on the Protection Profile /PP SSCD Type 3/ for Secure Signature-Creation Devices (SSCD) of Type 3. Concerning the communication between the TOE and the external Signature-Creation Application (SCA) some additions resp. changes to the original Protection Profile /PP SSCD Type 3/ have been made. Furthermore, some additions regards the smartcard initialisation and personalisation phase have been integrated. For details refer to chap. 7.2.

The level of assurance chosen for the TOE is **EAL 4 augmented**. The augmentation includes the assurance components AVA_MSU.3 and AVA_VLA.4 (as required by the original Protection Profile /PP SSCD Type 3/).

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

In order to be compliant with the requirements from the EU Directive on electronic signatures /ECDir/, the German Signature Act /SigG01/ and the German Signature Ordinance /SigV01/ the combination of the hardware and software part of the TOE as SSCD has to be evaluated and certified. In order to avoid redundancy and to minimize evaluation efforts, the evaluation of the TOE will be conducted as composite evaluation and will make use of the evaluation results of the CC evaluation of the underlying semiconductor AE55C1 (HD65255C1), Version 02 with related Advanced Cryptographic Library, Version 1.43 (ACL) provided by Renesas Technology Corp. The IC incl. ACL is evaluated according to Common Criteria EAL 4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 with a minimum strength level for its security functions of SOF high. The evaluation of the IC incl. ACL is based on the Protection Profile /BSI-PP-0002/ and is registered under the Certification ID BSI-DSZ-CC-0329.

2 TOE Description

2.1 TOE Definition

2.1.1 Structural Overview of the TOE

The TOE is realised as Smartcard IC (with contacts) with Cryptographic Library, Smartcard Embedded Software and the EEPROM part containing a dedicated Signature Application.

In technical view, the TOE as SSCD according to /ECDir/ and /SigG01/ is based on the so-called SECCOS operating system (Smartcard Embedded Software) as specified in the specifications /SECCOS/, /SECCOS GK/, /SECCOS EMV/, /SECCOS EC/ and /SECCOS Perso/ (refer to the list of specifications in chap. 1.2).

The SECCOS operating system provides a fully interoperable ISO 7816 compliant multi-application platform which can be used for smartcards processing high security applications. The wide range of the various technical, functional and security features of the SECCOS operating system platform as implemented in the Sagem ORGA product allows in particular beside the dedicated Signature Application ZKA-SigG-Q for further separated (banking) applications as GeldKarte Application, EMV Application, electronic cash Application, etc. For the additional banking applications, specific application commands are integrated in the platform, whereat the Signature Application only uses the standard and production commands of the SECCOS operating system platform and makes no use of the application commands.

The Smartcard Embedded Software, i.e. the SECCOS operating system, is realised in form of a native implementation.

The SECCOS operating system includes APDU commands of the following types:

- Standard commands according to /SECCOS/
- Application commands according to /SECCOS GK/, /SECCOS EMV/ and /SECCOS EC/
- Production commands for the smartcard initialisation and personalisation according to /SECCOS Perso/

Furthermore, the Smartcard Embedded Software provides the following functionality:

- File system according to /ISO 7816-4/
- Access Control for the file system
- Secure Messaging for secure communication with the external world
- Management of Security Environments
- Key and PIN management
- PIN based user authentication
- Key based component authentication

- Generation of RSA key pairs
- Creation and verification of electronic signatures (RSA based)
- Enciphering and Deciphering (RSA / DES based)
- Random number generation
- Hash value calculation (SHA-1, RIPEMD-160)
- Verification of CV certificates
- Debit, credit and purse functionality according to the specifications for electronic cash, EMV and GeldKarte

The SECCOS operating system platform is based on the Renesas microcontroller AE55C1 (HD65255C1), Version 02 and the related Renesas Advanced Cryptographic Library, Version 1.43 (ACL). The ACL provides core routines for RSA and DES based cryptographic operations, routines for hash value calculation (SHA-1, RIPEMD-160) and routines for random number generation.

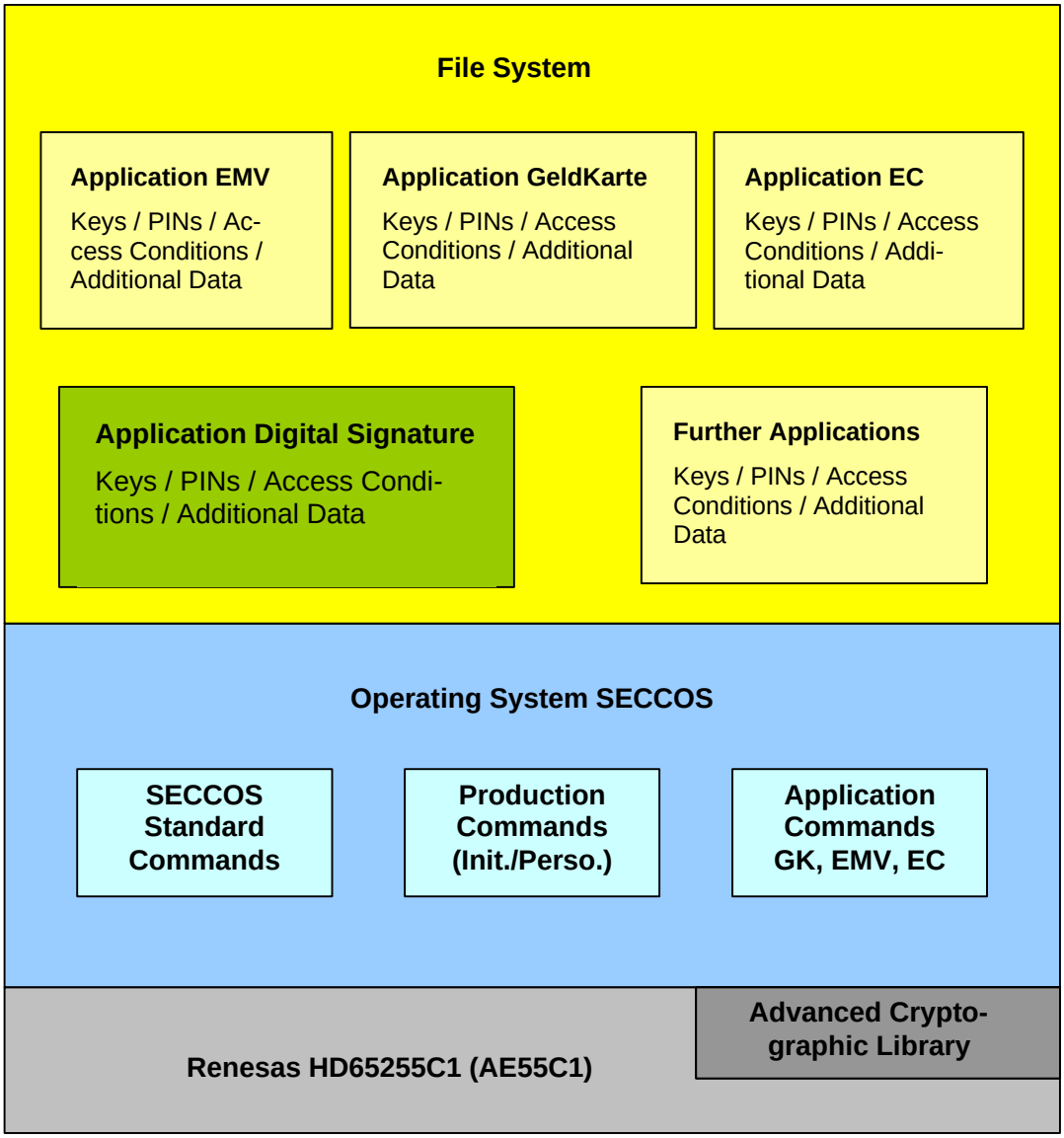
The pre-defined Signature Application ZKA-SigG-Q Application belonging to the TOE comprises an own dedicated file and data system with dedicated security structures, i.e. with application specific access rights for the access of subjects to objects and with application specific security mechanisms and PIN and key management. The design and implementation of the Signature Application and its security structure follow the specification /SECCOS Sig/. The Signature Application makes only use of the data structures, security architecture and standard and production commands as specified in /SECCOS/ and /SECCOS Perso/. Further information on the functionality of the Signature Application can be found in the following chapter 2.1.2.

Beside the dedicated Signature Application ZKA-SigG-Q additional (banking) applications can reside on the TOE. These applications use the same underlying IC, Cryptographic Library and Smartcard Embedded Software (SECCOS operating system) as platform as the TOE´s Signature Application, but a complete separation between these applications and the dedicated Signature Application is realised. The design of the different applications is set-up in such a manner that the additional applications do not influence the security of the Signature Application. In particular, no access of these additional applications to the dedicated Signature Application and its stored and processed (security) data is possible.

Roughly spoken, the TOE comprises the following components:

- Integrated Circuit (IC) AE55C1 (HD65255C1), Version 02 with related Advanced Cryptographic Library, Version 1.43 (ACL) provided by Renesas Technology Corp.
- Smartcard Embedded Software comprising the SECCOS operating system platform provided by Sagem ORGA GmbH
- EEPROM Initialisation Tables with the dedicated Signature Application provided by Sagem ORGA GmbH (possibly including additional (banking) applications as GeldKarte Application, EMV Application, electronic cash Application)

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



2.1.2 TOE´s Signature Application

The TOE is a Secure Signature-Creation Device (SSCD Type 3) according to 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-Lite assumes the SCA as environment of the TOE.

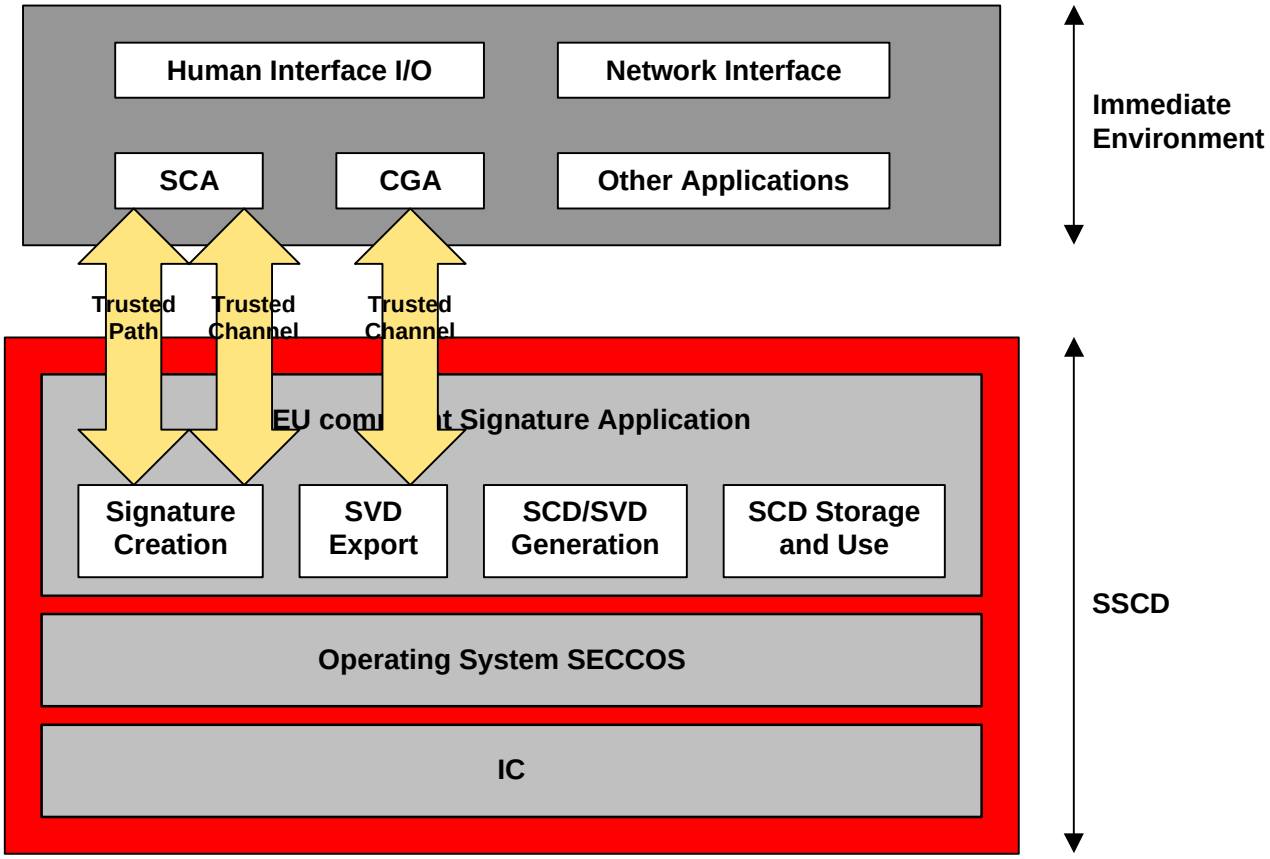
The TOE protects the SCD during the whole life-cycle as to be solely used in the signature-creation process by the legitimate signatory. The TOE as SSCD of Type 3 generates the signatory´s SCD oncard and serves for a secure storage of this data. The initialisation and personalisation of the TOE for the signatory´s use in the sense of the Protection Profile /PP SSCD Type 3/ 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 incl. the related ACL, the SECCOS operating system and the Signature Application ZKA-SigG-Q with SCD/SVD generation, SCD storage and use, SVD export, and the signature-creation functionality. The SCA and the CGA (beside optional additional other separated banking applications) 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:



For the configuration of the TOE´s dedicated Signature Application refer to chap. 1.2.

2.1.3 TOE Product Scope

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

TOE component	Description / Additional Information	Type	Transfer Form
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 Table developed by Sagem ORGA GmbH must be loaded during the initialisation phase by the Initialiser (Sagem ORGA GmbH or other initialisation facility).			
TOE			
TOE HW + SW part	TOE consisting of	HW+SW	Delivery of not-initialised / initialised

TOE component	Description / Additional Information	Type	Transfer Form
	- Renesas IC AE55C1 (HD65255C1), Version 02, whereat the ROM mask consisting of the Advanced Cryptographic Library, Version 1.43 (ACL) and the Smartcard Embedded Software (SECCOS operating system) provided by Sagem ORGA GmbH is already implemented - EEPROM Initialisation Table (provided by Sagem ORGA GmbH)		modules or smartcards Delivery of Initialisation Tables in electronic form (if applicable) Hint: The delivered Initialisation Tables have to be finalised by the Verlage der Kreditwirtschaft (insertion of additional verification data).
TOE Documentation			
Administrator Guide / Smartcard Initialisation	Administrator guidance for the Initialiser for the smartcard initialisation of the TOE (“System Administrator Guidance for the Initialiser of the Smartcard Product ZKA SECCOS Sig v1.5.2”, V1.00)	DOC	Document in paper / electronic form
Administrator Guide / Smartcard Personalisation	Administrator guidance for the Personaliser for the smartcard personalisation of the TOE (“System Administrator Guidance for the Personaliser of the Smartcard Product ZKA SECCOS Sig v1.5.2”, V1.00)	DOC	Document in paper / electronic form
Identification Data Sheet	Data Sheet with information on the actual identification data and configuration of the TOE delivered to the customer (in particular information on the relevant Initialisation Table, “Data Sheet - ZKA SECCOS Sig v1.5.2” (customer specific) based on form “Data Sheet - ZKA SECCOS Sig v1.5.2”, V1.00)	DOC	Document in paper / electronic form
Document „Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS“	Specification describing Initialisation and Personalisation processes, refer to /SECCOS Perso/	DOC	Document in paper / electronic form

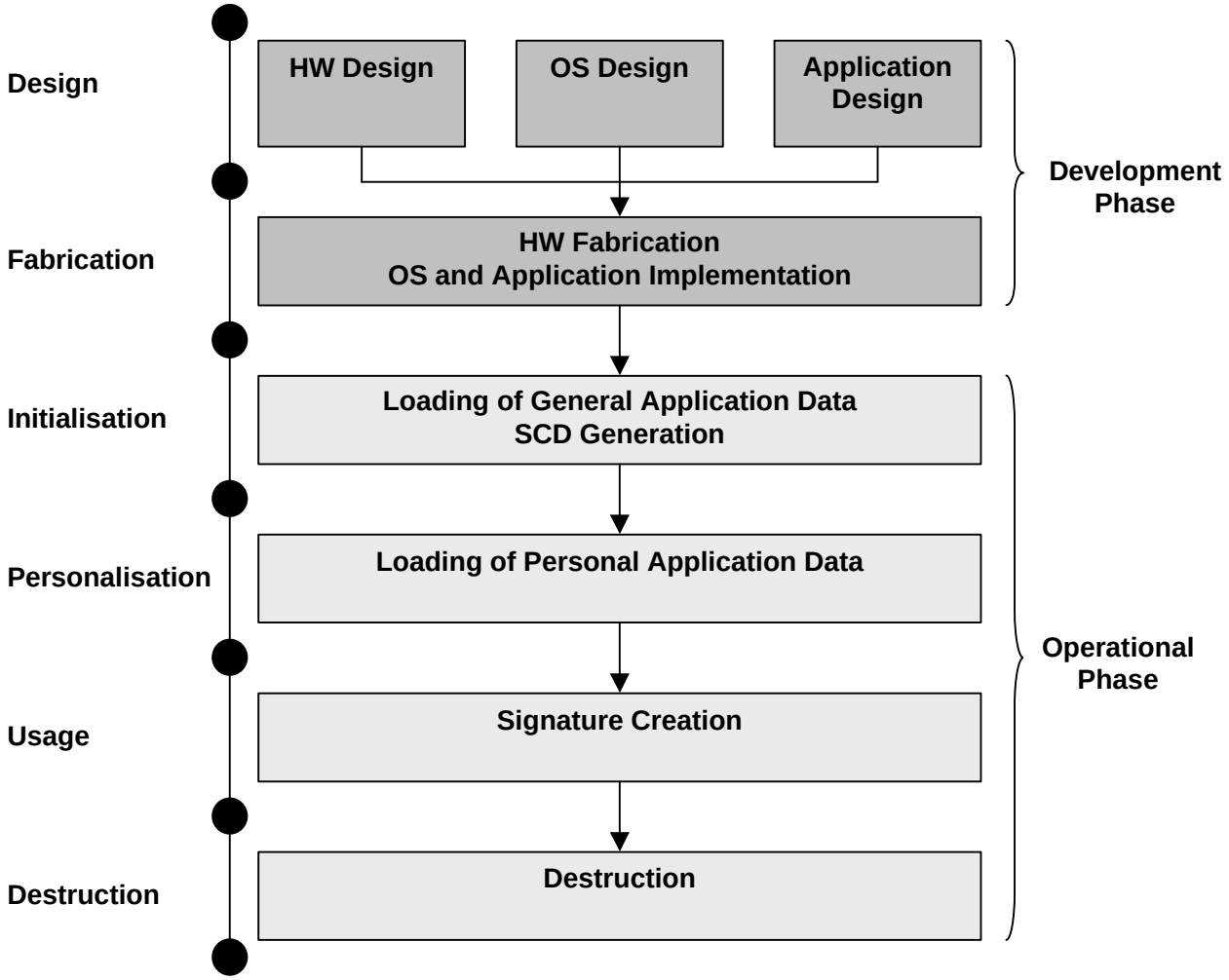
Note: Deliverables in paper form require a personal passing on or a procedure of at least the same security. For deliverables in electronic form an integrity and authenticity attribute will be attached.

2.2 TOE Life-Cycle

2.2.1 Overview of the TOE Life-Cycle

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

The TOE´s life-cycle is shown in the figure below. Basically, it consists of the development phase and the following operational phase.



The **development phase** includes:

- **Design**
  - **HW Design:** The IC Designer (Renesas Technology Corp.) designs the IC, develops the IC Dedicated Software and provides information, software or tools to the Smartcard Embedded Software Developer (Sagem ORGA GmbH). Furthermore, the IC Designer develops the Advanced Cryptographic Library for the IC.
  - **OS and Application Design:** The Smartcard Embedded Software Developer (Sagem ORGA GmbH) is in charge of the development of the Smartcard Embedded Software of the TOE (incl. integration of the Advanced Cryptographic Library), the development of the TOE related Applications and Initialisation Tables and the specification of the IC initialisation and pre-personalisation requirements. The Initialisation Tables are sent from the Smartcard Embedded Software Developer (Sagem ORGA GmbH) to the Verlage der Kreditwirtschaft who are responsible for the finalisation of the Initialisation Tables (insertion of additional verification data) and who perform the secured transfer of the finalised Initialisation Tables to the Initialiser for the TOE´s initialisation.
- **Fabrication**
  - **HW Fabrication and OS and Application Implementation:** The IC Designer (Renesas Technology Corp.) receives the Smartcard Embedded Software from the developer through trusted delivery and verification procedures. From the IC design, IC Dedicated Software, Advanced Cryptographic Library and Smartcard Embedded Software, the IC Designer (Renesas Technology Corp.) constructs the smartcard IC database, necessary for the IC photomask fabrication. The IC Manufacturer (Renesas Technology Corp.) is responsible for producing the IC through three main steps: IC manufacturing, IC testing, and IC pre-personalisation. Furthermore, the IC Manufacturer (Renesas Technology Corp.) generates the masks for the IC manufacturing based upon an output from the smartcard IC database. The IC Packaging Manufacturer (Sagem ORGA GmbH) is responsible for the IC packaging, i.e. the production of modules, and testing.

The **operational phase** includes:

- **Initialisation**
  - **Loading of general Application Data:** The Initialiser (Sagem ORGA GmbH resp. other initialisation facility) is responsible for the initialisation of the TOE with the relevant customer specific finalised Initialisation Table and the following testing (verification of the loaded data). Loading of all the data belonging to an application and being the same for all cards in view of this application is performed. Alternatively, the initialisation of modules or smartcards can be performed.
  - **SCD generation:** The Initialiser (Sagem ORGA GmbH resp. other initialisation facility) is responsible for the generation of the SCD. The generation of the SCD/SVD key pair is performed at the end of the initionalisation process.

- **Personalisation**
  - **Loading of personal Application Data:** The Personaliser (Sagem ORGA GmbH resp. other personalisation facility) is responsible for the smartcard personalisation and final tests. Data as personal user data and personal application secrets (PINs, keys) are loaded during the personalisation process.
- **Usage**
  - **Signature creation:** The usage of the TOE as SSCD as intended lies in the responsibility of the cardholder resp. signatory. The main functionality of the TOE in this phase is – beside further supporting functionality as SCD storage and use – the signature-creation functionality.
- **Destruction**
  - The life-cycle of the TOE as SSCD ends with its destruction.

The smartcard product finishing process which comprises the embedding of the (initialised) modules for the TOE and the card production can be done alternatively by Sagem ORGA GmbH or by the customer himself.

The personalisation step includes the SCD/SVD generation which assumes that the loading of the finalised Initialisation Table has been successfully finished.

The responsibility for the delivery of the personalised TOE to the end-user is up to the Card Issuer (Banks).

The evaluation process of the TOE is limited up to the end of the development phase of the product (including all delivery processes herein). Hence, since the generation of the TOE is not completed after the development phase has been finished, all of the remaining processes have to be in accordance with the security requirements defined in the following chapters.

2.2.2 Delivery of the TOE

With regard to the smartcard product life-cycle of the TOE described in chap. 2.2.1, the development phase of the TOE is part of the TOE´s CC evaluation. However, in the case of the delivery of the TOE in initialised form, the initialisation process at Sagem ORGA GmbH will be considered as well within the framework of the CC evaluation of the Sagem ORGA product.

More precise, and as indicated in chap. 1.2, the TOE will be delivered either as not-initialised or initialised product whereat in each case the delivery in form of modules or smartcards is possible.

2.2.3 Additional Information on Development and Production Processes

Design, Development and Production of the IC and ACL

For detailed information on the processes on Renesas Technology Corp. side concerning the security of the IC and ACL design, development and production procedures refer to /ST IC+ACL/ resp. further evaluation documentation from the CC evaluation of the IC and ACL.

In particular, the design and development process of the ACL used by the TOE´s Smartcard Embedded Software is performed under the control of Renesas Technology Corp. During the design and development process of the ACL, only the people directly involved in this development project have access to the design information, the documentation and the source code. The security measures installed at Renesas Technology Corp. ensure the quality, integrity and confidentiality of the delivered ACL source code. The ACL is delivered from Renesas Technology Corp. to Sagem ORGA GmbH in a trusted and secured way as explicitly defined for the certified Renesas product.

Smartcard Embedded Software and Application Development

To assure sufficient security for the development process of the TOE´s Smartcard Embedded Software and pre-defined Applications, 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 TOE´s Smartcard Embedded Software and pre-defined Applications. For design, implementation and test purposes secure computer systems preventing unauthorized access are employed. 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 TOE´s Smartcard Embedded Software and pre-defined Applications 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 a appropriate traceability and accountability.

The TOE´s Smartcard Embedded Software dedicated for the ROM of the IC is delivered to the IC Designer and Manufacturer through trusted delivery and verification procedures as defined for the certified Renesas product. The remaining parts of the TOE´s Smartcard Embedded Software (if existing) and the Application software are turned into so-called Initialisation Tables. All Initialisation Tables are delivered from Sagem ORGA GmbH in cryptographically secured form to the Verlage der Kreditwirtschaft, as well using trusted delivery and verification procedures.

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 performed in such a way that appropriate traceability and accountability exist.

Initialisation

For the initialisation of the TOE, secure initialisation processes are already prepared and supported by the TOE resp. by the SECCOS operating system platform and the pre-defined Applications. For details refer to /SECCOS Perso/, chap. 4.

Important information as necessary for the TOE´s initialisation and its security is provided by Sagem ORGA GmbH to the Initialiser in form of an administrator guidance (refer to chap. 2.1.3).

In case the initialisation process is performed by Sagem ORGA GmbH:

To assure sufficient security of the initialisation process of the TOE, a secure environment with adequate 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 initialisation and test activities.

Prior to the TOE´s initialisation, the involved Verlag der Kreditwirtschaft finalises the supplied customer specific Initialisation Table developed and delivered by Sagem ORGA GmbH with additional verification data. The initialisation process of the TOE comprises the loading of the EEPROM initialisation data contained within the finalised Initialisation Table as well as completing verification steps.

The TOE only allows an initialisation with the intended finalised Initialisation Table. Furthermore, for security reasons, secure systems within a separate network and preventing unauthorized access are used for the initialisation process.

In case the initialisation process is performed by a customer specific Initialiser:

It is in the responsibility of the Initialiser to garantuee for a correct and sufficiently secure initialisation process with the finalised Initialisation Table.

Smartcard Product Finishing Process

If the TOE is delivered in form of modules, the smartcard finishing process, i.e. the embedding of the delivered modules and final tests, is task of the customer. Otherwise, the smartcard finishing process is part of the production process at Sagem ORGA GmbH, and the TOE is delivered in form of smartcards.

All sensitive documentation, data and material concerning the production processes of the TOE at Sagem ORGA GmbH within this phase 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 process, the TOE is complete as smartcard and can be supplied for delivery to the personalisation center for personalisation (Sagem ORGA GmbH or other personalisation facility).

Smartcard Personalisation

For the personalisation of the TOE, secure personalisation processes are already prepared and supported by the TOE resp. by the SECCOS operating system platform and the predefined Applications. For details refer to /SECCOS Perso/, chap. 5 and /SECCOS Perso Sig/.

Important information as necessary for the TOE´s personalisation and its security is provided by Sagem ORGA GmbH to the Personaliser in form of an administrator guidance (refer to chap. 2.1.3).

In general, 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 center itself. Furthermore, the secure key management and handling of the keys (authentication keys, personalisation keys) for securing the data transfer within the personalisation process is task of the external world resp. the personalisation center.

The originator of the personalisation data and the personalisation center responsible for the personalisation of the TOE 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 and confidentiality.

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 TOE´s structure and according to the TOE´s personalisation requirements is as well in the responsibility of the external world and shall be done with care.

Smartcard End-Usage

The intended usage of the TOE as SSCD is described in detail in chap. 2.1.2, 2.3 and 2.4.

In particular, for the TOE´s Signature Application, the TOE is constructed in such a manner that it implements all functional and security requirements of /SECCOS Sig/. There is no possibility, even in an unsecure end-user environment, to disable or to circumvent the security features of the TOE´s Signature Application.

Delivery Processes in the Development 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 development phase of the TOE are established. This concerns any kind of delivery performed during the production process, 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 Renesas ACL follows the dedicated secured delivery process defined in /UG ACL/.

The delivery of the ROM mask and the EEPROM pre-personalisation data from Sagem ORGA GmbH to Renesas Technology Corp. is carried out by following the dedicated delivery procedure specified in /UG IC/ with the following exception: The Renesas´ Transport Key feature is skipped as the integration of special key data into the IC by the IC Manufacturer (Renesas Technology Corp.) himself (refer to chap. 2.2.4) provides at least the same security.

2.2.4 Generation of ROM Mask and EEPROM Initialisation Tables

The developer of the Smartcard Embedded Software (Sagem ORGA GmbH) generates the ROM mask and sends it to the IC Designer and Manufacturer (Renesas Technology Corp.) for IC production.

The IC Manufacturer generates special key data to ensure for the authenticity of the IC and its ROM mask and to secure the later initialisation process of the TOE. The IC Manufacturer integrates this special key data in a specific EEPROM area pre-defined by the developer of the Smartcard Embedded Software and supplies this data on a secure way to the Verlage der Kreditwirtschaft.

The IC Manufacturer delivers the ICs including the Sagem ORGA ROM mask and the special EEPROM key data to the IC Packaging Manufacturer (Sagem ORGA GmbH) for IC packaging and testing. Afterwards, the TOE is delivered in form of not-initialised modules or smartcards to the Initialiser (Sagem ORGA GmbH or other initialisation facility).

The Smartcard Embedded Software Developer (Sagem ORGA GmbH) is responsible for the development and testing of the so-called Initialisation Tables. Each Initialisation Table consists of a load script for the TOE´s initialisation and covers roughly spoken the following two parts:

- the EEPROM data/code area with the TOE´s EEPROM initialisation data (so-called Initialisation Image)
- the verification data area

The development of the Initialisation Tables covers in particular the configuration of the TOE´s dedicated Signature Application by setting the configurable elements defined in chap. 1.2 within the pre-defined limits due to customer wishes resp. as evaluated within the framework of the TOE´s CC evaluation.

For an Initialisation Table ordered by a Verlag der Kreditwirtschaft, the Verlag generates special key data which are sent on a secure way to the Smartcard Embedded Software Developer (Sagem ORGA GmbH). The key data are used by Sagem ORGA GmbH for the generation of a cryptographic checksum over the developed EEPROM data/code area. The checksum is inserted into the verification data area of the Initialisation Table by Sagem ORGA GmbH.

Afterwards, the secured Initialisation Table is sent from Sagem ORGA GmbH to the Verlag der Kreditwirtschaft for further post-processing. The Verlag der Kreditwirtschaft finalises the secured Initialisation Table delivered by Sagem ORGA GmbH by the generation of special verification data and insertion of these data into the verification data area of the secured Initialisation Table. In particular, the Verlag der Kreditwirtschaft integrates the data that ensure for the integrity and authenticity of the IC and its ROM mask into the Initialisation Table and secures afterwards the Initialisation Table by a signature to enable the later verification of the integrity and authenticity of the Initialisation Table.

The finalised Initialisation Table is delivered from the Verlag der Kreditwirtschaft to the Initialiser. The Initialiser performs the TOE´s initialisation by executing the supplied Initialisation Table. The load script contains only dedicated initialisation commands, and the TOE only accepts integer and authentic Initialisation Tables.

In addition, the Verlag der Kreditwirtschaft generates the personalisation data and sends them to the Personaliser (Sagem ORGA GmbH or other personalisation facility) for personalisation of the TOE. For the personalisation process, only dedicated personalisation commands are applicable.

For a more detailed description of the processes for the generation of the ROM mask and the (finalised) Initialisation Tables and the underlying concept for integration and handling of the integrity and authenticity data refer to /SECCOS Perso/.

In case that the product delivered by Sagem ORGA GmbH contains – due to customer requirements – additional banking applications as GeldKarte Application, EMV Application, electronic cash Application (/SECCOS EC/), etc. the insertion of the necessary additional application data into the Initialisation Table is perfomed by Sagem ORGA GmbH in such a manner that the evaluated TOE´s Signature Application is not altered or influenced by the additional applications.

2.3 TOE Operational Environment

Two different types of operational environment have to be considered for the TOE:

Initialisation and Personalisation Phase

Prior to the issuance of the TOE to the end-user (cardholder resp. signatory), the TOE has to be completed in its initialisation and personalisation phase. The initialisation data containing in particular the pre-defined TOE´s dedicated Signature Application are loaded during the TOE´s initialisation by executing the finalised Initialisation Table. The following personalisation phase covers the generation of the SCD/SVD pair and the loading of the personalisation data.

End-Usage Phase

After the issuance of the personalised TOE to the end-user (cardholder resp. signatory), the TOE is under control of the cardholder. Main interaction of the cardholder with the TOE as SSCD will be performed via the Signature-Creation Application (SCA) whereat the secure communication between the TOE and the SCA will be realised either by a trusted channel resp. trusted path using appropriate cryptographic means or alternatively by an environment trusted by the cardholder. In the latter case, it is up to the cardholder to set-up an appropriate trusted environment.

The TOE as SSCD and the external IT system (SCA) communicate via a terminal whereat the following types of terminals can be involved: Private / Company own Terminal, Business Terminal, Administration Terminal. The three types of terminals can be differentiated by the TOE as SSCD as different authentication certificates for key based component authentication are used. For details refer to /SECCOS Sig/.

2.4 TOE Intended Usage

The TOE - based on the so-called SECCOS operating system on a smartcard integrated circuit - is explicitly intended to be used as Secure Signature-Creation Device (SSCD) for qualified electronic signatures in accordance with the European Directive 1999/93/EC on electronic signatures /ECDir/, the German Signature Act /SigG01/ and the German Signature Ordinance /SigV01/. The EU compliant Signature Application ZKA-SigG-Q of the TOE is explicitly designed for the generation of legally binding qualified electronic signatures as defined in /ECDir/, /SigG01/ and /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 SECCOS operating system platform provides a fully interoperable ISO 7816 compliant multi-application platform which can be used for smartcards with high security applications. The wide range of the various technical, functional and security features of the SECCOS operating system platform as integrated in the Sagem ORGA product allows in particular beside the above mentioned Signature Application for further separated (banking) applications as GeldKarte Application, EMV Application, electronic cash Application, etc.

The TOE´s Signature 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.

To support the security of the above mentioned features of the TOE and to protect the TOE´s specific SSCD related assets (refer to chap. 3.1), the TOE provides appropriate countermeasures for resistance especially against the following attacks:

- Cloning of the product
- Unauthorised disclosure of confidential data (e.g. Signature-Creation Data (SCD), operating system code, keys, PINs)
- Unauthorised manipulation of data
- Identity usurpation (e.g. usage of the Signature Application by an unauthorised user, i.e. other than the legitimate signatory)
- Forgery of data (e.g. electronic signature, Signature-Verification Data (SVD), data to be signed (DTBS))
- Derivation of SCD from corresponding SVD

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

2.5 Application Note: Scope of SSCD ST Application

This ST-Lite is intended to be used for a CC evaluation of a Secure Signature-Creation Device (SSCD) in accordance to 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-Lite 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-Lite 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-Lite 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

Note:

Most of the following contents have been drawn without any change from the Protection Profile /PP SSCD Type 3/. For an easier understanding and comparison, all changes and supplements to /PP SSCD Type 3/ are marked as underlined text.

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-Lite for several reasons. First, the confidentiality is needed for the protection of intellectual and 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 applications. For instance, knowledge about the implementation of the Operating 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 Assets of the IC

For a detailed description of the TOE´s assets concerning the inderlying IC and ACL refer to /ST IC+ACL/ and /BSI-PP-0002/, chap. 3.1.

3.1.2 Assets of the TOE´s Signature Application

All the TOE´s assets concerning its dedicated Signature Application ZKA-SigG-Q as defined in the Protection Profile /PP SSCD Type 3/, chap. 3 have been taken over. Specific assets related to the initialisation and personalisation phase of the TOE´s life-cycle model are added.

Assets / ZKA-SigG-Q Application	
Name	**Description**
SCD	Private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained)
SVD	Public key linked to the SCD and used to perform an electronic signature verification (integrity of the SVD when it is exported must be maintained)

DTBS and DTBS-representation	Set of data, or its representation which is intended to be signed (their integrity must be maintained)
VAD	PIN code or biometrics data entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)
RAD	Reference PIN code or biometrics authentication reference used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)
Signature-creation function of the SSCD using the SCD	(The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures)
Electronic signature	(Unforgeabilty of electronic signatures must be assured)
Initialisation Table	EEPROM initialisation data related to the TOE´s dedicated Signature Application inclusive the verification data used to verifiy the authenticity of the IC and its ROM mask and to verifiy the integrity and authenticity of the EEPROM initialisation data during the TOE´s initialisation phase (integrity and authenticity of the initialisation and verification data must be assured)
Personalisation Data	Personalisation data related to the TOE´s dedicated Signature Application (integrity, authenticity and confidentiality of the personalisation data must be assured)
ChipPWD	Special PIN securing the initialisation and personalisation process, refer to /SECCOS Perso/ (integrity and confidentiality of ChipPWD must be maintained)

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

According to the Protection Profile /PP SSCD Type 3/, chap. 3, the following subjects deal with the assets of the TOE´s Signature Application:

Subjects / ZKA-SigG-Q Application	
Name	**Description**
S.User	End user of the TOE which can be identified as S.Admin or S.Signatory.
S.Admin	User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions.
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.
S.OFFCARD	Attacker. A human or a process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker

	is to access Application sensitive information. The attacker has a **high level potential attack** and **knows no secret**.

3.2 Assumptions

All assumptions on the environment of the TOE concerning its dedicated Signature Application ZKA-SigG-Q as defined according to /PP SSCD Type 3/, chap. 3.1 have been taken over. Specific assumptions related to the initialisation and personalisation phase of the TOE´s life-cycle model are added. The set of assumptions related to the TOE´s Signature Application is listed in the table below.

Assumptions for the Environment of the TOE / ZKA-SigG-Q Application	
Name	**Definition**
A.CGA	**Trustworthy Certification-Generation Application** The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.
A.SCA	**Trustworthy Signature-Creation Application** The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.
A.INIT_Process	**Security of the Initialisation Process** The Initialisation Table developed and delivered by the Smartcard Embedded Software Developer (Sagem ORGA GmbH) is handled by the customer (Verlag der Kreditwirtschaft) in an adequate secure manner. This concerns in particular the post-processing of the supplied Initialisation Table in which additional verification data for securing the later initialisation process are generated and inserted into the Initialisation Table by the customer himself. In particular, the security data used for the generation of the verification data related to the Initialisation Table are treated by the customer with sufficient security. The handling of the (finalised) Initialisation Tables at the Verlag der Kreditwirtschaft resp. at the initialisation center as well as the transfer of these data between the different sites is conducted with respect to data integrity and authenticity. The initialisation process itself and the preceding finalisation of the Initialisation Table for the initialisation by the customer is set-up and performed according to the descriptions and requirements given in /SECCOS Perso/. The ChipPWD is kept confidential.
A.PERS_Process	**Security of the Personalisation Process** The originator of the personalisation data and the personalisation center responsible for the personalisation of the TOE (in particular its dedicated Signa-

	ture 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 SECCOS 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. The personalisation process is set-up and performed according to the descriptions and requirements given in /SECCOS Perso/. The ChipPWD is kept confidential.

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.

Generally, threats can be split into the following types:

- threats against which a specific protection by the TOE is required
- threats against which a specific protection by the TOE environment is required
- threats against which a specific protection by a combination of the TOE and its environment is required.

Furthermore, in view of the target of an attack, the assumed threats can be divided into the following three types:

- Unauthorized disclosure of assets:

  This type of threats covers unauthorized disclosure of assets by attackers who may possess a wide range of technical skills, resources and motivation. Such attackers may also have technical awareness of the product.

- Theft or unauthorized use of assets:

  Potential attackers may gain access to the TOE and perform operation for which they are not allowed. For example, such attackers may personalize the product in an unauthorized manner, or try to gain fraudulently access to the smartcard system.

- Unauthorized modification of assets:

The TOE may be subjected to different types of logical or physical attacks which may compromise security. Due to the intended usage of the TOE (the TOE environment may be hostile), the TOE security parts may be bypassed or compromised reducing the integrity of the TOE security mechanisms and disabling their ability to manage the TOE security. This type of threat includes the implementation of malicious trojan horses, trapdoors, downloading of viruses or unauthorized programs.

3.3.1 Threats on the IC

Several threats on the assets of the underlying IC and ACL against which specific protection within the TOE or its environment is required are existing. The relevant threats can be found in detail in /ST IC+ACL/ and /BSI-PP-0002/, chap. 3.3.

3.3.2 Threats on the TOE´s Signature Application

Several threats on the TOE´s dedicated Signature Application ZKA-SigG-Q against which specific protection within the TOE or its environment is required are existing. These threats are defined according to /PP SSCD Type 3/, chap. 3.2 whereat specific threats related to the initialisation and personalisation phase of the TOE´s life-cycle model are added. The set of threats on the TOE´s Signature Application is listed in the table below.

Threats / ZKA-SigG-Q Application	
Name	**Definition**
T.Hack_Phys	**Physical Attacks through the TOE Interfaces** An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat addresses all the assets.
T.SCD_Divulg	**Storing, Copying, and Releasing of the Signature-Creation Data** An attacker can store, copy, the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE.
T.SCD_Derive	**Derive the Signature-Creation Data** An attacker derives the SCD from public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.
T.Sig_Forgery	**Forgery of the Electronic Signature** An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.Sig_Repud	**Repudiation of Signatures** If an attacker can successfully threaten any of the assets, then the non repudation of the electronic signature is compromised. This results in the signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his unrevoked certificate.
T.SVD_Forgery	**Forgery of the Signature-Verification Data** An attacker forges the SVD presented by the TOE to the CGA. This result in loss of SVD integrity in the certificate of the signatory.
T.DTBS_Forgery	**Forgery of the DTBS-Representation** An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intended to sign.
T.SigF_Misuse	**Misuse of the Signature-Creation Function of the TOE** An attacker misuses the signature-creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.
T.INIT_Aut	**Authentication for Initialisation Process** A successful loading of EEPROM initialisation data for the TOE´s Signature Application without authorisation (of the external world) would be a threat to the security of the TOE.
T.INIT_Data	**Loading of Manipulated Initialisation Data** An attacker loads EEPROM initialisation data for the TOE´s Signature Application (by usage of a manipulated Initialisation Table) for which the intended integrity and/or authenticity is not given.
T.PERS_Aut	**Authentication for Personalisation Process** A successful storage of personalisation data for the TOE´s Signature Application without authorisation (of the external world) would be a threat to the security of the TOE.
T.PERS_Data	**Modification or Disclosure of Personalisation Data** A successful modification or disclosure of personalisation data for the TOE´s Signature Application during the data import would be a threat to the security of the TOE.

3.4 Organisational Security Policies

The specific organisational security policies for the TOE´s dedicated Signature Application ZKA-SigG-Q are defined according to /PP SSCD Type 3/, chap. 3.3. The organisational se-

curity policies contain the requirement that the TOE as SSCD is used together with trustworthy applications in the framework of /ECDir/ and the generation of qualified electronic signatures.

The complete set of specific organisational security policies for the Signature Application is listed in the following table.

Organisational Security Policies for the TOE / ZKA-SigG-Q Application	
Name	**Definition**
P.CSP_QCert	**Qualified certificate** The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.
P.QSign	**Qualified electronic signatures** The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate (according to directive Annex 1) and is created by a SSCD.
P.Sigy_SSCD	**TOE as secure signature-creation device** The TOE implements the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

4 Security Objectives

Note:

Most of the following contents have been drawn without any change from the Protection Profile /PP SSCD Type 3/. For an easier understanding and comparison, all changes and supplements to /PP SSCD Type 3/ are marked as underlined text.

4.1 Security Objectives for the TOE

Principally, the security objectives for the TOE cover 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 Security Objectives for the IC

Several security objectives for the underlying IC and ACL are defined. For a detailed description of these security objectives refer to /ST IC+ACL/ and /BSI-PP-0002/, chap. 4.1.

4.1.2 Security Objectives for the TOE´s Signature Application

The security objectives for the TOE´s dedicated Signature Application ZKA-SigG-Q as defined in /PP SSCD Type 3/, chap. 4.1 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, specific security objectives related to the initialisation and personalisation phase of the TOE´s life-cycle model are added.

Security Objectives / ZKA-SigG-Q Application	
Name	**Definition**
OT.EMSEC_Design	**Provide Physical Emanations Security** Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.
OT.Lifecycle_Security	**Lifecycle Security** The TOE shall provide safe destruction techniques for the SCD in case of regeneration.
OT.SCD_Secrecy	**Secrecy of the Signature-Creation Data**

	The secrecy of the SCD (used for signature generation) is reasonably assured against attacks with a high attack potential.
OT.SCD_SVD_Corresp	**Correspondence between SVD and SCD** The TOE shall ensure the correspondence between the SVD and the SCD. The TOE shall verify on demand the correspondence between the SCD stored in the TOE and the SVD if it has been sent to the TOE.
OT.SVD_Auth_TOE	**TOE ensures Authenticity of the SVD** The TOE provides means to enable the CGA to verify the authenticity of the SVD that has been exported by that TOE.
OT.Tamper_ID	**Tamper Detection** The TOE provides system features that detect physical tampering of a system component, and use those features to limit security breaches.
OT.Tamper_Resistance	**Tamper Resistance** The TOE prevents or resists physical tampering with specified system devices and components.
OT.Init	**SCD/SVD Generation** The TOE provides security features to ensure that the generation of the SCD and the SVD is invoked by authorised users only.
OT.SCD_Unique	**Uniqueness of the Signature-Creation Data** The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible low.
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.Sigy_SigF	**Signature Generation Function for the Legitimate Signatory Only** The TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.
OT.Sig_Secure	**Cryptographic Security of the Electronic Signature** The TOE generates electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the electronic signatures. The electronic signa-

	tures shall be resistant against these attacks, even when executed with a high attack potential.
OT.INIT_Process	**Security of the Initialisation Process** The TOE shall only load and store EEPROM initialisation data for the TOE´s Signature Application after the authentication of the external world. The TOE shall only load and store unaltered and authentic EEPROM initialisation data. The TOE shall detect flaws during the initialisation process, i.e. during the loading of the EEPROM initialisation data and the following verification process (check of the imported data for integrity and authenticity).
OT.PERS_Process	**Security of the Personalisation Process** The TOE shall only load and store personalisation data for the TOE´s Signature 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.

4.2 Security Objectives for the Environment of the TOE

The security objectives for the environment of the TOE concerning the TOE´s dedicated Signature Application ZKA-SigG-Q as defined in /PP SSCD Type 3/, chap. 4.2. 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, specific security objectives related to the initialisation and personalisation phase of the TOE´s life-cycle model are added.

The complete set of security objectives for the environment of the TOE resp. its Signature Application is listed in the table below.

Security Objectives for the Environment of the TOE / ZKA-SigG-Q Application	
Name	**Definition**
OE.CGA_QCert	**Generation of Qualified Certificates** The CGA generates qualified certificates which include inter alia (a) the name of the signatory controlling the TOE, (b) the SVD matching the SCD implemented in the TOE under sole control of the signatory, (c) the advanced signature of the CSP.

OE.SVD_Auth_CGA	**CGA Verifies the Authenticity of the SVD** The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.
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.SCA_Data_Intend	**Data Intended to be Signed** The SCA (a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE, (b) sends the DTBS-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE (c) attaches the signature produced by the TOE to the data or provides it separately.
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.INIT_Process	**Security of the Initialisation Process** The Initialisation Table developed and delivered by the Smartcard Embedded Software Developer (Sagem ORGA GmbH) is handled by the customer (Verlag der Kreditwirtschaft) in an adequate secure manner. This concerns in particular the post-processing of the supplied Initialisation Table in which additional verification data for securing the later initialisation process are generated and inserted into the Initialisation Table by the customer himself. In particular, the security data used for the generation of the verification data related to the Initialisation Table are treated by the customer with sufficient security. The handling of the (finalised) Initialisation Tables at the Verlag der Kreditwirtschaft resp. at the initialisation center as well as the transfer of these data between the different sites is conducted with respect to data integrity and authenticity. The initialisation process itself and the preceding finalisation of the Initialisation Table for the initialisation by the customer is set-up and performed according to the descriptions and requirements given in /SECCOS Perso/. The ChipPWD is kept confidential.
OE.PERS_Process	**Security of the Personalisation Process**

	The originator of the personalisation data and the personalisation center responsible for the personalisation of the TOE (in particular its dedicated Signature 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 SECCOS 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. The personalisation process is set-up and performed according to the descriptions and requirements given in /SECCOS Perso/. The ChipPWD is kept confidential.

5 IT Security Requirements

5.1 TOE Security Requirements

This section contains information on the TOE security functional requirements, the SOF claim for the TOE security functional requirements and the 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 from /CC 2.2 Part2/ resp. /CC 2.1 Part2/, functional requirement components of /CC 2.2 Part2/ resp. /CC 2.1 Part2/ with extension as well as self-defined functional requirement components.

Note:

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.

Notation:

Operations done in /PP SSCD Type 3/: **bold** text

Completion of uncompleted operations in /PP SSCD Type 3/: ***bold italic*** text

Changes / supplements to /PP SSCD Type 3/: <u>underlined</u> text

5.1.1.1 TOE Security Functional Requirements for the IC

For a detailed overview of the SFRs defined for the underlying IC and ACL refer to /ST IC+ACL/ and /BSI-PP-0002/, chap. 5.1.1, 8.4, 8.5, 8.6.

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

For the TOE´s Signature Application ZKA-SigG-Q, the TOE maintains an SFP as defined as follows:

SFP ZKA-SigG-Q

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 ZKA-SigG-Q is subdivided into four SFPs according to /PP SSCD Type 3/, 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 Signature Application are specified in detail within /PP SSCD Type 3/, chap. 5.1.2.

For the initialisation of the TOE´s Signature Application ZKA-SigG-Q in the sense of loading the EEPROM initialisation data by usage of the relevant Initialisation Table resp. by usage of the applicable initialisation commands of the SECCOS operating system platform, the TOE maintains an SFP as defined as follows:

SFP Smartcard Initialisation

Subjects:

- User

Security attributes for subjects:

- General Attribute Role (Administrator, Signatory)

Objects:

- EEPROM initialisation data
- Verification data (over the EEPROM initialisation data)

Security attributes for objects:

- State Attribute Chip State (value between 1 and 20, refer to /SECCOS Perso/, chap. 7)

Operations (Access Modes):

- Loading of EEPROM initialisation data
- Import of verification data for verification of the loaded EEPROM initialisation data
- Modification of Chip State

Hint: The generation of the SCD / SVD key pair is part of the above defined SFP Initialisation.

A detailed description of the smartcard initialisation process and the handling of the attribute Chip State is given in the specification /SECCOS Perso/, chap. 4 and 7.

For the personalisation of the TOE´s Signature Application ZKA-SigG-Q in the sense of loading the personalisation data by usage of the applicable personalisation commands of the SECCOS operating system platform, the TOE maintains an SFP as defined as follows:

SFP Smartcard Personalisation

Subjects:

- User

Security attributes for subjects:

- General Attribute Role (Administrator, Signatory)

Objects:

- Personalisation data

Security attributes for objects:

- State Attribute Chip State (value between 1 and 20, refer to /SECCOS Perso/, chap. 7)

Operations (Access Modes):

- Loading of personalisation data

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 Personalisation.

A detailed description of the smartcard personalisation process and the handling of the attribute Chip State is given in the specification /SECCOS Perso/, chap. 5 and 7.

For the TOE´s Signature Application, the following SFRs are defined according to /PP SSCD Type 3/, chap. 5.1 whereat specific SFRs related to the initialisation and personalisation phase of the TOE´s life-cycle model are added. The SFRs can be categorized as follows: cryptographic support, user data protection, identification and authentication, security management, protection of the TSF, trusted paths/channels.

FCS **Cryptographic Support**	
FCS_CKM **Cryptographic Key Management**	
FCS_CKM.1 **Cryptographic Key Generation**	
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	**FCS_CKM.1.1** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***Renesas RSA Key Generation***] and specified cryptographic key sizes [***between 1024 bit and 1984 bit modulus length***] that meet the following: [***/ALGCAT/, chap. 1.3, 3.1, 4***].

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.4 **Cryptographic Key Destruction**	
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 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, 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.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [***physical erasure of private key value***] that meets the following: [***none***]. **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.
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*	**FCS_COP.1.1 / CORRESP** The TSF shall perform [**SCD/SVD correspondence verification**] in accordance with a specified cryptographic algorithm [***RSA***] and cryptographic key sizes

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	[***between 1024 bit and 1984 bit modulus length***] that meet the following: [***/ALGCAT/, chap. 3.1***]. ***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.1.1 / SIGNING The TSF shall perform [**digital signature-generation**] in accordance with a specified cryptographic algorithm [***RSA***] and cryptographic key sizes [***between 1024 bit and 1984 bit modulus length***] that meet the following: [***/ALGCAT/, chap. 3.1***].

FDP **User Data Protection**	
FDP_ACC **Access Control Policy**	
FDP_ACC.1 **Subset Access Control**	
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:	**FDP_ACC.1.1 / SVD Transfer SFP** The TSF shall enforce the [**SVD Transfer SFP**] on [**export of SVD by User**].

--- Audit: ---	
	FDP_ACC.1.1 / Initialisation SFP The TSF shall enforce the [**Initialisation SFP**] on [**generation of SCD/SVD pair by User**].
	FDP_ACC.1.1 / Personalisation SFP The TSF shall enforce the [**Personalisation SFP**] on [**creation of RAD by Administrator**].
	FDP_ACC.1.1 / 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.1.1 / Smartcard Initialisation SFP The TSF shall enforce the [**Smartcard Initialisation SFP**] on [**loading and verification of the EEPROM initialisation data by Administrator**].
	FDP_ACC.1.1 / Smartcard Personalisation SFP The TSF shall enforce the [**Smartcard Personalisation SFP**] on [**import of personalisation data y Administrator**].
FDP_ACF **Access Control Functions**	
FDP_ACF.1 **Security Attribute Based Access Control**	
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	**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" 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**].

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	
	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.1.1 / 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.1.1 / 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.1.1 / Smartcard Initialisation SFP The TSF shall enforce the [**Smartcard Initialisation SFP**] to objects based on the following: [**General attribute and State attribute**].

	FDP_ACF.1.2 / Smartcard 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" is allowed to perform the smartcard initialisation process (loading of the EEPROM initialisation data) and to set the security attribute "Chip State" to the value 7**]. **FDP_ACF.1.3 / Smartcard Initialisation SFP** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]. **FDP_ACF.1.4 / Smartcard Initialisation SFP** The TSF shall explicitly deny access of subjects to objects based on the [**none**].
	FDP_ACF.1.1 / Smartcard Personalisation SFP The TSF shall enforce the [**Smartcard Personalisation SFP**] to objects based on the following: [**General attribute and State attribute**]. **FDP_ACF.1.2 / Smartcard Personalisation 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" is allowed to perform the smartcard personalisation process (loading of the personalisation data) and to set the security attribute "Chip State" to the value 20**]. **FDP_ACF.1.3 / Smartcard Personalisation SFP** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]. **FDP_ACF.1.4 / Smartcard 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**	
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.	**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.

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_ITC **Import from Outside TSF Control**	
FDP_ITC.1 **Import of User Data without Security Attributes**	
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 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	**FDP_ITC.1.1 / DTBS** The TSF shall enforce the [**Signature-Creation SFP**] when importing user data, controlled under the SFP, from outside of the TSC. **FDP_ITC.1.2 / DTBS** The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC. **FDP_ITC.1.3 / DTBS** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [**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**	
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.1.1** 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**].
FDP_SDI **Stored Data Integrity**	
FDP_SDI.2 **Stored Data Integrity Monitoring and Action**	
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	**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.2.1 / 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**].

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 DTBS-representation temporarily stored by TOE has the user data attribute “integrity checked stored data”. **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**	
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	**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.

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.1.1 / 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. **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. **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.

FIA **Identification and Authentication**	
FIA_AFL **Authentication Failures**	
FIA_AFL.1 **Authentication Failure Handling**	
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	**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**].

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_ATD **User Attribute Definition**	
FIA_ATD.1 **User Attribute Definition**	
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.1.1** 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**	
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.	**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.

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.1.2** 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**	
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.1.1** 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**	
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 functions - 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_MOF.1.1** The TSF shall restrict the ability to [**enable**] the functions [**signature-creation function**] to [**Signatory**].
FMT_MSA **Management of Security Attributes**	
FMT_MSA.1 **Management of Security Attributes**	
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_SMR.1 Security roles Management:	**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**].

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.1.1 / Signatory The TSF shall enforce the [**Signature-Creation SFP**] to restrict the ability to [**modify**] the security attributes [**SCD operational**] to [**Signatory**].
	FMT_MSA.1.1 / Smartcard Initialisation The TSF shall enforce the [**Smartcard Initialisation SFP**] to restrict the ability to [**switch to value 7**] the security attributes [**Chip State**] to [**Administrator**].
	FMT_MSA.1.1 / Smartcard Personalisation The TSF shall enforce the [**Smartcard Personalisation SFP**] to restrict the ability to [**switch to value 20**] the security attributes [**Chip State**] to [**Administrator**].
FMT_MSA.2 **Secure Security Attributes**	
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.2.1** The TSF shall ensure that only secure values are accepted for security attributes.
FMT_MSA.3 **Static Attribute Initialisation**	
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 secu-	**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.

rity 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: a) Basic: Modifications of the default setting of permissive or restrictive rules b) Basic: All modifications of the initial values of security attributes	**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.
	FMT_MSA.3.1 / Smartcard Initialisation The TSF shall enforce the [**Smartcard Initialisation SFP**] to provide [**restrictive**] default values **"Chip State" is set to value 1** for security attributes that are used to enforce the SFP. **FMT_MSA.3.2 / Smartcard Initialisation** The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.
FMT_MTD **Management of TSF Data**	
FMT_MTD.1 **Management of TSF Data**	
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_SMR.1 Security roles Management:	**FMT_MTD.1.1** The TSF shall restrict the ability to [**modify**] the [**RAD**] to [**Signatory**].

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_SMF **Specification of Management Functions**	
FMT_SMF.1 **Specification of Management Functions**	
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.1.1** 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 /AIS 32/.
FMT_SMR **Security Management Roles**	
FMT_SMR.1 **Security Roles**	
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.1.1** The TSF shall maintain the roles [**Administrator and Signatory**]. **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**	
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 abstract 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_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).*
FPT_EMSEC **TOE Emanation**	
FPT_EMSEC.1 **TOE Emanation**	
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*].	**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**].

Hierarchical to: No other components Dependencies: No dependencies Management: --- Audit: ---	**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**	
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.1.1** 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. SECCOS operating system 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*** - ***Inconsistencies in the signature-creation process*** - ***Fault injection attacks***].

	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**	
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. Hierarchical to: No other components Dependencies: - FMT_MOF.1 Management of security functions behaviour Management: --- Audit: a) Minimal: if detection by IT means, detection of intrusion.	**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.
FPT_PHP.3 **Resistance to Physical Attack**	
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.3.1** The TSF shall resist [***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 [***IC***] by responding automatically such that the TSP is not violated.

FPT_TST **TSF Self Test**	
FPT_TST.1 **TSF Testing**	
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.1.1** 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***]. ***Application Note*** *During initial start-up means before code execution.* ***Refinement*** *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.* **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 Smartcard Embedded Software of the TOE 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	
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.1.1 / 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 CGA***] to initiate communication via the trusted channel. **FTP_ITC.1.3 / SVD Transfer** The TSF **or the CGA** shall initiate communication via the trusted channel for [**export SVD**].
	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 chan-

	nel 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.1.1 / Smartcard Personalisation The TSF shall provide a communication channel between itself and a remote trusted IT product **personalisation device** 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 / Smartcard Personalisation** The TSF shall permit [**the remote trusted IT product (personalisation device)**] to initiate communication via the trusted channel. **FTP_ITC.1.3 / Smartcard Personalisation** The TSF **or the personalisation device** shall initiate communication via the trusted channel for [**import of personalisation data**].
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	**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.

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	

5.1.2 SOF Claim for TOE Security Functional Requirements

According to the Protection Profile /PP SSCD Type 3/ the required level for the Strength of Function of the TOE security functional requirements listed in the preceding chap. 5.1.1 is rated “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 claimed as

EAL4 augmented by AVA_MSU.3 and AVA_VLA.4

Hence, the assurance level claimed for the TOE matches the evaluation assurance requirements stated in the Protection Profile /PP SSCD Type 3/, chap. 5.2.

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.1 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.1 Testing: High-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 2.2 Part3/ and /CEM 2.2 Part2/ resp. /CC 2.1 Part3/ and /CEM 1.0 Part2/. No further refinements of the chosen assurance components are specified, except the following one:

AVA_MSU.3

AVA_MSU.3 is interpreted resp. refined as follows:

Additionally evaluator tests are required where necessary. This testing, can be part of the penetration testing under AVA_VLA4. It is decided on a case by case basis if the evaluator performs misuse-testing as additional part of penetration testing to confirm or disprove the misuse analysis. Specifically, if high attack potential is assumed, such independent misuse-testing is performed.

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.

5.2.1.1 Certification Generation Application (CGA)

For the Certification Generation Application (CGA), the following SFRs are defined according to /PP SSCD Type 3/, 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: - [FDP_ITC.1 Import of user data without security attributes or	**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/***].

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.3.1 / 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. <u>Hierarchical to:</u> No other components <u>Dependencies:</u> - [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] <u>Management:</u> --- <u>Audit:</u> 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.1.1 / 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.1.1 / 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 Type 3/, 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.1.1 / SCA Hash** The TSF shall perform [**hashing the DTBS**] in accordance with a specified cryptographic algorithm [***SHA-1 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 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	**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.

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 trusted channel is required*].	**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 the trusted channel for [**signing DTBS-representation by means of the SSCD**].

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_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 all trusted path failures, if available c) Basic: All attempted uses of the trusted path func-	**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***].

tions 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 specific security requirements for the Non-IT-environment of the TOE are defined according to /PP SSCD Type 3/, 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.

Security Requirements for the Non-IT-Environment of the TOE / ZKA-SigG-Q Application	
Name	**Definition**
R.Administrator_Guide	**Application of Administrator Guidance** The implementation of the requirements of the Directive, ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (e), stipulates employees of the CSP or other relevant entities to follow the administrator guidance provided for the TOE. Appropriate supervision of the CSP or other relevant entities shall ensures the ongoing compliance.
R.Sigy_Guide	**Application of User Guidance** The SCP implementation of the requirements of the Directive, ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (k), stipulates the signatory to follow the user guidance provided for the TOE.
R.Sigy_Name	**Signatory's Name in the Qualified Certificate** The CSP shall verify the identity of the person to which a qualified certificate is issued according to the Directive [1], ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (d). The CSP shall verify that this person holds the SSCD which implements the SCD corresponding to the SVD to be included in the qualified certificate.
R.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.INIT_Process	**Security of the Initialisation Process** The Initialisation Table developed and delivered by the Smartcard Embedded Software Developer (Sagem ORGA GmbH) shall be handled by the customer (Verlag der Kreditwirtschaft) in an adequate secure manner. This concerns in particular the post-processing of the supplied Initialisation Table in which additional verification data for securing the later initialisation process are generated and inserted into the Initialisation Table by the cus-

	tomer himself. In particular, the security data used for the generation of the verification data related to the Initialisation Table shall be treated by the customer with sufficient security. The handling of the (finalised) Initialisation Tables at the Verlag der Kreditwirtschaft resp. at the initialisation center as well as the transfer of these data between the different sites shall be conducted with respect to data integrity and authenticity. The initialisation process itself and the preceding finalisation of the Initialisation Table for the initialisation by the customer shall be set-up and performed according to the descriptions and requirements given in /SECCOS Perso/. The ChipPWD shall be kept confidential.
R.PERS_Process	**Security of the Personalisation Process** The originator of the personalisation data and the personalisation center responsible for the personalisation of the TOE (in particular its dedicated Signature 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 SECCOS 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. The personalisation process shall be set-up and performed according to the descriptions and requirements given in /SECCOS Perso/. The ChipPWD shall be kept confidential.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 TOE Security Functions / TOE-IC

For a detailed description of the TOE´s TSF concerning the inderlying IC and ACL refer to /ST IC+ACL/.

6.1.2 TOE Security Functions for the TOE´s Signature Application

The following section gives a survey of the TSFs concerning the TOE´s dedicated Signature Application ZKA-SigG-Q.

TOE Security Functions / ZKA-SigG-Q Application	
Access Control	
F.ACS_SIG	**Security Attribute Based Access Control / ZKA-SigG-Q Application**
	For the TOE´s dedicated Signature Application ZKA-SigG-Q, the TSF enforces the SFP AC-ZKA-SigG-Q as defined in chap. 5.1.1.2. 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. The TSF covers the following functionality: • The TSF manages the following security attributes: - For subject User: General Attribute “Role” (Administrator, Signatory), 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) • The user with the security attribute “Role” set to “Administrator” 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 op-

	erational" 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.
F.ADMIN_SIG	**Administration of the TOE / ZKA-SigG-Q Application**
	The TSF manages the TOE´s initialisation and personalisation process within the initialisation and personalisation phase of the TOE´s life-cycle. As supplement to the functionality covered by the TSF F.ACS_SIG the TSF provides the following functionality: • 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. Furthermore, the TSF enforces the SFPs Smartcard Initialisation and Smartcard Personalisation as defined in chap. 5.1.1.2. The TSF controls the initialisation and personalisation process for the TOE. In detail: • The TSF manages a further security attribute of the TOE: State attribute "Chip State" which controls the different phases of the TOE´s life-cycle and the availability of the platform commands. • The user with the security attribute "Role" set to "Administrator" is allowed to perform a secure modification of the security attribute "Chip State" (according to the rules defined in /SECCOS Perso/). • The user with the security attribute "Role" set to "Administrator" is allowed to load the EEPROM initialisation data and to trigger the subsequent verification process of the loaded data (according to the rules defined in /SECCOS Perso/, chap. 4 and 7). • The user with the security attribute "Role" set to "Administrator" is allowed to import the personalisation data (according to the rules defined in /SECCOS Perso/, chap. 5 and 7).
Identification and Authentication	
F.PIN_SIG	**PIN Based User Authentication for the Signatory**

	The TSF handles the PIN based user authentication of the Signatory (authentication towards the TOE). The TSF is only active during the end-usage phase of the TOE´s life-cycle. For the PIN based user authentication process, the TSF compares the verification authentication data (VAD) provided by a subject against the corresponding secret reference authentication data (RAD) stored permanently on the card. The TSF uses for the authentication process the RAD referenced by the external world. The access to RAD is controlled by the relevant SFP for access control as defined in chap. 5.1.1.2, which is realised by the corresponding TSF F.ACS_SIG for access control. The RAD used for authentication purposes is connected with an own error usage counter. The TSF detects for RAD when a pre-defined number of consecutive unsuccessful authentication attempts occurs related to the user authentication process. Each consecutive unsuccessful comparison of the presented VAD against RAD is recorded by the TSF in order to limit the number of further authentication attempts with RAD. In the case of a successful authentication attempt a corresponding actual security state for RAD is set and the error usage counter of RAD is re-initialised. If an authentication attempt with RAD fails, the corresponding actual security state is reset and the error usage counter of RAD is decreased. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF blocks RAD for further authentication attempts. RAD with an expired error usage counter can be unblocked by usage of the related resetting code (if existing), provided that the resetting code itself is not blocked. Otherwise, there is no way to unblock RAD so that RAD is invalid for each further authentication process. The unblocking of a blocked RAD 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 RAD, the expired error usage counter is re-initialised and hence, RAD can be used further on for authentication attempts. The TSF supports the following options: - Authentication procedure without change of RAD (OS command Verify) - Authentication procedure with change of RAD (OS command Change Reference Data) - Authentication procedure by usage of the resetting code related to RAD with change of RAD and reset of the expired error usage counter to its initial value (OS command Reset Retry Counter) The security state set due to a successful authentication attempt with RAD can be valid for several following TOE commands which depend on RAD (in particular, this concerns the signature-creation function). However, the validity of such an authentication state for the following OS commands depending on RAD is restricted by an internal counter. After the counter has expired, a further authentication attempt has to be performed for enabling the execution of further OS commands depending on RAD. The TSF does not check the quality of RAD; the sufficient quality of RAD lies in the responsibility of the external world only. In particular, the size of RAD and the resetting code(if existing) shall not be smaller than 6 digits. The transfer of VAD 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 TSF F.SEC_EXCH is involved.
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 - Security critical data in the RAM area (e.g. status information as actual security status for key or PIN based authentication, information on the actual Security Environment, information on Secure Messaging, information on Chaining) - (Intermediate) Hash values The monitoring is based on the following attributes: - Checksum (CRC16) attached to the header of each file - Checksum (CRC16) attached to the data body of each file (if applicable) - Checksum (CRC16) attached to security critical data in the RAM area - Checksum (CRC16) attached to the (intermediate) hash value As PIN reference values and cryptographic keys incl. related attributes which are stored in the non-volatile memory are stored within EFs, especially the objects SCD, SVD and RAD are secured for integrity errors. Furthermore, access rules as stored as well in EFs are secured in the same way, and access rule references as stored in file headers are secured by the checksum of the respective file header. Before the TOE accesses to checksum secured data, the TSF carries out 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, and the calling command will be aborted. If the data contained in a file are not of integrity, the affected data will not be used for data processing, and the calling command will be aborted. In particular, if the objects SCD, SVD or RAD are corrupted, the data will not be processed. If security critical RAM data are not of integrity, the TOE immediately jumps into an endless-loop (re-activation by reset possible). Corrupted (intermediate) hash values will as well not be processed, in particular not used for signature-creation.
Secure Data Exchange	
F.SEC_EXCH	**Integrity and 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. Furthermore, 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 confidentiality resp. integrity for the data exchange. Securing the data transfer with regard to data confidentiality resp. integrity is done by Secure Messaging according to the standard ISO/IEC 7816-4. The cryptographic keys used for securing the data transfer are keys negotiated during a preceding mutual authentication process (based on a random challenge and response procedure) between the TOE and the external world. For encryption / decryption and checksum securing / 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 its deallocation whereat the following memory areas are involved: - All volatile and non-volatile memory areas used for operations in which security relevant material as e.g. cryptographic data, PINs or other security critical data is operated - In particular affected: objects SCD, VAD and RAD The explicit erasure is carried out as physical erasure. The TSF is supported by the IC and ACL specific TSFs which integrate themselves memory re-preparation functionality.
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 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. SECCOS operating system 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 - Inconsistencies in the signature-creation process - Fault injection attacks The TSF makes use of HW and SW based security mechanisms to monitor resp. detect failures and attacks of the above mentioned types. In particular, the TSF is supported by the IC and ACL specific TSFs which integrate themselves appropriate functionality. Upon the detection of a failure or attack of the above mentioned types, the TSF reacts in such a way that the TSP is not violated. At least, the TOE reacts with the abortion of all related current processes. In the case of serious failures, the TOE immediately shuts down and cannot be used any longer within the actual session. Depending on the type of the detected failure or attack to the underlying IC, the ACL or the Smartcard Embedded Software code or data, the TOE afterwards will either be irreversible locked or can be used in further sessions (after re-activation 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 is active in the complete operational phase of the TOE´s life-cycle (initialisation, personalisation and end-usage phase), except for the usage of the insecured variant of the RSA key pair generation functionality which can be chosen for an accelerated initialisation process instead of the secured variant. 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 ensures that all countermeasures available are used in such a way that they support each other. In particular, the TSF is supported by the TSFs of the underlying IC and ACL whcih integrate themselves appropriate 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 PINs. 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 RAD and SCD. 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 re-formatting 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 processing of the output data. For DES operations the following requirements are enforced: During the execution of DES/3DES based operations, it is not possible to disclose the processed DES/3DES keys or parts of the key data. Furthermore, it is not possible to recover information about the input and output message or parts of it, if regarded as to be kept confidential. For RSA operations with private keys the following requirements are enforced: During the execution of the RSA operation, it is not possible to disclose the processed private key or

	parts of the key data. Furthermore, it is not possible to recover information about the later output message or parts of it, if regarded as to be kept confidential. For RSA operations with public keys the following requirements are enforced: During the execution of the RSA operation, it is not possible to recover information about the private key (or parts of the key data) corresponding to the processed public key. Furthermore, it is not possible to recover information about the input data or parts of it, if regarded as to be kept confidential. For hash value calculations processing security critical data the following requirements are enforced: During the execution of the hash value calculation, it is not possible to disclose the processed input data or parts of it. For the secured variant of the RSA key pair generation function the following requirements are enforced: During the generation of the RSA key pair, especially during the generation of the primes, the calculation of the CRT parameters of the private key part and the following key check, it is not possible to disclose the processed secret data of the private key part. For the random number generation the following requirements are enforced: During the generation of random numbers as well as during the online-tests of the HW-RNG it is not possible to gain information on the randoms given out to the operating system for further processing.
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 code and data. The TSF provides 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, as well as periodically during run-time to demonstrate the correct operation of its TSFs. The self test of the TOE is performed automatically 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 itself - with the capability to verify the integrity of TSF data during run-time. The self test is performed automatically and is directly 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´s life-cycle. Prior to the initialisation of the TOE, the ROM-code of the TOE can be verified on demand by the developer of the Smartcard Embedded Software. For this task, the TSF is supported by the TSF F.CRYPTO (part for SHA-1 hash value calculation). The integrity of the EEPROM-code is automatically checked by the TOE during the storage of the Initialisation Table in the framework of the TOE´s initialisation. For this task, the TSF is as well supported by the TSF F.CRYPTO (part for DES operations). The TSF supports all other TSFs defined for the TOE and its dedicated Signature Application.
Cryptographic Operations	
F.CRYPTO	**Cryptographic Support**
	The TSF provides cryptographic support for the other TSFs using cryptographic mechanisms. The TSF is directly supported by the TSFs of the underlying IC and ACL which supply cryptographic functionality.

	The TSF supports: - SHA-1 hash value calculation according to /ALGCAT/, chap. 2 resp. /FIPS 180-2/ - RIPEMD-160 hash value calculation according to /ALGCAT/, chap. 2 resp. /ISO 10118-3/ - DES/3DES algorithm according to the standard /ANSI X9.52/ with a key length of 56 resp. 112 bit entropie (used for encryption, decryption, MAC generation and verification) - RSA core algorithm according to the standard /PKCS1/ with key lengths between 1024 bit and 1984 bit modulus lengths (used for encryption, decryption, signature generation and verification) - Random number generation incl. online-test of the HW-RNG (used for key generation, authentication processes, ...) The resistance of the TSF against SPA, DPA, DFA and TA is discussed under the TSF F.SIDE_CHAN.
F.RSA_KEYGEN	**RSA Key Pair Generation**
	The TSF generates RSA key pairs with key lengths between 1024 bit and 1984 bit for asymmetric cryptography which can be used later on e.g. for electronic signatures. 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 the HW-RNG of 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. - Sufficient 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 pri-

	vate 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 discussed under the TSF F.SIDE_CHAN. The TSF directly makes use of the TSF of the ACL providing key pair generation functionality. Furthermore, functionality from the TSF F.CRYPTO (random number generation, RSA signature generation and verification) is used by the TSF. The public part of the generated key pair can only be exported via a trusted channel (refer to F.ACS_SIG).
F.GEN_SIG	**RSA Generation of Electronic Signatures**

	The TSF provides a signature-creation functionality based on asymmetric cryptography, particularly based on the RSA algorithm with key lengths between 1024 bit and 1984 bit.
	
	The TSF covers the following functionality:
	- Receiving (intermediate) hash values (without associated security attributes) and calculating hash values for the signing process
	- Generating electronic signatures according to
	  - /DIN 66291-4/, Annex A, chap. 2.1.1 “DSI according to ISO/IEC 9796-2 with Random Number” (with usage of hash algorithm RIPEMD-160)
	  - /DIN 66291-4/, Annex A, chap. 2.1.2 “DSI according to PKCS#1” (with usage of hash algorithm SHA-1)
	- Proving the correspondence of SCD and SVD
	
	The TSF function for generation of an electronic signature uses the signature scheme and 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 (part for random number generation). Furthermore, for the signature calculation itself, the TSF makes use of the TSF F.CRYPTO (part for RSA operations), and the computation of hash values is based on the TSF F.CRYPTO (parts for SHA-1 and RIPEMD-160 calculations).
	
	The resistance of the TSF against SPA, DPA, DFA and TA is discussed under the TSF F.SIDE_CHAN. For each private key the TSF 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 works in such a manner that no information about the private key can be disclosed during the generation of the electronic signature.

6.2 SOF Claim for TOE Security Functions

According to Common Criteria /CC 2.2 Part1/ and /CC 2.2 Part3/, resp. /CC 2.1 Part1/ and /CC 2.1 Part3/, all TOE security functions which are relevant for the assurance requirement AVA_SOF.1 are identified in this section.

For the TSFs defined for the underlying IC and ACL, information on the SOF claim can be found in /ST IC+ACL/.

The TSFs for the TOE´s Signature Application 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_SIG	Not applicable	The TSF is not realised by permutational or probabilistic mechanisms.
F.ADMIN_SIG	SOF high	The TSF includes a probabilistic password mechanism for the authentication of the Administrator.
F.PIN_SIG	SOF-high	The TSF includes a probabilistic password mechanism for the authentication of the Signatory.
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.SEC_EXCH	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 / 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-1,

		RIPEMD-160, RSA with key lengths between 1024 bit and 1984 bit modulus lengths as well as random number generation by usage of the HW-RNG incl. online-test of the HW-RNG. The HW-RNG satisfies the quality class P2 as stated in the evaluation of the underlying IC and its ACL. 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.
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 (incl. online-test of the HW-RNG) and the key check. In particular, functionality from the TSFs of the underlying IC and ACL related to the key generation function and the HW-RNG online-test of the ACL and from the TSF F.CRYPTO (random number generation, RSA signature generation and verification) is used by this TSF.
F.GEN_SIG	SOF high	The TSF implements under usage of the TSF F.CRYPTO, parts for RSA operations, hash value calculation and random number generation, a cryptographic mechanism for signature generation. The signature schemes and key lengths defined for the TSF comply with the requirements in /ALGCAT/, chap. 3.1 for qualified electronic signatures and fulfill therefore the requirements for SOF high.

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 documentation 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 and application part of the TOE, 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 Smartcard Embedded Software and applications are provided by its developer. The table below contains only the directly related documents, references to further documentation can be taken from the bibliography inside the mentioned documents.

Overview of Developer´s Smartcard Embedded Software and Application 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	- Functional Specification - High-Level Design - Low-Level Design
	ADV_SPM	- Document TOE Security Policy Model
AGD Guidance Documents	AGD_ADM	- User Guidance for the initialisation and personalisation of the TOE and its dedicated Signature Application - Additional information concerning initialisation and personalisation processes
	AGD_USR	- User Guidance for the usage of the TOE´s dedicated Signature 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 be performed as composite evaluation on basis of the evaluated IC AE55C1 (HD65255C1), Version 02 and the related Advanced Cryptographic Library, Version 1.43 (ACL) provided by Renesas Technology Corp. Therefore, for the underlying IC and its ACL the following documents will be at least provided by the IC and ACL developer:

Overview of Developer´s IC and ACL related Documents	
Class	**Documents**
Security Target	Security Target of the IC evaluation incl. Crypto Library, /ST IC+ACL/
Evaluation Report	Evaluation Technical Report Lite (ETR Lite) of the IC evaluation incl. Crypto Library, /ETRLite IC+ACL/
Configuration List	Configuration List for composite evaluation with Sagem ORGA, /ConfListRenesas/
User Guidances and Data Sheets	Data Sheet for the IC, /DS IC/
	User Guidance for the IC, /UG IC/
	User Guidance for the Crypto Library, /UG ACL/

7 PP Claims

7.1 PP References

The Security Target Lite for the TOE is based on the Protection Profile /PP SSCD Type 3/ 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 differences to the Protection Profile /PP SSCD Type 3/ 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 Type 3/ 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.

- Initialisation and Personalisation Phase of the TOE:

  The phases initialisation and personalisation of the TOE´s life-cycle model are considered as part of the operational phase (refer to chap. 2.2 and 2.3).

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 Type 3/ refer to the following section.

7.2 PP Changes and Supplements

The following changes and supplements with respect to the Protection Profile /PP SSCD Type 3/ for SSCDs of Type 3 are performed:

PP Changes and Supplements		
Name	**Reference**	**Description**
Initialisation Table	Chap. 3.1.2	New asset for the TOE´s initialisation phase
Personalisation Data	Chap. 3.1.2	New asset for the TOE´s personalisation phase
A.INIT_Process	Chap. 3.2	New assumption for the TOE´s initialisation phase
A.PERS_Process	Chap. 3.2	New assumption for the TOE´s personalisation phase
T.INIT_Aut	Chap. 3.3.2	New threat for the TOE´s initialisation phase

T.INIT_Data	Chap. 3.3.2	New threat for the TOE´s initialisation phase
T.PERS_Aut	Chap. 3.3.2	New threat for the TOE´s personalisation phase
T.PERS_Data	Chap. 3.3.2	New threat for the TOE´s personalisation phase
OT.DTBS_Integrity_TOE	Chap. 4.1.2	Changed objective due to extension of PP regards trusted channel/path
OT.INIT_Process	Chap. 4.1.2	New security objective for the TOE´s initialisation phase
OT.PERS_Process	Chap. 4.1.2	New security objective for the TOE´s personalisation phase
OE.HI_VAD	Chap. 4.2	Changed objective due to extension of PP regards trusted channel/path
OE.Trusted_Environment	Chap. 4.2	New objective due to extension of PP regards trusted channel/path
OE.INIT_Process	Chap. 4.2	New security objective for the TOE´s initialisation phase
OE.PERS_Process	Chap. 4.2	New security objective for the TOE´s personalisation phase
FDP_ACC.1 / Smartcard Initialisation SFP	Chap. 5.2.2	New SFR for the TOE´s initialisation phase
FDP_ACC.1 / Smartcard Personalisation SFP	Chap. 5.2.2	New SFR for the TOE´s personalisation phase
FDP_ACF.1 / Signature-Creation SFP	Chap. 5.1.1.2	New Application Note due to extension of PP regards trusted channel/path
FDP_ACF.1 / Smartcard Initialisation SFP	Chap. 5.2.2	New SFR for the TOE´s initialisation phase
FDP_ACF.1 / Smartcard Personalisation SFP	Chap. 5.2.2	New SFR for the TOE´s personalisation phase
FDP_ITC.1 / DTBS	Chap. 5.1.1.2	Changed Application Note due to extension of PP regards trusted channel/path
FDP_UIT.1 / TOE DTBS	Chap. 5.1.1.2	New Application Note due to extension of PP regards trusted channel/path
FMT_MSA.1 / Smartcard Initialisation	Chap. 5.2.2	New SFR for the TOE´s initialisation phase
FMT_MSA.1 / Smartcard Personalisation	Chap. 5.2.2	New SFR for the TOE´s personalisation phase
FMT_MSA.3 / Smartcard Initialisation	Chap. 5.2.2	New SFR for the TOE´s initialisation phase
FTP_ITC.1 / DTBS Import	Chap. 5.1.1.2	New Application Note due to extension of PP regards trusted channel/path
FTP_TRP.1 / TOE	Chap. 5.1.1.2	New Application Note
FPT_AMT.1	Chap. 5.1.1.2	New Application Note
FPT_FLS.1	Chap. 5.1.1.2	New Refinement
FPT_TST.1	Chap. 5.1.1.2	New Application Note and Refinements

FMT_SMF.1	Chap. 5.1.1.2	New SFR due to /AIS 32/
FTP_ITC.1 / Smartcard Personalisation	Chap. 5.1.1.2	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.INIT_Process	Chap. 5.2.2	New requirement for the TOE´s initialisation phase
R.PERS_Process	Chap. 5.2.2	New requirement for the TOE´s personalisation phase

8 Rationale

8.1 Introduction

The following chapters cover the Security Objectives Rationale (chap. 8.2), the Security Requirements Rationale (chap. 8.3), the TOE Summary Specification Rationale (8.7), the Dependency Rationale (8.4) and further CC related rationales (chap. 8.5, 8.6, 8.8, 8.9, 8.10).

The rationales are taken from the Protection Profile /PP SSCD Type 3/, chap. 6 with appropriate changes and supplements due to the differences outlined in the chapters 3 - 5 resp. 7.2 of this ST.

The tables in the subsections 8.2.1 “Security Objectives Coverage” and 8.3.1 “Security Requirement Coverage” provide the mapping of the security objectives and security requirements for the TOE. Information in informal form explicating the tables is given in the related subsections 8.2.2 “Security Objectives Sufficiency” and 8.3.2 “Security Requirement Sufficiency”.

The table in subsection 8.4.1 “Functional and Assurance Requirements Dependencies” lists all relevant dependencies, added with a justification for unsupported dependencies in the following subsection 8.4.2 and further information in subsection 8.5.

The rationale for extensions to /CC 2.2 Part2/ resp. /CC 2.1 Part2/ (new security functional requirements) is given in subsection 8.6.

Subsection 8.7 covers the TOE Summary Specification Rationale with a mapping of the TOE security functional requirements to the TOE security functions in subsection 8.7.1 and a rationale for the assurance measures in subsection 8.7.2.

Finally, the rationales for the specified strength of functions and assurance level is contained in subsections 8.8 and 8.9.

8.2 Security Objectives Rationale

According to the requirements of Common Criteria /CC 2.2 Part1/ and /CC 2.2 Part3/, resp. /CC 2.1 Part1/ and /CC 2.1 Part3/, the Security Objectives Rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. In detail, the Security Objectives Rationale shows that the security objectives stated for the TOE and its environment are suitable to counter the identified threats to security and to cover all of the identified organisational security policies and assumptions. Furthermore, the Security Objectives Rationale shows that each security objective of the TOE and its environment at least counters one threat or is correlated to one organisational security policy or assumption.

8.2.1 Security Objectives Coverage

Security Environment to Security Objectives Mapping

Threats – Assumptions – Policies / Security Objectives	OT.EMSEC_Design	OT.Lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.INIT_Process	OT.PERS_Process	OE.CGA_QCert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend	OE.Trusted_Environment	OE.INIT_Process	OE.PERS_Process
T.Hack_Phys	X			X			X	X													
T.SCD_Divulg				X																	
T.SCD_Derive									X			X									
T.SVD_Forgery						X										X					
T.DTBS_Forgery										X								X	X		
T.SigF_Misuse										X	X						X	X	X		
T.Sig_Forgery	X	X		X	X	X	X	X				X			X	X		X			
T.Sig_Repud	X	X		X	X	X	X	X	X	X	X	X			X	X		X	X		
T.INIT_Aut													X								
T.INIT_Data													X								
T.PERS_Aut														X							
T.PERS_Data														X							
A.CGA															X	X					
A.SCA																		X			
A.INIT_Process																				X	
A.PERS_Process																					X
P.CSP_Qcert					X										X						
P.Qsign											X	X			X			X			
P.Sigy_SSCD			X						X		X										

8.2.2 Security Objectives Sufficiency

8.2.2.1 Policies and Security Objectives Sufficiency

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

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

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

8.2.2.2 Threats and Security Objectives Sufficiency

T.Hack_Phys (Exploitation of physical vulnerabilities) deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. Physical attacks through the TOE interfaces or observation of TOE emanations are countered by OT.EMSEC_Design. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tamper attacks.

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

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

T.DTBS_Forgery (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which than does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. In the case a trusted channel by cryptographic means is established the TOE counters this threat by the means of OT.DTBS_Integrity_TOE by verifying the integrity of the DTBS-representation. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.SCA_Data_Intend and OE.Trusted_Environment.

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

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. This threat is in general addressed by OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance) and OT.Lifecycle_Security (Lifecycle security), as follows:

OT.Sig_Secure ensures by means of robust encryption techniques that the signed data and the electronic signature are securely linked together. OE.SCA_Data_Intend provides that the methods used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation is appropriate for the cryptographic methods employed to generate the electronic signature. The combination of OE.CGA_QCert, OT.SCD_SVD_Corresp, OT.SVD_Auth_TOE, and OE.SVD_Auth_CGA provides the integrity and authenticity of the SVD that is used by the signature verification process. OT.Sig_Secure, OT.SCD_Secrecy, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

T.Sig_Repud (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGA_Qcert (Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the

SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signature-creation data), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OE.Trusted_Environment (Trusted Environment for SCA and TOE) and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity).

OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. OE.CGA_QCert and OT.SCD_SVD_Corresp ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OT.SCD_Unique provides that the signatory's SCD can practically occur just once. OT.Sig_Secure, OT.SCD_Transfer, OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD. OT.Sigy_SigF provides that only the signatory may use the TOE for signature generation. OT.Sig_Secure ensures by means of robust cryptographic techniques that valid electronic signatures may only be generated by employing the SCD corresponding to the SVD that is used for signature verification and only for the signed data. OE.SCA_Data_Intend, OE.Trusted_Environment and OT.DTBS_Integrity_TOE ensure that the TOE generates electronic signatures only for DTBS-representations which the signatory has decided to sign as DTBS.

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

T.INIT_Aut (Authentication for initialisation process) covers the circumvention of the authentication of the external world prior to loading EEPROM initialisation data into the TOE. T.INIT_Aut is addressed by OT.INIT_Process which ensures that the initialisation process can be started only after a preceding successful authentication of the external world.

T.INIT_Data (Loading of manipulated initialisation data) deals with the loading of manipulated initialisation data. T.INIT_Data is addressed by OT.INIT_Process which ensures that only integer and authentic EEPROM initialisation data can be loaded into the TOE.

T.PERS_Aut (Authentication for personalisation process) covers the circumvention of the authentication of the external world prior to loading personalisation data into the TOE. T.PERS_Aut is addressed by OT.PERS_Process which ensures that the personalisation process can be started only after a preceding successful authentication of the external world.

T.PERS_Data (Modification or disclosure of personalisation data) deals with the modification and disclosure of personalisation data imported during the personalisation process.

T.PERS_Data is addressed by OT.PERS_Process which ensures for the integrity, authenticity and confidentiality of the data import of the personalisation data.

8.2.2.3 Assumptions and Security Objectives Sufficiency

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

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

A.INIT_Process (Security of the initialisation process) covers the security of the TOE´s initialisation process and is directly adressed by OE.INIT_Process.

A.PERS_Process (Security of the personalisation process) covers the security of the TOE´s personalisation process and is directly adressed by OE.PERS_Process.

8.3 Security Requirements Rationale

According to the requirements of Common Criteria /CC 2.2 Part1/ and /CC 2.2 Part3/, resp. /CC 2.1 Part1/ and /CC 2.1 Part3/, the Security Requirements Rationale demonstrates that the set of security requirements defined for the TOE is suitable to meet the security objectives for the TOE and its environment. In particular, it will be shown that the combination of the individual functional and assurance requirements components for the TOE and its IT environment together meet the specified security objectives and that the set of security requirements together form a mutually supportive and internally consistent whole.

8.3.1 Security Requirements Coverage

Functional Requirements to TOE Security Objectives Mapping

TOE Security Functional Requirements / TOE Security Objectives	OT.EMSEC_Design	OT.Lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper-Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.INIT_Process	OT.PERS_Process
FCS_CKM.1				X	X				X					
FCS_CKM.4		X		X										
FCS_COP.1/CORRESP					X									
FCS_COP.1/SIGNING												X		
FDP_ACC.1/Initialisation SFP			X	X										
FDP_ACC.1/SVD Transfer SFP						X								
FDP_ACC.1/Personalisation SFP											X			
FDP_ACC.1/Signature-Creation SFP										X	X			
FDP_ACC.1/Smartcard Initialisation SFP													X	
FDP_ACC.1/Smartcard Personalisation SFP														X
FDP_ACF.1/Initialisation SFP						X								
FDP_ACF.1/SVD Transfer SFP			X	X										
FDP_ACF.1/Personalisation SFP											X			
FDP_ACF.1/Signature-Creation SFP										X	X			
FDP_ACF.1/Smartcard Initialisation SFP													X	
FDP_ACF.1/Smartcard Personalisation SFP														X
FDP_ETC.1/SVD Transfer						X								
FDP_ITC.1/DTBS										X				
FDP_RIP.1				X							X			
FDP_SDI.2/Persistent				X	X						X	X		
FDP_SDI.2/DTBS										X				
FDP_UIT.1/SVD Transfer						X								
FDP_UIT.1/TOE DTBS										X				
FIA_AFL.1			X								X			
FIA_ATD.1			X								X			
FIA_UAU.1			X								X		X	X
FIA_UID.1			X								X		X	X

FMT_MOF.1				X							X			
FMT_MSA.1/Administrator			X	X										
FMT_MSA.1/Signatory											X			
FMT_MSA.1/Smartcard Initialisation													X	
FMT_MSA.1/Smartcard Personalisation														X
FMT_MSA.2											X			
FMT_MSA.3			X	X							X			
FMT_MSA.3/Smartcard Initialisation													X	
FMT_MTD.1											X			
FMT_SMF.1											X			
FMT_SMR.1				X							X			
FPT_AMT.1		X		X								X		
FPT_EMSEC.1	X													
FPT_FLS.1				X										
FPT_PHP.1							X							
FPT_PHP.3								X						
FPT_TST.1		X										X		
FTP_ITC.1/SVD Transfer						X								
FTP_ITC.1/DTBS Import										X				
FTP_ITC.1/Smartcard Personalisation														X
FTP_TRP.1/TOE											X			

IT Environment Functional Requirements to Environment Security Objectives Mapping

Environment Security Requirements / Environment Security Objectives	**OE.CGA_QCert**	**OE.HI_VAD**	**OE.SCA_Data_Intend**	**OE.SVD_Auth_CGA**	**OE.Trusted_Environment**	**OE.INIT_Process**	**OE.PERS_Process**
FCS_CKM.2/CGA	X						
FCS_CKM.3/CGA	X						
FCS_COP.1/SCA Hash			X				
FDP_UIT.1/SVD Import				X			
FTP_ITC.1/SVD Import				X			
FDP_UIT.1/SCA DTBS			X				
FTP_ITC.1/SCA DTBS			X				
FTP_TRP.1/SCA		X					
R.Sigy_Name	X						
R.Trusted_Environment		X			X		
R.INIT_Process						X	
R.PERS_Process							X

Assurances Requirements to Security Objectives Mapping

Objectives	Requirements
Security Assurance Requirements	
OT.Lifecycle_Security	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ADO_DEL.2, ADO_IGS.1
OT.SCD_Secrecy	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ADO_DEL.2, ADO_IGS.1
OT.Sigy_SigF	AVA_MSU.3, AVA_SOF.1
OT.Sig_Secure	AVA_VLA.4
Security Objectives	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2, ADO_DEL.2, ADO_IGS.1, ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1, AGD_ADM.1, AGD_USR.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2

8.3.2 Security Requirements Sufficiency

8.3.2.1 TOE Security Requirements Sufficiency

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

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

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

OT.SCD_Secrecy (Secrecy of signature-creation data) counters that, with reference to recital (18) of the Directive, storage or copying of SCD causes a threat to the legal validity of electronic signatures. OT.SCD_Secrecy is provided by the security functions specified by FDP_ACC.1/Initialisation SFP and FDP_ACF.1/Initialisation SFP that ensure that only authorised user can initialise the TOE and create or load the SCD. The authentication and access management functions specified by FMT_MOF.1, FMT_MSA.1, FMT_MSA.3 corresponding to the actual TOE (i.e., FMT_MSA.1/Administrator, FMT_MSA.3), and FMT_SMR.1

ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.

The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been used for signature creation and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_AMT.1 and FPT_FLS.1 test the working conditions of the TOE and guarantee a secure state when integrity is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS is differential fault analysis (DFA).

The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation, AVA_SOF HIGH by requesting strength of function high for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

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

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

OT.DTBS_Integrity_TOE (Verification of DTBS-representation integrity) covers that integrity of the DTBS-representation to be signed is to be verified, as well as the DTBS-representation is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms of FDP_ITC.1/DTBS, FTP_ITC.1/DTBS Import, and by FDP_UIT.1/TOE DTBS. The verification that the DTBS-representation has not been altered by the TOE is done by integrity functions specified by FDP_SDI.2/DTBS. The access control requirements of FDP_ACC.1/Signature-Creation SFP and FDP_ACF.1/Signature-Creation SFP keep unauthorised parties off from altering the DTBS-representation.

OT.Sigy_SigF (Signature generation function for the legitimate signatory only) is provided by FIA_UAU.1 and FIA_UID.1 that ensure that no signature generation function can be invoked before the signatory is identified and authenticated.

The security functions specified by FDP_ACC.1/Personalisation SFP, FDP_ACC.1/Signature-Creation SFP, FDP_ACF.1/Personalisation SFP, FDP_ACF.1/Signature-Creation SFP, FMT_MTD.1 and FMT_SMR.1 ensure that the signature process is restricted to the signatory.

The security functions specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, and FMT_MSA.3 and FMT_SMF.1 ensure that the access to the signature generation functions remain under the sole control of the signatory, as well as FMT_MSA.1/Signatory provides that the control of corresponding security attributes is under signatory's control.

The security functions specified by FDP_SDI.2 and FPT_TRP.1/TOE ensure the integrity of stored data both during communication and while stored.

The security functions specified by FDP_RIP.1 and FIA_AFL.1 provide protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.

The assurance measures specified by AVA_MSU.3 by requesting analysis of misuse of the TOE implementation, AVA_SOF.1 by requesting high strength level for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

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

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

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

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

OT.INIT_Process (Security of the initialisation process) guarantees for a secure initialisation process and is provided by the security functions specified by FDP_ACC.1/Smartcard Initialisation SFP, FDP_ACF.1/Smartcard Initialisation SFP, FIA_UID.1 and FIA_UAU.1 which ensure that only authorised users can load the EEPROM initialisation data and that only EEPROM initialisation data of integrity and authenticity can be loaded into the TOE. The security functions specified by FMT_MSA.1/Smartcard Initialisation and FMT_MSA.3/Smartcard Initialisation provide the secure handling of the security attributes related to the initialisation process.

OT.PERS_Process (Security of the personalisation process) guarantees for a secure personalisation process and is provided by the security functions specified by FDP_ACC.1/Smartcard Personalisation SFP, FDP_ACF.1/Smartcard Personalisation SFP, FIA_UID.1, FIA_UAU.1 and FTP_ITC.1/Smartcard Personalisation which ensure that only authorised users can load the personalisation data and that the personalisation process is secured for integrity, authenticity and confidentiality. The security function specified by FMT_MSA.1/Smartcard Personalisation provides the secure handling of the security attributes related to the personalisation process.

8.3.2.2 TOE Environment Security Requirements Sufficiency

OE.CGA_QCert (Generation of qualified certificates) addresses the requirement of qualified certificates. The functions specified by FCS_CKM.2/CGA provide the cryptographic key distribution method. The functions specified by FCS_CKM.3/CGA ensure that the CGA imports the SVD using a secure channel and a secure key access method.

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

OE.SCA_Data_Intend (Data intended to be signed) is provided by the functions specified by FTP_ITC.1/SCA DTBS and FDP_UIT.1/SCA DTBS that ensure that the DTBS can be checked by the TOE, and FCS_COP.1/SCA Hash that provides that the hashing function corresponds to the approved algorithms.

OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) is provided by FTP_ITC.1/SVD.IMPORT which assures identification of the sender and by FDP_UIT.1/ SVD Import which guarantees its integrity.

OE.Trusted_Environment (Trusted Environment for SCA and TOE) is provided by R.Trusted_Environment which serves in the case that a trusted channel resp. trusted path between the TOE and the SCA by cryptographic means is not established that the environment for the TOE usage is secured with the target to keep confidentiality and integrity of the VAD and integrity of the DTBS within the data transfer to the TOE.

OE.INIT_Process (Security of the initialisation process) is directly provided by R.INIT_Process which serves for a secure initialisation process.

OE.PERS_Process (Security of the personalisation process) is directly provided by R.PERS_Process which serves for a secure personalisation process.

8.4 Dependency Rationale

8.4.1 Functional and Assurance Requirements Dependencies

The functional and assurance requirements dependencies for the TOE are completely fulfilled. The functional requirements dependencies for the TOE environment are not completely fulfilled (see section 8.4.2 for justification).

Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FCS_CKM.1	FCS_COP.1/SIGNING, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2
FCS_COP.1/CORRESP	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/SIGNING	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1/Initialisation SFP	FDP_ACF.1/Initialisation SFP
FDP_ACC.1/SVD Transfer SFP	FDP_ACF.1/SVD Transfer SFP
FDP_ACC.1/Personalisation SFP	FDP_ACF.1/Personalisation SFP
FDP_ACC.1/Signature-Creation SFP	FDP_ACF.1/Signature-Creation SFP
FDP_ACC.1/Smartcard Initialisation SFP	FDP_ACF.1/Smartcard Initialisation SFP
FDP_ACC.1/Smartcard Personalisation SFP	FDP_ACF.1/Smartcard Personalisation SFP
FDP_ACF.1/Initialisation SFP	FDP_ACC.1/Initialisation SFP, FMT_MSA.3
FDP_ACF.1/SVD Transfer SFP	FDP_ACC.1/Personalisation SFP, FMT_MSA.3
FDP_ACF.1/Personalisation SFP	FDP_ACC.1/SVD Transfer SFP, FMT_MSA.3
FDP_ACF.1/Signature-Creation SFP	FDP_ACC.1/Signature-Creation SFP, FMT_MSA.3
FDP_ACF.1/Smartcard Initialisation SFP	FDP_ACC.1/Smartcard Initialisation SFP, FMT_MSA.3/Smartcard Initialisation
FDP_ACF.1/Smartcard Personalisation SFP	FDP_ACC.1/Smartcard Personalisation SFP, FMT_MSA.3 not applicable (unsupported dependency, see subsection 8.4.2 for justification)
FDP_ETC.1/SVD Transfer	FDP_ACC.1/SVD Transfer SFP
FDP_ITC.1/DTBS	FDP_ACC.1/Signature-Creation SFP, FMT_MSA.3
FDP_RIP.1	---
FDP_SDI.2/Persistent	---
FDP_SDI.2/DTBS	---
FDP_UIT.1/SVD Transfer	FTP_ITC.1/SVD Transfer, FDP_ACC.1/SVD Transfer SFP
FDP_UIT.1/TOE DTBS	FDP_ACC.1/Signature-Creation SFP, FTP_ITC.1/DTBS Import
FIA_AFL.1	FIA_UAU.1
FIA_ATD.1	---
FIA_UAU.1	FIA_UID.1
FIA_UID.1	---
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/Administrator	FDP_ACC.1/Initialisation SFP, FMT_SMR.1

FMT_MSA.1/Signatory	FDP_ACC.1/Signature-Creation SFP, FMT_SMR.1
FMT_MSA.1/Smartcard Initialisation	FDP_ACC.1/Smartcard Initialisation SFP, FMT_SMR.1
FMT_MSA.1/Smartcard Personalisation	FDP_ACC.1/Smartcard Personalisation SFP, FMT_SMR.1
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1/Personalisation SFP, FDP_ACC.1/Smartcard Initialisation SFP, FDP_ACC.1/Smartcard Personalisation SFP, FMT_SMR.1, FMT_MSA.1/Administrator, FMT_MSA.1/Signatory, FMT_MSA.1/Smartcard Initialisation, FMT_MSA.1/Smartcard Personalisation
FMT_MSA.3	FMT_MSA.1/Administrator, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.3/Smartcard Initialisation	FMT_MSA.1/Smartcard Initialisation, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1
FMT_SMF.1	---
FMT_SMR.1	FIA_UID.1
FPT_AMT.1	---
FPT_EMSEC.1	---
FPT_FLS.1	ADV_SPM.1
FPT_PHP.1	FMT_MOF.1
FPT_PHP.3	---
FPT_TST.1	FPT_AMT.1
FTP_ITC.1/SVD Transfer	---
FTP_ITC.1/DTBS Import	---
FTP_ITC.1/Smartcard Personalisation	---
FTP_TRP.1/TOE	---
Assurance Requirements	
ACM_AUT.1	ACM_CAP.3
ACM_CAP.4	ACM_SCP.1, ALC_DVS.1
ACM_SCP.2	ACM_CAP.3
ADO_DEL.2	ACM_CAP.3
ADO_IGS.1	AGD_ADM.1
ADV_FSP.2	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1, ADV_RCR.1
ADV_IMP.1	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1
ADV_LLD.1	ADV_HLD.2, ADV_RCR.1
ADV_RCR.1	---
ADV_SPM.1	ADV_FSP.1
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ALC_DVS.1	---
ALC_LCD.1	---
ALC_TAT.1	ADV_IMP.1
ATE_COV.2	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	ADV_HLD.1, ATE_FUN.1
ATE_FUN.1	---
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.3	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.4	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1

Functional Requirements for Certification Generation Application (CGA)	
FCS_CKM.2/CGA	unsupported dependencies, see subsection 8.4.2 for justification
FCS_CKM.3/CGA	unsupported dependencies, see subsection 8.4.2 for justification
FDP_UIT.1/SVD Import	FTP_ITC.1/SVD IMPORT, unsupported dependencies, see subsection 8.4.2 for justification
FTP_ITC.1/SVD Import	None
Functional Requirements for Signature-Creation Application (SCA)	
FCS_COP.1/SCA Hash	unsupported dependencies, see subsection 8.4.2 for justification
FDP_UIT.1/SCA DTBS	FTP_ITC.1/SCA DTBS, unsupported dependencies on FDP_ACC.1, see subsection 8.4.2 for justification
FTP_ITC.1/SCA DTBS	None
FTP_TRP.1/SCA	None

8.4.2 Justification of Unsupported Dependencies

The security functional dependencies for the TOE itself are not completely supported by security functional requirements in section 5.2.1.

Functional Requirement	Justification
FDP_ACF.1/Smartcard Personalisation SFP	FMT_MSA.3 is not applicable in the framework of FDP_ACF.1/Smartcard Personalisation SFP as no initialisation of the attribute “Chip State” is possible during the TOE´s personalisation phase.

The security functional dependencies for the TOE environment CGA and SCA are not completely supported by security functional requirements in section 5.2.1.

Functional Requirement	Justification
FCS_CKM.2/CGA	The CGA generates qualified electronic signatures including the SVD imported from the TOE. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this ST.
FCS_CKM.3/CGA	The CGA imports SVD via trusted channel implemented by FTP_ITC.1/SVD import. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security

	management for the CGA by FMT_MSA.2 is outside of the scope of this ST.
FDP_UIT.1/SVD Import (CGA)	The access control (FDP_ACC.1) for the CGA is outside the scope of this ST.
FCS_COP.1/SCA Hash	The hash algorithm implemented by FCS_COP.1/SCA Hash does not require any key or security management. Therefore FDP_ITC.1, FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2 are not required for FCS_COP.1/SCA Hash in the SCA.
FDP_UIT.1/SCA DTBS	Access control (FDP_ACC.1.1) for the SCA are outside of the scope of this ST.

8.5 Security Requirements Grounding in Objectives

This chapter covers the grounding that have not been done in the precedent chapter.

Assurance Requirements to Security Objectives Mapping

Requirement	Security Objectives
Security Assurance Requirements	
ACM_AUT.1	EAL 4
ACM_CAP.4	EAL 4
ACM_SCP.2	EAL 4
ADO_DEL.2	EAL 4
ADO_IGS.1	EAL 4
ADV_FSP.2	EAL 4
ADV_HLD.2	EAL 4
ADV_IMP.1	EAL 4
ADV_LLD.1	EAL 4
ADV_RCR.1	EAL 4
ADV_SPM.1	EAL 4
AGD_ADM.1	EAL 4
AGD_USR.1	EAL 4
ALC_DVS.1	EAL 4, OT.Lifecycle_Security
ALC_LCD.1	EAL 4, OT.Lifecycle_Security
ALC_TAT.1	EAL 4, OT.Lifecycle_Security
ATE_COV.2	EAL 4
ATE_DPT.1	EAL 4
ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_MSU.3	OT.Sigy_SigF
AVA_SOF.1	EAL 4, OT.SCD_Secrecy, OT.Sigy_SigF
AVA_VLA.4	OT.SCD_Secrecy, OT.Sig_Secure
Security Objectives for the Environment	
R.Administrator_Guide	AGD_ADM.1
R.Sigy_Guide	AGD_USR.1
R.Sigy_Name	OE.CGA_QCert
R.Trusted_Environment	AGD_USR.1
R.INIT_Process	AGD_ADM.1
R.PERS_Process	AGD_ADM.1

8.6 Rationale for Extensions

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. 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. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations.

8.6.1 FPT_EMSEC TOE Emanation

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC.1 TOE Emanation has two constituents:

- FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMSEC.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

FPT_EMSEC.1 TOE Emanation

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 other components.

8.7 TOE Summary Specification Rationale

According to the requirements of Common Criteria /CC 2.2 Part1/ and /CC 2.2 Part3/, resp. /CC 2.1 Part1/ and /CC 2.1 Part3/, the TOE summary specification rationale demonstrates that the TOE security functions (TSFs) and assurance measures are suitable to meet the TOE security requirements. In particular, it will be demonstrated that the combination of the specified TOE´s IT security functions work together in such a manner that they satisfy the TOE security functional requirements.

8.7.1 TOE Security Functions Rationale

Security Functional Requirements / TOE Security Functions	F.ACS_SIG	F.ADMIN_SIG	F.PIN_SIG	F.DATA_INT	F.SEC_EXCH	F.RIP	F.FAIL_PROT	F.SIDE_CHAN	F.SELFTEST	F.CRYPTO	F.RSA_KEYGEN	F.GEN_SIG	TSFs of IC+ACL
FCS_CKM.1		X						X		(X)	X		(X)
FCS_CKM.4						X					X		
FCS_COP.1/CORRESP								X		(X)		X	(X)
FCS_COP.1/SIGNING								X		(X)		X	(X)
FDP_ACC.1/Initialisation SFP	X	X	X		X								
FDP_ACC.1/SVD Transfer SFP	X	X	X		X								
FDP_ACC.1/Personalisation SFP	X	X			X								
FDP_ACC.1/Signature-Creation SFP	X		X		X								
FDP_ACC.1/Smartcard Initialisation SFP		X											
FDP_ACC.1/Smartcard Personalisation SFP		X			X								
FDP_ACF.1/Initialisation SFP	X	X	X		X								
FDP_ACF.1/SVD Transfer SFP	X	X	X		X								
FDP_ACF.1/Personalisation SFP	X	X			X								
FDP_ACF.1/Signature-Creation SFP	X		X		X								
FDP_ACF.1/Smartcard Initialisation SFP		X											
FDP_ACF.1/Smartcard Personalisation SFP		X			X								
FDP_ETC.1/SVD Transfer		X											
FDP_ITC.1/DTBS												X	
FDP_RIP.1						X							
FDP_SDI.2/Persistent				X									
FDP_SDI.2/DTBS				X									
FDP_UIT.1/SVD Transfer					X					(X)			(X)
FDP_UIT.1/TOE DTBS					X					(X)			(X)
FIA_AFL.1			X										
FIA_ATD.1	X												
FIA_UAU.1	X		X										
FIA_UID.1	X		X										
FMT_MOF.1	X		X										
FMT_MSA.1/Administrator	X	X											
FMT_MSA.1/Signatory	X		X										
FMT_MSA.1/Smartcard Initialisation		X											
FMT_MSA.1/Smartcard Personalisation		X											
FMT_MSA.2	X	X											

FMT_MSA.3		X											
FMT_MSA.3/Smartcard Initialisation		X											
FMT_MTD.1	X		X										
FMT_SMF.1	X	X	X										
FMT_SMR.1	X												
FPT_AMT.1									X				
FPT_EMSEC.1								X					(X)
FPT_FLS.1							X	X					
FPT_PHP.1													X
FPT_PHP.3													X
FPT_TST.1									X				
FTP_ITC.1/SVD Transfer					X					(X)			(X)
FTP_ITC.1/DTBS Import			X		X					(X)			(X)
FTP_ITC.1/Smartcard Personalisation		X			X					(X)			(X)
FTP_TRP.1/TOE			X		X					(X)			(X)

Note:

X directly contributing TSF

(X) supporting TSF

The detailed description and analysis of the TOE Security Functions in chap. 6.1 demonstrate how the defined functions work together and support each other. Furthermore, this description shows that no inconsistencies exist.

The deliberations above support this result. Additionally, for the TSFs of the underlying IC and ACL as defined in /ST IC+ACL/ such analysis is done in the scope of the CC evaluation of the IC and ACL resp. within the correlated ST.

The rationale here is presented in form of tables. The full rationale as given in the TOE´s Security Target is not intended to be published and hence not part of the ST-Lite.

8.7.2 Assurance Measures Rationale

The assurance measures of the developer as mentioned in chap. 6.3 are considered as being suitable and sufficient to meet the CC assurance level EAL4 augmented by AVA_MSU.3 and AVA_VLA.4 as claimed in chap. 5.1.3. Especially the deliverables listed in chap. 6.3 are seen as being suitable and sufficient to prove the fulfillment of the assurance requirements in detail.

As the development and production process of the TOE is very complex and a great number of assurance measures are implemented by the developer, a detailed description of these measures beyond the information given in chap. 2.2 as well as a detailed mapping of the assurance measures to the assurance requirements is not in the scope of this ST.

8.8 Rationale for Strength of Function High

The TOE shall demonstrate to be highly resistant against penetration attacks in order to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. The protection against attacks with a high attack potential dictates a strength of function high rating for functions in the TOE that are realised by probabilistic or permutational mechanisms.

8.9 Rationale for Assurance Level 4 Augmented

The assurance level for this protection profile is EAL4 augmented.EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this protection profile is just such a product. Augmentation results from the selection of:

AVA_MSU.3	Vulnerability Assessment - Misuse - Analysis and testing for insecure states
AVA_VLA.4	Vulnerability Assessment - Vulnerability Analysis – Highly resistant

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

In **AVA_MSU.3**, an analysis of the guidance documentation by the developer is required to provide additional assurance that the objective has been met, and this analysis is validated and confirmed through testing by the evaluator. AVA_MSU.3 has the following dependencies:

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

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

AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. AVA_VLA.4 has the following dependencies:

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

AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

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

8.10 Rationale for PP Claims

Not applicable.

Reference

I Bibliography

/CC 2.1 Part1/
Title: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model
Identification: CCIMB-99-031
Version: Version 2.1
Date: August 1999
Author: CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CC 2.1 Part2/
Title: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements
Identification: CCIMB-99-032
Version: Version 2.1
Date: August 1999
Author: CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CC 2.1 Part3/
Title: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements
Identification: CCIMB-99-032
Version: Version 2.1
Date: August 1999
Author: CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CEM 0.6 Part1/
Title: Common Methodology for Information Technology Security Evaluation, Part 1: Introduction and General Model
Identification: CEM-97/017
Version: Draft 0.6
Date: Jan. 1997
Author: CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CEM 1.0 Part2/
Title: Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology
Identification: CEM99/045
Version: V1.0
Date: Aug. 1999
Author: CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CC 2.2 Part1/
Title: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model
Identification: CCIMB-2004-01-001
Version: Version 2.2 Revision 256
Date: January 2004
Author: CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CC 2.2 Part2/
Title: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements
Identification: CCIMB-2004-01-002
Version: Version 2.2 Revision 256
Date: January 2004
Author: CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CC 2.2 Part3/
Title: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements
Identification: CCIMB-2004-01-003
Version: Version 2.2 Revision 256
Date: January 2004
Author: CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/CEM 2.2 Part2/
Title: Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology
Identification: CCIMB-2004-01-004
Version: Version 2.2 Revision 256
Date: January 2004
Author: CC Project Sponsoring Organisations CSE, SCSSI, BSI, NLNCSA, CESG, NIST, NSA

/AIS32/
Title: Übernahme international abgestimmter CC Interpretationen
Identification: AIS 32
Date: 02.07.2001
Publisher: Bundesamt für Sicherheit in der Informationstechnik

/BSI-PP-0002/
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

/PP SSCD Type 3/
Title: Protection Profile – Secure Signature-Creation Device Type 3 “EAL 4+”
Identification: BSI-PP-0006-2002
Version: Version 1.05
Date: July 25th 2001
Publisher: CEN/ISSS – Information Society Standardization System, Workshop on Electronic Signatures

/DS IC/
Title: Renesas 32-bit Smart Card Microcomputer AE-5 Series – Hardware Manual AE55C1 (HD65255C1)
Version: Rev. 1.00
Date: March 15th 2005
Publisher: Renesas Technology Corp.

/UG IC/
Title: Renesas 32-bit Smart Card Microcomputer AE-5 Series – User Guidance Manual
Version: Rev. 4.40
Date: Jan. 27th 2006
Publisher: Renesas Technology Corp.

/UG ACL/
Title: Renesas 32-bit Smart Card Microcomputer AE-5 Series – Cryptographic Library Version 1.43 – User´s Manual
Version: Rev. 1.70
Date: Jan. 27th 2006
Publisher: Renesas Technology Corp.

/ST IC+ACL/
Title: AE55C1 (HD65255C1) Version 02 with ACL Version 1.43 - Smartcard Security Target (Public Version)
Identification: ST for Certification ID BSI-DSZ-CC-0329
Version: Revision 4.0
Date: Jan. 30th 2006
Publisher: Renesas Technology Corp.

/ETRLite IC+ACL/
Title: BSI-DSZ-CC-0329: ETR-lite for composition according to AIS 36
Version: V1.0
Date: March 22th 2006
Publisher: T-Systems GEI GmbH

/ConfListRenesas/
Title: AE55C1F06UD (HWD65255C1F06UD) – Configuration List
Version: Revision 3.0
Date: Feb. 20th 2006
Publisher: Renesas Technology Corp.

/ISO 7816-2/
Title: Identification Cards - Integrated circuit(s) cards with contacts - Part 2: Dimension and location of contacts
Identification: ISO/IEC 7816-2
Version: First edition
Date: 1999-03-01
Publisher: International Organization for Standardization / International Electrotechnical Commission

/ISO 7816-3/
Title: Identification Cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission
Identification: ISO/IEC 7816-3
Version: CD2
Date: 2004-02-17
Publisher: International Organization for Standardization / International Electrotechnical Commission

/ISO 7816-4/
Title: Identification Cards - Integrated circuit(s) cards with contacts. Part 4: Interindustry commands for interchange
Identification: ISO/IEC 7816-4
Version: FDIS
Date: 2004-06-27
Publisher: International Organization for Standardization / International Electrotechnical Commission

/ISO 7816-8/
Title: Identification Cards - Integrated circuit(s) cards with contacts. Part 8: Command for security operations
Identification: ISO/IEC 7816-8
Version: IS, Second edition
Date: 2004
Publisher: International Organization for Standardization / International Electrotechnical Commission

/ISO 7816-9/
Title: Identification Cards - Integrated circuit(s) cards with contacts. Part 9: Additional interindustry commands and security attributes
Identification: ISO/IEC 7816-9

Version: FDIS
Date: 2004
Publisher: International Organization for Standardization / International Electrotechnical Commission

/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
Date: 2002
Publisher: International Organization for Standardization / International Electrotechnical Commission

/ISO 11770-3/
Title: Information Technology – Security Techniques – Key Management – Part 3: Mechanisms Using Asymmetric Techniques
Identification: ISO/IEC 11770-3
Date: 1996
Publisher: International Organization for Standardization / International Electrotechnical Commission

/ISO 10118-3/
Title: Information Technology – Security Techniques – Hash Functions – Part 3: Dedicated hash functions
Identification: ISO/IEC 10118-3
Date: 2004
Publisher: International Organization for Standardization / International Electrotechnical Commission

/FIPS 180-2/
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)

/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)

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

/SECCOS/
Title: Schnittstellenspezifikation für die ZKA-Chipkarte – Secure Chip Card Operating System (SECCOS) (mit Errata vom 13.06.2001)
Version: Version 5.0
Date: 05.06.2001
Publisher: Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH, Bundesverband Öffentlicher Banken-ZVD GmbH

/SECCOS Sig/
Title: Schnittstellenspezifikation für die ZKA-Chipkarte, Signatur-Anwendung
Version: Version 5.1
Date: 28.04.2004
Publisher: Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH, Bundesverband Öffentlicher Banken-ZVD GmbH

/SECCOS EMV/
Title: Schnittstellenspezifikation für die ZKA-Chipkarte, EMV-Kommandos
Version: Version 1.0
Date: 19.11.2001
Publisher: Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH, Bundesverband Öffentlicher Banken-ZVD GmbH

/SECCOS EC/
Title: Schnittstellenspezifikation für die ZKA-Chipkarte, electronic cash, Applikation electronic cash
Version: Version 5.0
Date: 01.10.2003
Publisher: Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH, Bundesverband Öffentlicher Banken-ZVD GmbH

/SECCOS GK/
Title: Schnittstellenspezifikation für die ZKA-Chipkarte, GeldKarte, Applikation elektronische Geldbörse
Version: Version 5.0
Date: 01.10.2003
Publisher: Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH, Bundesverband Öffentlicher Banken-ZVD GmbH

/SECCOS Perso/
Title: Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS
Version: Version 1.3
Date: 29.12.2004
Publisher: Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH, Bundesverband Öffentlicher Banken-ZVD GmbH

/SECCOS Perso Sig/
Title: Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS, Anhang - Signaturkarte
Version: Version 1.1
Date: 08.05.2003
Publisher: Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH, Bundesverband Öffentlicher Banken-ZVD GmbH

/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 Nr. 59, S. 4695-4696
Date: 30.03.2005
Publisher: RegTP

/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: Amtblatt der Europäischen Gemeinschaften, L13/12-L13/20
Date: 19.01.2001
Publisher: Europäisches Parlament und Rat der Europäischen Union

/DIN 66291-1/
Title: Chipkarten mit Digitaler Signatur-Anwendung / Funktion nach SigG/SigV - Teil 1: Anwendungsschnittstelle
Identification: DIN V66291-1
Date: 2000
Publisher: DIN

/DIN 66291-4/
Title: Chipcards with digital signature application/function according to SigG and SigV - Part 4: Basic Security Services
Identification: DIN V66291-4
Date: 2000
Publisher: DIN

II Summary of abbreviations

A.x	Assumption
AC	Access Condition
ACL	Advanced Cryptographic Library
ALW	Always
AM	Access Mode
AR	Access Rule
ATR	Answer To Reset
AUT	Key Based Authentication
BS	Basic Software
CC	Common Criteria
CGA	Certification Generation Application
CH	Cardholder
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
EC	Electronic Cash
EF	Elementary File
EMV	Europay, MasterCard, Visa
ES	Embedded Software
GK	GeldKarte
IC	Integrated Circuit
IFD	Interface Device
MAC	Message Authentication Code
MF	Master File
O.x	Security Objective
OS	Operating System
P.x	Organisational Security Policy
PIN	Personal Identification Number
PP	Protection Profile
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
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-0002/, Chap. 8.7

/ST IC+ACL/, Glossary

/PP SSCD Type 3/, Terminology

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 „ZKA SECCOS Sig v1.5.2“ 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_SIG (Zugriffskontrolle) und F.PIN_SIG (Prozesse der PIN-basierten Authentisierung). Ein Export des Signaturschlüssels über die regulären Betriebssystem-Kommandos ist aufgrund der gesetzten Zugriffsregeln ebenfalls nicht möglich (TSF F.ACS_SIG). Die Generierung des Signaturschlüsselpaares der Signaturapplikation der sicheren Signaturerstellungseinheit „ZKA SECCOS Sig v1.5.2“ 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 Initialisierung / 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_SIG). Die Sicherheit des Prozesses der Signaturerzeugung, insbesondere bzgl. der Gewinnung von Informationen über den benutzten Signaturschlüssel, wird über TSF F.GEN_SIG, 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	/SigG01/, §17 „Produkte für qualifizierte elektronische Signaturen“,	Siehe Erklärungen zu Tabellenzeile 1.

	und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen, ...	(3), Satz 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 „ZKA SECCOS Sig v1.5.2“ ist ausschließlich nur 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_SIG (Zugriffskontrolle) und F.PIN_SIG (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_SIG). Die Generierung des Signaturschlüsselpaares der Signaturapplikation der sicheren Signaturerstellungseinheit „ZKA SECCOS Sig v1.5.2“ 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 Initialisierung / 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_SIG). Die Sicherheit des Prozesses der Signaturerzeugung, insbesondere bzgl. der Gewinnung von Informationen über den benutzten Signaturschlüssel, wird über TSF F.GEN_SIG, 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 „ZKA SECCOS Sig v1.5.2“ beinhaltet geeignete Sicherungsmechanismen, die einen sicheren Betriebszustand des Produktes garantieren und dem Nutzer (direkt oder indirekt, je nach Fehlerfall) Information hierüber geben. Die Si-

			cherungsmechanismen werden in TSF F.FAIL_PROT, F.SELFTEST und F.SIDE_CHAN realisiert.
5	Restriktionen zur PIN-/PUK-Funktionalität	---	Die Signaturapplikation der sicheren Signaturerstellungseinheit „ZKA SECCOS Sig v1.5.2“ sieht folgende Restriktionen für die dem Signaturschlüssel zugeordnete Signatur-PIN 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) - Keine Verwendung von PUKs (Resetting Codes)
6	Restriktionen zur Nutzung der Display-Message	---	Die Signaturapplikation der sicheren Signaturerstellungseinheit „ZKA SECCOS Sig v1.5.2“ verwendet kein Datenfeld für die Display-Message.
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 „ZKA SECCOS Sig v1.5.2“ unterliegt einer Evaluierung und Zertifizierung nach dem Standard Common Criteria Version 2.2 mit dem Evaluierungslevel EAL 4+ (mit den Augmentierungen 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 „ZKA SECCOS Sig v1.5.2“ unterliegt einer Evaluierung und Zertifizierung nach dem Standard Common Criteria Version 2.2 mit dem Evaluierungslevel EAL 4+ (mit den Augmentierungen 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 „ZKA SECCOS Sig v1.5.2“ berücksichtigt für die Signaturerzeugung, Hashwert-Berechnung, Zufallszahlengenerierung und Schlüsselgenerierung Algorithmen und Parameter, die dem aktuellen Algorithmenkatalog /ALGCAT/ entsprechen. Vergleiche hierzu die TSFs F.GEN_SIG, F.RSA_KEYGEN und F.CRYPTO.