Security Target STARCOS 3.2 QES V2.0B

Version 1.0/Status 08.01.2009

F&E

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

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

Contents

1 Introduction

1.1 ST Identification

Title: Security Target STARCOS 3.2 QES V2.0B

Version Number/Date: Version 1.0/Status 08.01.2009

Origin: Giesecke & Devrient GmbH

TOE: STARCOS 3.2 QES V2.0B

TOE documentation:

- User Manual STARCOS 3.2 QES V2
- Installation, generation and start-up STARCOS 3.2 HBA, STARCOS 3.2 QES V2
- Administrator Guidance STARCOS 3.2 HBA, STARCOS 3.2 QES V2
  - Generic Application STARCOS 3.2 QES V2
  - Smart Card Application Verifier STARCOS 3.2 QES V2.0B

HW-Part of TOE: Infineon SLE66CX680PE/m1534a13 (Certificate: BSI-DSZ-CC-0322-2005, Assurance Continuity Maintenance Report BSI-DSZ-CC-0322-2005-MA-04)

1.2 ST Overview

The aim of this document is to describe the Security Target for the 'STARCOS 3.2 QES V2.0B'.

The related product is the STARCOS 3.2 Operating System (OS) on a Smart Card Integrated Circuit. It is intended to be used as Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC [1], so the TOE consists of the part of the implemented software related to the generation of qualified electronic signatures in combination with the underlying hardware ('Composite Evaluation'). The functional and assurance requirements for SSCDs defined in Annex III of this EU Directive [1] have been mapped into three Protection Profiles (PPs) for different types of SSCDs (see chap. 2.1.1 for details). The Security Target for the 'STARCOS 3.2 QES V2.0B' is compliant to the PP for SSCDs of Type 3 (generation of SCD/SVD pair, storage of Signature Creation Data and Signature Creation Component) [7].

STARCOS 3.2 is a fully interoperable ISO 7816 compliant multiapplication Smart Card OS, including a cryptographic library enabling the user to generate high security RSA signatures up to 2048 Bit. The EU compliant Electronic Signature Application is designed for the creation of legally

binding Qualified Electronic Signatures as defined in the EU Directive [1]. The various features of STARCOS 3.2 allow for additional applications like banking, ticketing or health care.

The software part of the TOE is implemented on the Infineon SLE66CX680PE, which is certified according to CC EAL5+ [15]. So the TOE consists of the software part and the underlying hardware. The RSA2048 crypto library provided with the underlying hardware is not used in this composite TOE, but the software part of the RSA calculations is implemented in the operating system. The corresponding Security Target (Lite) [8] is compliant to the BSI-PP-0002-2001 [9].

This document describes

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

The assurance level for the TOE is CC **EAL4+**.

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

1.3 CC Conformance

This ST is in accordance with Common Criteria V2.3 (ISO/IEC 15408:2005) (see [2], [3], [4]).

This ST is compliant with CC V2.3 Part 2 [3], extended by an additional functional component as stated in [7].

This ST is compliant with CC V2.3 Part 3 [4], level **EAL4** augmented by

- AVA_MSU.3 (Analysis and testing for insecure states)
- AVA_VLA.4 (Highly resistant)

as stated in [7].

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

1.4 PP Compliance

This Security Target is compliant to “Secure Signature-Creation Device Protection Profile Type 3”, v1.05 EAL4+, BSI-PP-0006-2002, 25 July 2001 [7].

1.5 Sections Overview

Section 1 provides the introductory material for the Security Target.

Section 2 provides general purpose and TOE description.

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

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

Section 5 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [3] and Part 3 [4], that must be satisfied.

Section 6 contains the TOE Summary Specification.

Section 7 provides the PP compliance claims.

Section 8 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next section 8 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the security target requirements

Section 9 provides information on applied conventions and used terminology.

Section 10 identifies background material (reference section).

Section 11 provides definitions of frequently used acronyms.

2 TOE Description

2.1 Product Type

2.1.1 Secure Signature Creation Devices

(This description is taken from the SSCD Protection Profile [7] and should be used as general introduction to SSCDs.)

The present document assumes a well defined process signature-creation to take place. The present chapter defines three possible SSCD implementations, referred to as 'SSCD types', as illustrated in Figure 1.

The left part of Figure 1 shows two SSCD components: A SSCD of Type 1 representing the SCD/SVD generation component, and a SSCD of Type 2 representing the SCD storage and signature-creation component. The SCD generated on a SSCD Type 1 shall be exported to a SSCD Type 2 over a trusted channel. The right part of Figure 1 shows a SSCD Type 3 which is analogous to a combination of Type 1 and Type 2, but no transfer of the SCD between two devices is provided.

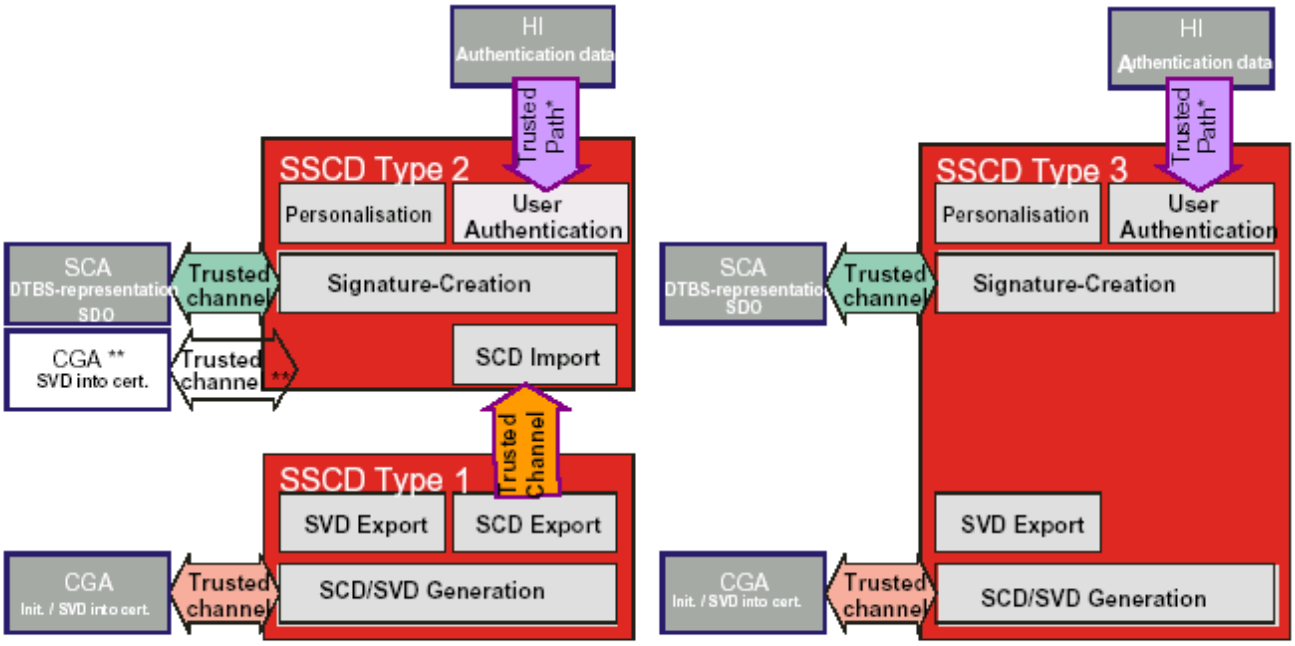
If the SSCD holds the SVD and exports the SVD to a CGA for certification, a trusted channel is to be provided. The CGA initiates SCD/SVD generation ("Init.") and the SSCD exports the SVD for generation of the corresponding certificate ("SVD into cert.").

The signatory must be authenticated to create signatures that he sends his authentication data (e.g., a PIN) to the SSCD Type 2 or Type 3 (e.g., a smart card). If the human interface (HI) for such signatory authentication is not provided by the SSCD, a trusted path (e.g., a encrypted channel) between the SSCD and the SCA implementing to HI is to be provided. The data to be signed (DTBS) representation (i.e., the DTBS itself, a hash value of the DTBS, or a pre-hashed value of the DTBS) shall be transferred by the SCA to the SSCD only over a trusted channel. The same shall apply to the signed data object (SDO) returned from a SSCD to the SCA.

SSCD Type 1 is not a personalized component in the sense that it may be used by a specific user only, but the SCD/SVD generation and export shall be initiated by authorized persons only (e.g., system administrator).

SSCD Type 2 and Type 3 are personalized components which means that they can be used for signature creation by one specific user – the signatory -only.

Type 2 and Type 3 are not necessarily to be considered mutually exclusive.



* The trusted path for user authentication will be required if the HI is not provided by the TOE itself (e. g., it is provided by a SCA outside the SSCD)
** The trusted channel between the SSCD Type 2 and the CGA is required for cases where the SSCD type 2 holds the SVD and export of the SVD to the CGA for certification is provided.

Figure 1: SSCD types and modes of operation

2.1.2 Intended use of the TOE

The TOE is implemented as a Smart Card on an IC and is intended to be used as Secure Signature Creation Device. This includes the Generation and Secure Storage of multiple SCD/SVD pairs and the generation of Qualified Electronic Signatures up to a length of 2048 Bit. Before one of these SCD/SVD pairs is re-generated, the previous content is destructed. Generation of SCDs by the Card Holder in the usage phase is possible.

Beside this the use of multiple separated additional applications like banking, ticketing and health care is possible. Therefore the TOE provides ISO 7816 compliant commands for the different kinds of applications. Due to security reasons the commands provided by the TOE can not be altered or extended, therefore all applications can only be realised with the existing commands.

2.2 Limits of the TOE

2.2.1 Structural view of the TOE

The TOE is a secure signature-creation device (SSCD Type3) according to Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1].

The TOE is realised by a smartcard, consisting of the embedded software residing on the underlying certified IC.

The TOE comprises

- the certified chip,
- the operating system STARCOS 3.2,
- the documentation
  - User Manual STARCOS 3.2 QES V2
  - Installation, generation and start-up STARCOS 3.2 HBA, STARCOS 3.2 QES V2
  - Administrator Guidance STARCOS 3.2 HBA, STARCOS 3.2 QES V2
  - Generic Application STARCOS 3.2 QES V2
- and the Smart Card Application Verifier STARCOS 3.2 QES V2.0B[1].

The operating system STARCOS 3.2 is implemented in the ROM area of the IC, whereas some parts may also reside in the EEPROM. The file system containing the application data is installed in the EEPROM of the IC. Beside the files for the digital signature application there may be additional files for other applications, e.g. for the German health system, which do not belong to the TOE.

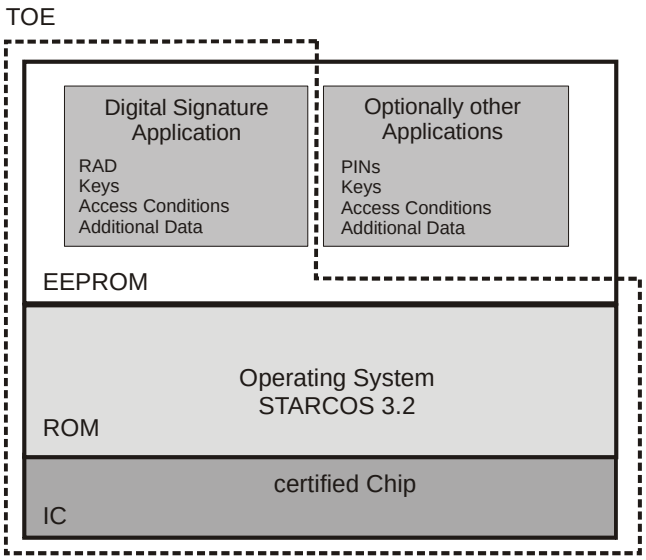


Figure 2: TOE description

[1] The Smart Card Application Verifier STARCOS 3.2 QES V2.0B is not part of the TOE delivery. It is solely used by G&D to verify that the signature application conforms to the requirements of “Generic Application STARCOS 3.2 QES V2”.

The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures:
(a) after allowing for the data to be signed (DTBS) to be displayed correctly by an appropriate environment
(b) using appropriate hash functions that are, according to [6], agreed as suitable for qualified electronic signatures
(c) after appropriate authentication of the signatory by the TOE
(d) using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed as suitable according to [6].

The TOE ensures for the secrecy of the SCDs. To prevent the unauthorised usage of the SCDs the TOE provides user authentication and access control. The user authenticates himself with the knowledge of the Verification Authentication Data (VAD) against the Reference Authentication Data (RAD) securely stored inside the card. The TOE implements IT measures to support the establishment of a trusted path or trusted channel by cryptographic means.

The TOE does not implement the signature-creation application (SCA), that 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. So this ST assumes the SCA as environment of the TOE.

The TOE protects the SCD during the whole life cycle as to be solely used in the signature creation process by the legitimate signatory. The SSCD of Type 3 generates the signatory's SCDs and stores them in a secure manner. The TOE will be personalised for the signatory's use by
(1) generation of the SCD/SVD pairs,
(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 certificate-service-provider (CSP).

From the structural perspective, the SSCD comprises the underlying IC, the STARCOS 3.2 operating system (OS) and the signature application providing the functionality for SCD/SVD generation, authentic SVD export, SCD storage and use, and generation of electronic signatures. The SCA and the CGA (beside optional other applications) are part of the immediate environment of the TOE. The SCA and the CGA (beside optional other applications) are part of the immediate environment of the TOE. They shall communicate with the TOE over a trusted channel, a trusted path for the human interface provided by the SCA, respectively.

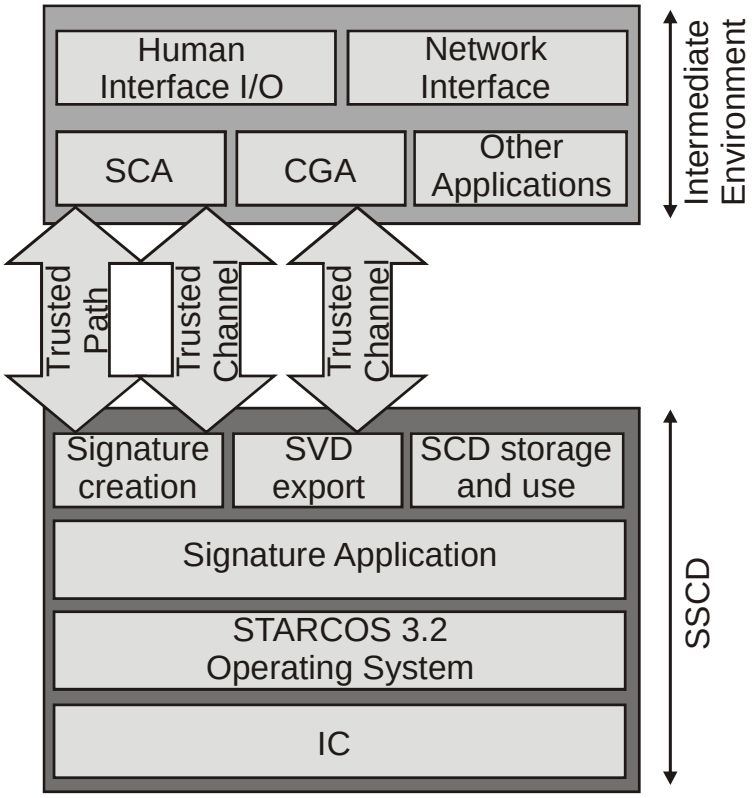


Figure 3: Scope of the SSCD, structural view

Beside the Signature Application there are also additional applications possible to reside on the card that contains the TOE for e.g. banking, ticketing or health care. These applications are using the same underlying IC and OS as the Signature Application. Each application, in particular the Signature Application, can define access rules to protect itself against misuse and unauthorised access. Usually the data structures for applications are loaded onto the card during initialisation and personalisation. Nevertheless it is still possible to add some data structures in the usage phase to the Signature Application like loading the qualified certificate for the SCD. Furthermore the complete data structures of additional applications may be loaded during the usage phase. These data structures does not include any executable code, therefore application functionality is always limited to the functionality of the operating system.

2.2.2 TOE Life Cycle

The TOE life cycle is shown in Figure 4. Basically, it consists of a development phase and the operational phase. The development phase includes OS Design and Application Design (responsibility: G&D), HW design (responsibility: Chip Manufacturer), HW Fabrication as well as OS Implementation (responsibility: Chip Manufacturer). The operational phase starts with the initialisation (responsibility: Initialiser: G&D or other card initialising facility), where the general signature application data is loaded, followed by the personalisation (responsibility: Personaliser: G&D or other card personaliser) including SCD generation and loading of personal signature application data. These phases represent installation, generation, and startup in the CC terminology. The delivery to the end user either happens after the personalisation or at some point during the personalisation phase (responsibility: Card Issuer). During initialisation phase and a personalisation

phase before TOE issuance the state of the TOE can be reverted to the state at the beginning of the initialisation phase. There are no other possibilities of reversion to an earlier life cycle state during the whole life cycle of the TOE. Re-generation of SCD/SVD key pairs is only possible in the personalisation phase before TOE issuance.
The operational phase is concluded by the usage phase. The main functionality in the usage phase is signature-creation including all supporting functionality (e.g. SCD storage and SCD use).

The evaluation process is limited to the development phase including all delivery procedures therein. Since the generation of the TOE is not completed after the development phase, all of the remaining processes have to be in agreement with the IT security requirements defined in chapter 5.

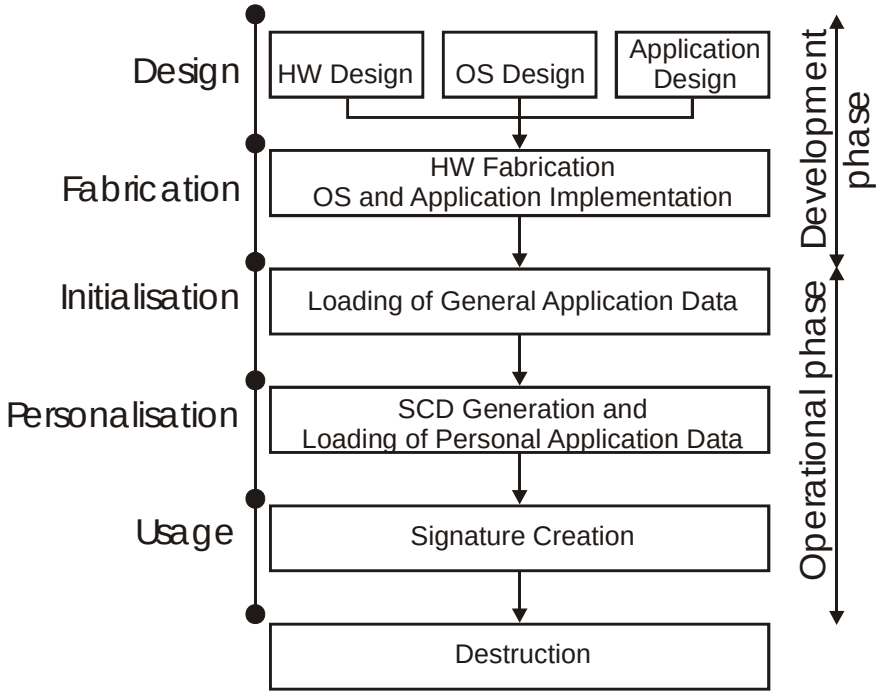


Figure 4. SSCD life cycle

2.2.3 Creation of initialisation data

The file system for the Digital Signature Application is specified in “Generic Application STARCOS 3.2 QES V2”. However this specification allows the card issuer to choose from several options for e.g. key lengths, hash algorithms and others. Beside this the card issuer may specify additional files e.g. for other applications. G&D then creates the initialisation data and checks with the “Smart Card Application Verifier STARCOS 3.2 QES V2.0B” if it conforms to the requirements of “Generic Application STARCOS 3.2 QES V2”. In the case of successful verification the initialisation data will be secured using secret data.

2.2.4 Delivery of ROM-Mask and initialisation data

As shown in Fig. 2, the Software part of the TOE consists of the STARCOS 3.2 operating system located in the ROM of the IC and the File System located in the EEPROM. Parts of the operating system may also reside in the EEPROM. The operating system developer (i.e. G&D) creates the ROM mask and sends this representation of the operating system together with secret data allowing

secure loading of initialisation data to the Chip Manufacturer (see Fig. 5). The Chip manufacturer manufactures the chips including the operating system and stores the secret data in a special area of the EEPROM of the Chip and delivers the chips packaged in modules to the Initialiser. The secret data is used by the OS developer to secure the initialisation data which is sent afterwards to the card initialising facility. The Card Initialising Facility manufactures the cards, performs the initialisation and then delivers the cards to the personalising facility.

With the secured initialisation data secret data is imported into the TOE allowing secure loading of personalisation data. This secret data is sent by the OS developer to the card issuer who uses it to secure the personalisation data and then send the secured personalisation data to the personalising facility which performs the personalisation before issuance of the TOE.

The Initialisation and Personalisation Process can be done partly or completely by G&D. The generation of the Personalisation data can also be done partly or completely at G&D.

During the personalisation before issuance, trust anchors can be imported into the TOE to allow a completion of the personalisation after issuance.

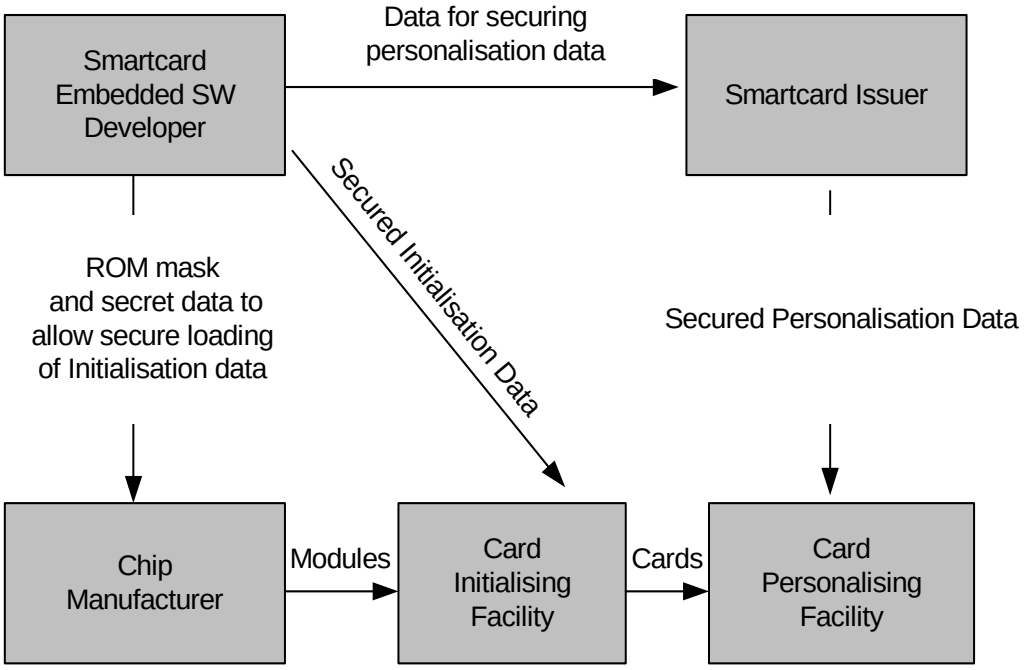


Figure 5: ROM Mask and initialisation data delivery

2.3 TOE operational environment

The TOE is used in two different types of operational environment. Prior to the issuance, the TOE has to be completed in the initialsation phase and the personalisation phase. After the issuance, the Card Holder controls the TOE. In case the personalisation of the signature application was not finished before issuance, he can only use other applications existing on the card until he provides the TOE to a personaliser for finishing of the personalisation. The Card Holder mainly interacts with the personalised TOE via the SCA.

2.4 Application Note: Scope of ST application

This ST is intended to be used for CC evaluation of a Secure Signature Creation Device (SSCD) in agreement with the requirements specified in Annex III of [1] as well as the requirements from German signature Act (§17 Abs.1 and 3 Nr.1 [17] and §15 Abs. 1, 4 [18]). Supported cryptographic algorithms are RSA with key lengths up to 2048 Bit for signature generation and SHA-2 (224 bit, 256 bit, 384 bit, 512 bit) as well as RIPEMD160 for Hashing - all of them in agreement with [6]. Beside the signature application itself there are additional applications possible, which reside also on the SSCD and are completely separated from the signature application. While the main application scenario of a SSCD will assume a qualified certificate (i.e. an electronic attestation of the SVD corresponding to the signatory's SCD) to be used in combination with a SSCD, there still is a large benefit in the security when such a SSCD is applied in other areas, since other applications can use the trustworthy evaluated security related functionality used by the signature application.

According to [1], for the generation of a legally binding advanced electronic signature based on a qualified certificate the use of a SSCD as well as the existence of a qualified certificate for the signatory's SVD is mandatory. In addition, the EU Directive [1] does not prevent the use of a SSCD together with a non-qualified certificate and still regard the device itself as SSCD.

3 TOE Security Environment

This chapter has been taken from [7] without modification, except for Note1 for the Assets defined in this chapter.

Assets:

1. SCD: private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).

2. 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).

3. DTBS and DTBS-representation: set of data, or its representation which is intended to be signed (Their integrity must be maintained).

4. VAD: PIN code or biometrics data entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD must be maintained)

5. RAD: Reference PIN code or biometrics authentication reference used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)

6. 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)

7. Electronic signature: (Unforgeabilty of electronic signatures must be assured).

Note1: Biometric authentication is not supported by the TOE. Therefore 'biometric data' or 'biometric authentication references' are not used by the TOE.

Subjects:

Subjects	Definition
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.

Threat agents:

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**.

3.1 Assumptions

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.

In addition to these assumptions the assumptions made in [8] for the certification of the IC have to be considered by the user.

3.2 Threats to Security

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 atacker 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 un-revoked 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.

In addition to these threats the threats described in [8] for the certification of the IC have to be considered by the user.

3.3 Organisational Security Policies

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

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions. This chapter has been taken from [7] without modification.

4.1 Security Objectives for the TOE

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 detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-generation.

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*

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 signatures shall be resistant against these attacks, even when executed with a high attack potential.

4.2 Security Objectives for the Environment

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 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.

5 IT Security Requirements

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

Security functional requirements components given in section 5.1 “TOE security functional requirements” excepting FPT_EMSEC.1 which is explicitly stated, are drawn from Common Criteria part 2 [3]. Some security functional requirements represent extensions to [3]. Operations for assignment, selection and refinement have been made.

The TOE security assurance requirements statement given in section 5.2 “TOE Security Assurance Requirement” refers to the security assurance components from Common Criteria part 3 [4].

Section 5.3 identifies the IT security requirements that are to be met by the IT environment of the TOE.

The non-IT environment is described in section 5.4.

Any operations performed in the E-Sign F PP [7] are identified by an underline.
Any uncompleted operations from the E-Sign F PP [7] that have been completed in this ST are identified by an underline and in *italic*.
Any changes to operations performed in the E-Sign F PP [7] and application notes defined in [7] (including introduction of additional notes) are marked by segmented unterline. Any other changes are marked in the text.

5.1 TOE Security Functional Requirements

5.1.1 Cryptographic support (FCS)

5.1.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *G&D_RSAGen* and specified cryptographic key sizes *between 1728 bit and 2048 bit* that meet the following: *[6]*.

5.1.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1/ RE-GENERATION	The TSF shall destroy cryptographic keys in case of regeneration of a new SCD in accordance with a specified cryptographic key destruction method *physical deletion of key value* that meets the following: *none*.

Note:

The cryptographic key SCD will be destroyed on demand of the Administrator during the Initialisation or Personalisation phase by deletion of the EEPROM containing the SCD. The deletion of the EEPROM is mandatory before the SCD/SVD pair is re-generated by the TOE within the Initialisation or Personalisation phase. Re-generation of the SCD/SVD pair is not possible during the usage phase.

5.1.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP	The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *between 1728 bit and 2048 bit* that meet the following: *[6]*.
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 1728 bit and 2048 bit* that meet the following: *[6]*.

5.1.2 User data protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1)

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

5.1.2.2 Security attribute based access control (FDP_ACF.1)

The security attributes for the user, TOE components and related status are

User, subject or object the attribute is associated with	Attribute	Status
General attribute		
User	Role	Administrator, Signatory
Initialisation attribute		
User	SCD / SVD management	authorised, not authorised

Signature-creation attribute group		
SCD	SCD operational	no, yes
DTBS	sent by an authorised SCA	no, yes

Initialisation SFP

FDP_ACF.1.1/ Initialisation SFP	The TSF shall enforce the Initialisation SFP to objects based on 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.

Refinement
The user with the security attribute “role” set to “Signatory” is not 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.

SVD Transfer

FDP_ACF.1.1/ SVD Transfer SFP	The TSF shall enforce the SVD Transfer SFP to objects based on General attribute.
FDP_ACF.1.2/ SVD Transfer SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 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 rule: none.

Personalisation SFP

FDP_ACF.1.1/ Personalisation SFP	The TSF shall enforce the Personalisation SFP to objects based on General attribute.
FDP_ACF.1.2/ Personalisation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 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 rule: none.

Signature-creation SFP

FDP_ACF.1.1/ Signature-creation SFP	The TSF shall enforce the Signature-creation SFP to objects based on General attribute and Signature-creation attribute group.
FDP_ACF.1.2/ Signature-creation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 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”.

5.1.2.3 Export of user data without security attributes (FDP_ETC.1)

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

5.1.2.4 Import of user data without security attributes (FDP_ITC.1)

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

Note:

A SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature and is able to establish a trusted channel to the SSCD as required by FTP_ITC.1.3/SCA DTBS.

5.1.2.5 Subset residual information protection (FDP_RIP.1)

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from the following objects: SCD, VAD, RAD.

5.1.2.6 Stored data integrity monitoring and action (FDP_SDI.2)

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 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.

5.1.2.7 Data exchange integrity (FDP_UIT.1)

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

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1	The TSF shall detect when *3* unsuccessful authentication attempts occur related to consecutive failed authentication attempts.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall block RAD.

5.1.3.2 User attribute definition (FIA_ATD.1)

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

5.1.3.3 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [

1. Identification of the user by means of TSF required by FIA_UID.1.
2. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE.
3. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import.
4. *Receiving DTBS by means of TSF required by FDP_ITC.1.]*

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.

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.

5.1.3.4 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow

1. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE.
2. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import.
3. Receiving DTBS by means of TSF required by FDP_ITC.1.]

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

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to enable the signature-creation function to Signatory.

5.1.4.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/ Administrator The TSF shall enforce the Initialisation SFP to restrict the ability to modify the security attributes SCD / SVD management to Administrator.

FMT_MSA.1.1/ Signatory The TSF shall enforce the Signature-creation SFP to restrict the ability to modify the security attributes SCD operational to Signatory.

5.1.4.3 Secure security attributes (FMT_MSA.2)

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

5.1.4.4 Static attribute initialisation (FMT_MSA.3)

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

Refinement
The security attribute of the SCD “SCD operational” is set to “no” after generation of the SCD.

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

Refinement
The TOE does not allow specifying alternative initial values at all for security reasons. Therefore even the Administrator cannot specify alternative initial values.

5.1.4.5 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to modify the RAD to Signatory.

5.1.4.6 Specification of Management (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: *security function management, security attribute management and TSF data management.*

Note: This chapter was not part of [7] but had to be introduced due to [16].

5.1.4.7 Security roles (FMT_SMR.1)

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.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Abstract machine testing (FPT_AMT.1)

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

5.1.5.2 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit *information about IC power consumption and command execution time* 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 *VCC, GND, IO* to gain access to RAD and SCD.

Note:

The TOE implements countermeasures against state-of-the-art attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE.

5.1.5.3 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *inconsistencies in the calculation of the signature and fault injections during the operation of the TSF.*

5.1.5.4 Passive detection of physical attack (FPT_PHP.1)

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

5.1.5.5 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist *tampering of the physical operating conditions voltage supply, clock frequency and temperature beyond the valid limits* to the *IC* by responding automatically such that the TSP is not violated.

5.1.5.6 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Refinement
The security properties, in particular access control, of the signature application can not be modified by data structures of additional applications residing or loaded on the TOE.

Note: This chapter was not part of [7].

5.1.5.7 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Refinement
The security properties, in particular access control, of the signature application can not be modified by data structures of additional applications residing or loaded on the TOE.

Note: This chapter was not part of [7].

5.1.5.8 TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, at the condition Reset of the TOE* to demonstrate the correct operation of the TSF.

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

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

5.1.6 Trusted path/channels (FTP)

5.1.6.1 Inter-TSF trusted channel (FTP_ITC.1)

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* 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 **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.

5.1.6.2 Trusted path (FTP_TRP.1)

The trusted path between the TOE and the SCA will be required only if the human interface for user authentication is not provided by the TOE itself but by the SCA.

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 *initial user authentication*.

5.2 TOE Security Assurance Requirements

The assurance components for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

AVA_MSU.3 and AVA_VLA.4.

Table 5.1 : Assurance Requirements: EAL(4)

Assurance Class	Assurance Components
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO	ADO_DEL.2 ADO_IGS.1
ADV	ADV_FSP.2 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1 ALC_LCD.1 ALC_TAT.1
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.3 AVA_SOF.1 AVA_VLA.4

5.3 Security Requirements for the IT Environment

5.3.1 Certification generation application (CGA)

5.3.1.1 Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1/ CGA — The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method qualified certificate that meets the following: *none*.

5.3.1.2 Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/ CGA — The TSF shall perform import the SVD in accordance with a specified cryptographic key access method import through a secure channel that meets the following: *none*.

5.3.1.3 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ SVD import — The TSF shall enforce the SVD import SFP to be able to receive user data in a manner protected from modification and insertion errors.

FDP_UIT.1.2/ SVD import — The TSF shall be able to determine on receipt of user data, whether modification and insertion has occurred.

5.3.1.4 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SVD import	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/ SVD import	The TSF shall permit *the 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.

5.3.2 Signature creation application (SCA)

5.3.2.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ SCA Hash	The TSF shall perform hashing the DTBS in accordance with a specified cryptographic algorithm *SHA-2 (224 bit, 256 bit, 384 bit, 512 bit) or RIPEMD-160* and cryptographic key sizes none that meet the following: *[6].*

5.3.2.2 Data exchange integrity (FDP_UIT.1)

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

5.3.2.3 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SCA DTBS	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/ SCA DTBS	The TSF shall permit the TSF to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCA DTBS	The TSF **or the TOE** shall initiate communication via the trusted channel for signing DTBS-representation by means of the SSCD.

5.3.2.4 Trusted path (FTP_TRP.1)

The trusted path between the TOE and the SCA will be required only if the human interface for user authentication is not provided by the TOE itself but by the SCA.

FTP_TRP.1.1/ SCA	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2/ SCA	The TSF shall permit *local users* to initiate communication via the trusted path.
FTP_TRP.1.3/ SCA	The TSF shall require the use of the trusted path for *initial user authentication.*

5.4 Security Requirements for the Non-IT Environment

R.Administrator_Guide *Application of Administrator Guidance*

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

R.Sigy_Guide *Application of User Guidance*

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

R.Sigy_Name *Signatory’s name in the Qualified Certificate*

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

6 TOE Summary Specification

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

6.1 TOE Security Functions

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

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

Table 6.1 : SOF claims for TOE Security Functions

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

The SFs described in 6.1.1 to 6.1.7 are realised by software components supported by the underlying hardware in accordance with the description in 6.1.8 (hardware related SF).

6.1.1 SF.ACCESS Access Control

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

For this purpose this Security function maintains security attributes to store the data to verify authentication attempts and to store the results of authentications with passwords or cryptographic protocols. Furthermore SF.ACCESS implements the conditions on security attributes and communication protection required for specific operations.

This Security Function is composed of:

1) Maintenance of the Security Attributes “Role”, “SCD/SVD management”, “SCD operational”, “RAD” and “sent by an authorised SCA”.
2) The generation of the SCD/SVD pair is for the Administrator allowed only if “SCD/SVD management” is set to "authorised".
3) The export of the SVD is allowed for the Administrator. The usage of a trusted channel for the export of the SVD is required.
4) The creation of RAD is allowed for the administrator during the initialisation and personalisation phase.
5) The creation of a signature is only for the Signatory allowed during the usage phase if the DTBS is sent by an authorised SCA and “SCD operational” is set to “yes”.
6) Receiving DTBS, establishing a trusted path or a trusted channel is allowed before Identification and Authentication of the user. Other TSF mediated actions on behalf of a user require his prior successful authentication.
7) Enabling the signature-creation function is only allowed for the Signatory.
8) Modifying RAD and “SCD operational” is only allowed for the Signatory.
9) Modifying “SCD/SVD management” is only allowed for the Administrator.

6.1.2 SF.ADMIN Administration of the TOE

The administration of the TOE is managed by this Security Function. The TOE administration is mainly done in the initialisation and personalisation phase and therefore SF.ADMIN covers the TSF functionality dedicated to these phases.

This Security Function is composed of:

1) Authentication mechanism for the Administrator. During initialisation and personalisation phase the authentication mechanism is based on symmetric cryptography and for the usage phase the authentication mechanism can be based on symmetric or asymmetric cryptography.
2) Secure Modification of the Security Attributes “Role” and “SCD/SVD management” by the authentication of the administrator.

3) Management of SCD/SVD generation with key sizes between 1728 bit and 2048 bit. The SCD/SVD pair can be generated during the initialisation/personalisation phase and the usage phase.
4) Before a new SCD is generated the old SCD is physically deleted. Re-generation of the SCD is only possible in the initialisation and personalisation phase.
5) The security attribute “SCD operational” is set to “no” after generation of the SCD.
6) The SVD is exported without associated security attributes. The SVD can be exported in the personalisation phase and in the usage phase. In both cases the integrity and authenticity of the SVD can be ensured by symmetric or asymmetric cryptography. This protection can be achieved in both phases by exporting the SVD in conjunction with a MAC or a signature and additionally in the usage phase by performing a mutual authentication with negotiation of session keys used for the protection of the SVD.
7) Creation of RAD during the personalisation phase. Usually a Transport-RAD is created which must be replaced by the signatory before the first usage of the SCD.

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

6.1.3 SF.AUTH Authentication of the Signatory

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

This Security Function is composed of:

1) Authentication mechanism for the Signatory based on the knowledge of a PIN or password. If there are 3 or more consecutive failed authentication attempts the RAD is blocked. If a Transport-RAD is stored an authentication of the signatory is not possible.
2) Secure Modification of the Security Attributes “Role”, “SCD operational” and “RAD” and unblocking of the Security Attribute "RAD". The signatory has to replace a Transport-RAD with a normal RAD and with that changing “SCD operational” to “yes” before his authentication can be performed. This security function does not allow to import a Transport-RAD. The number of unblocking operations on the RAD is limited to ten.
3) Enabling the signature-creation function if the authentication of the signatory was successful.

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

6.1.4 SF.SIG Signature Creation

The Signature Creation is managed by this Security Function. This Security function is only active during the usage phase.

This Security Function is composed of:

1) Receiving hash values (without associated security attributes) and calculating hash values for the signing process,
2) Ensuring the integrity of the hash value used for the signing process,
3) Generating digital signatures according to DIN V66291-4[11] and PKCS#1[12]:
   - "DSI according to ISO/IEC 9796-2 with Random Number" specified in Annex A, chapter 2.1.1. of DIN V66291-4[11],
   - "EMSA-PKCS1-v1_5" specified in chapter 9.2 of PKCS#1[12],
   - "EMSA-PSS" specified in chapter 9.1 of PKCS#1[12],

   The hash calculation and the RSA calculation are provided by SF.CRYPTO.

6.1.5 SF.CRYPTO Cryptographic Support

This Security Function provides the cryptographic support for the other Security Functions.

This Security Function is composed of:

1) Calculating hash values according to SHA-2 (224 bit, 256 bit, 384 bit, 512 bit) and RIPEMD-160,
2) RSA calculation with key sizes between 1728 bit and 2048 bit,
3) Triple DES calculation with key sizes of 128 bit in ECB and CBC mode,
4) Random number generation, e.g. used for key generation and authentication process. There are two random number generators. The deterministic one is rated K3 (high) according to AIS20 [14]. To provide random numbers generated by the physical generator this security function calls SF.IC_SF.
5) Calculation of block check values to insure data integrity.
6) Generation of RSA key pairs with key sizes between 1728 bit and 2048 bit.

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

6.1.6 SF.TRUST Trusted Communication

This Security Function manages the establishing of trusted channels/paths and the application of the protection of the communication data.

This Security Function is composed of:

1) Establishing a trusted channel/path based on mutual authentication with negotiation of symmetric cryptographic keys used for the protection of the communication data. The mutual authentication is based on a challenge response protocol using either the RSA algorithm according the key transport protocol of [10] or the DES algorithm according [10].
2) Ensuring the confidentiality of communication data, e.g. by encrypting the communication data (e.g. the VAD) using symmetric cryptography.

3) Ensuring the integrity of communication data, e.g. by calculating a cryptographic checksum for the communication data (e.g. the DTBS representation) using symmetric cryptography or by calculating a signature for the communication data using asymmetric cryptography.
4) Secure Modification of the Security Attributes “sent by an authorised SCA”.

6.1.7 SF.PROTECTION Protection of TSC

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

This Security Function is composed of:

1) Upon the de-allocation of resources from SCD, VAD and RAD the information content of these resources is physically deleted.
2) Ensuring the integrity of SCD, SVD and RAD when using them.
3) Demonstrating the correct operation of the IC by among other things checking environment sensors and testing the hardware random generator as well as other hardware devices.
4) Demonstrating the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections.
5) Hiding information about IC power consumption and command execution time, to ensure that the interfaces VCC, GND and IO can not be used to gain access to RAD and SCD.
6) Preserving a secure state in the case of inconsistencies in the calculation of the signature and fault injections during the operation of the TSF.

6.1.8 SF.IC_SF Security Functions of the IC

This Security Function covers the Security Functions of the IC [8].

This Security Function is composed of:

1) Detection of physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation.
2) Resistance to physical tampering of the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analysing and physical tampering.
3) Random number generation. For the P2 rating of the HW-RNG according to AIS31 [13] see [15].
4) Cryptographic support for Triple DES calculations with cryptographic key sizes of 128 bit that comply to FIPS PUB 46-3, 1999 October 25, keying option 2 and support for RSA calculations, with cryptographic key sizes between 1728 bit and

2048 bit that comply with ISO/IEC 9796-1, Annex A, section A.4 and A.5 and Annex C.

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

6.2 Assurance Measures

This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 5.2.

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

Table 6.1 : References of Assurance Measures

Assurance Measures	Description
AM_ACM	The configuration management is described in the configuration management documentation.
AM_ADO	The delivery, installation, generation and start-up of the TOE is described in the delivery documentation and the IGS documentation.
AM_ADV	The representing of the TSF is described in the documentation for security policy modelling, in the documentation for functional specification, in the documentation for high level design, in the documentation for low level design, in the documentation for implementation representation and in the documentation for representation correspondence.
AM_AGD	The guidance documentation is described in the user guidance documentation for the user and in the administrator guidance documentation for the administrator.
AM_ALC	The life cycle support of the TOE during its development and maintenance is described in the life cycle documentation.
AM_ATE	The testing of the TOE is described in the test documentation..
AM_AVA	The vulnerability assessment for the TOE is described in the documentation for misuse, in the strength of TOE security functions documentation and in the vulnerability analysis documentation.

7 PP Compliance Claims

7.1 PP Reference

Secure Signature-Creation Device Protection Profile Type 3, v1.05 EAL4+, BSI-PP-0006-2002, 25 July 2001 [7].

7.2 PP changes and additions

The following changes and additions with respect to the SSCD PP [7] have been made:

- FIA_UAU.1 (changed)
- FIA_UID.1 (changed)
- FMT_SMF.1 (added)
- FPT_RVM.1 (added)
- FPT_SEP.1 (added)
- Notes added: FMT_SMF.1, FPT_RVM.1, FPT_SEP.1

7.3 PP compliance

This Security Target is compliant to the referenced Protection Profile as the described deviations are not in conflict with the SSCD PP [7].

8 Rationale

The chapters 8.1 to 8.6 as well as 8.8 and 8.9 have been taken from [7] with modifications only according to the changes in the previous chapters.

8.1 Introduction

The tables in sub-sections 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 .

8.2 Security Objectives Rationale

8.2.1 Security Objectives Coverage

Table 8.1: Security Environment to Security Objectives Mapping

Threads - 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	OE.CGA_Qcert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend
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
T.SigF_Misuse										X	X				X	X
T.Sig_Forgery	X	X		X	X	X	X	X				X	X	X		X
T.Sig_Repud	X	X		X	X	X	X	X	X	X	X	X	X	X		X
A.CGA													X	X		
A.SCA																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 Objective 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 [1], article 5, paragraph 1. Directive [1], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The requirement of qualified electronic signatures being based on qualified certificates is addressed by OE.CGA_QCert. OE.SCA_Data_Intend provides that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. OT.Sig_Secure and OT.Sigy_SigF address the generation of advanced signatures by the TOE.

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

8.2.2.2 Threats and Security Objective 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 [1], 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.

The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by verifying the integrity of the DTBS-representation. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.SCA_Data_Indent.

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

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. This threat is in general addressed by OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.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 signaturecreation 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), 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, 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.

8.2.2.3 Assumptions and Security Objective 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.

8.3 Security Requirements Rationale

8.3.1 Security Requirement Coverage

Table 8.2 : Functional Requirement to TOE Security Objective Mapping

TOE Security Functional Requirement / 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
FCS_CKM.1				X	X				X			
FCS_CKM.4		X		X								
FCS_COP.1/CORRESP					X							
FCS_COP.1/SIGNING												X
FDP_ACC.1/SVD_TRANSFER SFP						X						
FDP_ACC.1/INITIALISATION SFP			X	X								
FDP_ACC.1/PERSONALISATION SFP											X	
FDP_ACC.1/SIGNATURE-CREATION SFP										X	X	
FDP_ACF.1/INITIALISATION SFP			X	X								
FDP_ACF.1/SVD_TRANSFER SFP						X						
FDP_ACF.1/PERSONALISATION SFP											X	
FDP_ACF.1/SIGNATURE-CREATION SFP										X	X	
FDP_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	
FIA_UID.1			X								X	
FMT_MOF.1				X							X	
FMT_MSA.1/ADMINISTRATOR			X	X								
FMT_MSA.1/SIGNATORY											X	
FMT_MSA.2											X	
FMT_MSA.3/			X	X							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_RVM.1				X						X	X	
FPT_SEP.1				X						X	X	

FPT_TST.1		X										X
FTP_ITC.1/SVD TRANSFER						X						
FTP_ITC.1/DTBS IMPORT										X		
FTP_TRP.1/TOE											X	

Table 8.3 : IT Environment Functional requirements to Environment Security Objective Mapping

Environment Security Requirement / Environment Security objectives	OE.CGA_Qcert	OE.HI_VAD	OE.SCA_Data_Intend	OE.SVD_Auth_CGA
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			

Table 8.4 : Assurance Requirement to Security Objective 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	AVA_SOF.1, AVA_VLA.4
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.

FPT_RVM.1 and FPT_SEP.1 ensure that the TSF dealing with granting access to the SCD can not be bypassed or corrupted by additional applications on the TOE.

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 use 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 [1], 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 keeps unauthorised parties off from altering the DTBS-representation. FPT_RVM.1 and FPT_SEP.1 ensure that the TSF dealing with controlling access to the DTBS-representation can not be bypassed or corrupted by additional applications on the TOE.

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_SMF.1, 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_SMF.1, FMT_MSA.2, and FMT_MSA.3 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.

FPT_RVM.1 and FPT_SEP.1 ensure that the TSF dealing with granting access to the signature generation function can not be bypassed or corrupted by additional applications on the TOE.

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.

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.

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 it's integrity.

8.4 Depencency 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).

Table 8.5 : 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/ Personalisation SFP	FDP_ACF.1/Personalisation SFP
FDP_ACC.1/ Signature-Creation SFP	FDP_ACF.1/Signature Creation SFP
FDP_ACC.1/ SVD Transfer SFP	FDP_ACF.1/SVD Transfer SFP
FDP_ACF.1/ Initialisation SFP	FDP_ACC.1/Initialisation SFP, FMT_MSA.3
FDP_ACF.1/ Personalisation SFP	FDP_ACC.1/Personalisation SFP, FMT_MSA.3
FDP_ACF.1/ Signature-Creation SFP	FDP_ACC.1/Signature-Creation SFP, FMT_MSA.3
FDP_ACF.1/ SVD Transfer SFP	FDP_ACC.1/SVD Transfer SFP, FMT_MSA.3
FDP_ETC.1/ SVD Transfer SFP	FDP_ACC.1/ SVD Transfer SFP
FDP_ITC.1/DTBS	FDP_ACC.1/ Signature-Creation SFP, FMT_MSA.3
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_UAU.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Administrator	FDP_ACC.1/Initialisation SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	FDP_ACC.1/ Signature_Creation SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1/Personalisation SFP, FMT_SMR.1 FMT_MSA.1/Administrator, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1/Administrator, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1
FMT_SMR.1	FIA_UID.1
FPT_FLS.1	ADV_SPM.1
FPT_PHP.1	FMT_MOF.1
FPT_TST.1	FPT_AMT.1
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_SPM.1	ADV_FSP.1
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.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_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 sub-section 8.4.2 for justification
FCS_CKM.3/CGA	unsupported dependencies, see sub-section 8.4.2 for justification

FDP_UIT.1/SVD IMPORT	FTP_ITC.1/SVD_IMPORT, unsupported dependencies, see subsection 8.4.2 for justification
Functional Requirements for Signature creation application (SCA)	
FCS_COP.1/SCA HASH	unsupported dependencies, see sub-section 8.4.2 for justification
FDP_UIT.1/SCA DTBS	FTP_ITC.1/ SCA DTBS, unsupported dependencies on FDP_ACC.1, see sub-section 8.4.2 for justification

8.4.2 Justification of Unsupported Dependencies

The security functional dependencies for the TOE environment CGA and SCA are not completely supported by security functional requirements in section 5.3.

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 cannel 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 precedent chapter

Table 8.6 : Functional and Assurance Requirements Dependencies

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

8.6 Rationale for Extensions

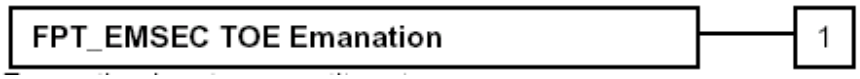
The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena 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 Rationale for TOE Summary Specification

8.7.1 Rationale for TOE Security Functions

8.7.1.1 TOE Security Functions

The following table gives the coverage of the TOE Security Functional Requirements by the TOE Security Functions. The numbers in the table give the corresponding component of the Security Function covering the requirement. If not obvious it is explained below the table how the identified components satisfy the requirements.

Table 8-7 Functional Requirements to Security Function mapping

SFR / Security Function	SF.ACCESS	SF.ADMIN	SF.AUTH	SF.SIG	SF.CRYPTO	SF.TRUST	SF.PROTECTION	SF.IC_SF
FCS_CKM.1.1		3			4,6			3
FCS_CKM.4.1/ RE-GENERATION		4						
FCS_COP.1.1/ CORRESP				3	6			
FCS_COP.1.1/ SIGNING				3	1,2			4
FDP_ACC.1.1/ SVD Transfer SFP	3	1				3		
FDP_ACC.1.1/ Initialisation SFP	2	1,2						
FDP_ACC.1.1/ Personalisation SFP	4	1,7						
FDP_ACC.1.1/ Signature-creation SFP	5		1					

FDP_ACF.1/ SVD Transfer SFP	3	1				3		
FDP_ACF.1/ Initialisation SFP	2	1,2						
FDP_ACF.1/ Personalisation SFP	4	1,7						
FDP_ACF.1/ Signature-creation SFP	5		1					
FDP_ETC.1/ SVD Transfer		6						
FDP_ITC.1/ DTBS	5			1		3,4		
FDP_RIP.1.1							1	
FDP_SDI.2/ Persistent					5		2	
FDP_SDI.2/ DTBS				2	5			
FDP_UIT.1/ SVD Transfer					2,3	3		4
FDP_UIT.1/ TOE DTBS					3	3		4
FIA_AFL.1			1					
FIA_ATD.1.1	1							
FIA_UAU.1	6							
FIA_UID.1	6							
FMT_MOF.1.1	7		3					
FMT_MSA.1.1/ Administrator	9	2						
FMT_MSA.1.1/ Signatory	8		2					
FMT_MSA.2.1		2	2			4		
FMT_MSA.3		5						
FMT_MTD.1.1	8		2					
FMT_SMF.1.1		2	2,3					
FMT_SMR.1	1							
FPT_AMT.1.1							3	
FPT_EMSEC.1							5	
FPT_FLS.1.1							6	
FPT_PHP.1								1
FPT_PHP.3.1								2
FPT_RVM.1	2,5,6, 7,8,9							
FPT_SEP.1	2,5,6, 7,8,9							
FPT_TST.1							4	
FTP_ITC.1/ SVD Transfer		6				1,2,3		

FTP_ITC.1/ DTBS import			1			1,2,3		
FTP_TRP.1/ TOE			1			1,2,3		

FCS_CKM.1.1 is fulfilled by **SF.ADMIN.3** which uses the functionality of **SF.CRYPTO.6**, **SF.CRYPTO.4** and **SF.IC_SF.3**.

FCS_CKM.4.1/ RE-GENERATION is fulfilled by **SF.ADMIN.4** enforcing the deletion of an old SCD before re-generation.

FCS_COP.1.1/ CORRESP is fulfilled by **SF.CRYPTO.6** which generates corresponding SCD/SVD pairs and **SF.SIG.3** which can calculate a signature over SVD to prove the correspondence of a SCD and SVD. The proof can be verified by verifying the signature.

FCS_COP.1.1/ SIGNING is fulfilled by **SF.SIG.3**, **SF.CRYPTO.2** and **SF.IC_SF.4** are used for the RSA calculations. **SF.CRYPTO.1** allows to calculate hash values from DTBS,

FDP_ACC.1.1/ SVD Transfer SFP and **FDP_ACF.1/ SVD Transfer SFP** are fulfilled by **SF.ACCESS.3.** Only the administrator is able to request from the TSF the protection of the integrity and authenticity of SVD via **SF.TRUST.3**. **SF.ADMIN.1** allows the authentication of the administrator.

FDP_ACC.1.1/ Initialisation SFP and **FDP_ACF.1/ Initialisation SFP: SF.ACCESS.2** ensures that only the administrator can generate the SCD/SVD pair. **SF.ADMIN.2** sets “SCD/SVD management” to "authorised", when the administrator is authenticated by **SF.ADMIN.1.**

FDP_ACC.1.1/ Personalisation SFP and **FDP_ACF.1/ Personalisation SFP: SF.ACCESS.4** ensures that only the administrator can create RAD with **SF.ADMIN.7** after the administrator was authenticated by **SF.ADMIN.1**

FDP_ACC.1.1/ Signature-creation SFP and **FDP_ACF.1/ Signature-creation SFP** are fulfilled by **SF.ACCESS.5.** With **SF.AUTH.1** the signatory is authenticated, the SCA is authorised and ensured that SCD is operational.

FDP_ETC.1/ SVD Transfer: The SVD is exported by **SF.ADMIN.6** without associated security attributes.

FDP_ITC.1/ DTBS is fulfilled by **SF.SIG.1**, **SF.ACCESS.5, SF.TRUST.3** and **SF.TRUST.4**. **SF.ACCESS.5** allows the signature creation only if "sent by an authorised SCA" is set to "yes" by **SF.TRUST.4** when the SCA uses a trusted channel to the SSCD by using SF.TRUST.3. With **SF.SIG.1** the DTBS-representation can only be sent without associated security attributes to the TSF.

FDP_RIP.1.1: Upon the de-allocation of resources from SCD, VAD and RAD the information content of these resources is physically deleted by **SF.PROTECTION.1**.

FDP_SDI.2/ Persistent: SF.PROTECTION.2 ensures the integrity of SCD, SVD and RAD with the support from **SF.CRYPTO.5.**

FDP_SDI.2/ DTBS: SF.SIG.2 ensures the integrity of the hash value with the support from **SF.CRYPTO.5.**

FDP_UIT.1/ SVD Transfer is fulfilled by **SF.TRUST.3** which uses **SF.CRYPTO.2** or **SF.CRYPTO.3** and **SF.IC_SF.4**.

FDP_UIT.1/ TOE DTBS is realised by SF.TRUST.3 which ensures the integrity by using SF.CRYPTO.3 which uses SF.IC_SF.4.

FIA_AFL.1: If there are 3 or more consecutive failed authentication attempts the RAD is blocked by **SF.AUTH.1**.

FIA_ATD.1.1: SF.ACCESS.1 maintains RAD.

FIA_UAU.1 and **FIA_UID.1**: **SF.ACCESS.6** ensures that receiving DTBS, establishing a trusted path or a trusted channel is allowed before Identification and Authentication of the user. Other TSF mediated actions on behalf of a user require his prior successful authentication.

FMT_MOF.1.1 is fulfilled by **SF.ACCESS.7** which restricts the usage of **SF.AUTH.3** to the signatory.

FMT_MSA.1.1/ Administrator: SF.ACCESS.9 ensures that only the administrator can modify "SCD/SVD management" by using **SF.ADMIN.2**.

FMT_MSA.1.1/ Signatory is fulfilled by **SF.ACCESS.8** which restricts the usage of **SF.AUTH.2** to the signatory.

FMT_MSA.2.1 is fulfilled as all security attributes mentioned in **SF.ADMIN.2**, **SF.AUTH.2** and **SF.TRUST.4** are set by the TSF itself with secure values. Only RAD can be set by the signatory, but **SF.AUTH.2** verifies if the new RAD has a sufficient length.

FMT_MSA.3: SF.ADMIN.5 ensures that “SCD operational” is set to “no” after generation of the SCD.

FMT_MTD.1.1 is fulfilled by **SF.ACCESS.8** which restricts the usage of **SF.AUTH.2** to the signatory.

FMT_SMF.1.1 is fulfilled by **SF.AUTH.3** managing the signature-creation function, **SF.ADMIN.2** managing security attributes and **SF.AUTH.2** managing beside security attributes also the TSF data RAD.

FMT_SMR.1: SF.ACCESS.1 maintains the security attribute “role”.

FPT_AMT.1.1: SF.PROTECTION.3 demonstrates the correct operation of the IC.

FPT_EMSEC.1: SF.PROTECTION.5 hides information about IC power consumption and command execution time.

FPT_FLS.1.1: SF.PROTECTION.6 preserves a secure state in the case of inconsistencies in the calculation of the signature and fault injections during the operation of the TSF.

FPT_PHP.1: SF.IC_SF.1 detects physical tampering of the TSF.

FPT_PHP.3.1: SF.IC_SF.2 provides resistance to physical tampering of the TSF.

FPT_RVM.1: The design of the TOE ensures that the TSF are active and control the access to the TSC before the interfaces of the TOE can be used to proceed any function within the TSC. Therefore SF.ACCESS.2, SF.ACCESS.5, SF.ACCESS.6, SF.ACCESS.7, SF.ACCESS.8 and SF.ACCESS.9 can not be bypassed by additional applications residing on the TOE beside the signature application.

FPT_SEP.1.1: The design of the TOE ensures that the TSF can maintain its own security domain, so that entities external to that domain cannot modify data structures or code internal to the protected domain. The access control provided by the TSF, in particular SF.ACCESS.2, SF.ACCESS.5, SF.ACCESS.6, SF.ACCESS.7, SF.ACCESS.8 and SF.ACCESS.9, enforce the separation between security domains of subjects in the TSC, so that subjects using or loading

additional applications on the TOE are not able to observe or modify protected data structures of the signature application.

FPT_TST.1: SF.PROTECTION.4 demonstrates the correct operation of ht TSF.

FTP_ITC.1/ SVD Transfer is fulfilled by **SF.ADMIN.2**. The mutual authentication is provided by **SF.TRUST.1**, **SF.TRUST.3** ensures the integrity and authenticity of SVD and **SF.TRUST.2** can be used to protect the confidentiality.

FTP_ITC.1/ DTBS import: The trusted channel is established by **SF.TRUST.1** which uses **SF.TRUST.2** and **SF.TRUST.3**.

FTP_TRP.1/ TOE: The trusted path is established by **SF.TRUST.1** which uses **SF.TRUST.2** and **SF.TRUST.3**.

8.7.2 Rationale for Assurance Measures

The following table demonstrates the coverage of the Assurance Requirements by the Assurance measures by indicating the correspondence with crosses.

Table 8-8 Assurance Requirements to Assurance Measures mapping

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

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 security target 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 security target 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.
The evaluation level of the underlying HW is CC EAL5+. The evaluation level of the HW is sufficient for this composite evaluation according to CC EAL4+.

8.10 Rationale for PP Claims

Since the ST security objectives and requirements are identical to those of the claimed SSCD PP [7], this part of the ST is omitted.

9 Conventions and Terminology

9.1 Conventions

The document follows the rules and conventions laid out in Common Criteria 2.3, part 1 [2], Annex B “Specification of Security Targets”. Admissible algorithms and parameters for algorithms for secure signature-creation devices (SSCD) are given in a separate document [6]. Therefore, the ST refers to [6].

9.2 Terminology

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

Advanced electronic signature (defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control, and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

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

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

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

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

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

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

Data to be signed representation (DTBS-representation) means the data sent by the SCA to the TOE for signing and is
(a) a hash-value of the DTBS or
(b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or
(c) the DTBS. The SCA indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.

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

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

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

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

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

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

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

Signature-creation application (SCA) means the application used to create an electronic signature, excluding the SSCD. I.e., the SCA is a collection of application elements (a) to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision, (b) to send a DTBS-representation to the TOE, if the signatory indicates by specific nonmisinterpretable input or action the intend to sign, (c) to attach the qualified electronic signature generated by the TOE to the data or provides the qualified electronic signature as separate data.

Signature-creation data (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. (defined in the Directive [1], article 2.4)

Signature-creation system (SCS) means the overall system that creates an electronic signature. The signature-creation system consists of the SCA and the SSCD.

Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (defined in the Directive [1], article 2.7)

Signed data object (SDO) means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.

SSCD provision service means a service that prepares and provides a SSCD to subscribers.

User means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics.

10 References

[1] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[2] International Organization for Standardization, ISO/IEC 15408-1:2005 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

[3] International Organization for Standardization, ISO/IEC 15408-2:2005 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements

[4] International Organization for Standardization, ISO/IEC 15408-3:2005 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements

[5] Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive.

[6] Geeignete Kryptoalgorithmen In Erfüllung der Anforderungen nach §17 (1) bis (3) SigG in Verbindung mit Anlage 1, I 2, SigV, Bundesanzeiger Nr. 19, S.376, 05.02.2008

[7] Secure Signature-Creation Device Protection Profile Type 3, v1.05 EAL4+, BSI-PP-0006-2002, 25 July 2001

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

[9] Smart Card IC Platform Version 1.0, Juli 2001, BSI-PP-0002-2001

[10] CWA 14890-1 "Application Interface for SmartCards used as Secure Signature Creation Devices, Part 1 – Basic Requirements", March 8th 2004.

[11] Chipcards with digital signature application/function according to SigG and SigV, Part 4: Basic Security Services, DIN V66291-4, 2002

[12] PKCS#1: RSA Cryptography Standard, RSA Laboratories, Version 2.1, 14.06.2002

[13] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31; Bundesamt für Sicherheit in der Informationstechnik, Version 1, 25.09.2001

[14] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20; Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 2.12.1999

[15] Certification Report, BSI-DSZ-CC-0322-2005 for Infineon Smart Card IC (Security Controller) SLE66CX680PE/m1534a13 and SLE66CX360PE/m1536a13 both with RSA 2048 V1.4 and specific IC Dedicated Software from Infineon Technologies AG, 14.09.2005
Assurance Continuity Maintenance Report, BSI-DSZ-CC-0322-2005-MA04 for Infineon Smart Card IC (Security Controller) SLE66CX680PE/m1534a13 and SLE66CX360PE/m1536a13 both with RSA 2048 V1.4 and specific IC Dedicated Software from Infineon Technologies AG, 20.09.2006
Assurance Continuity Maintenance Report, BSI-DSZ-CC-0322-2005-MA06 for Infineon Smart Card IC (Security Controller) SLE66CX680PE/m1534a13 and SLE66CX360PE/m1536a13 both with RSA

2048 V1.4 and specific IC Dedicated Software from Infineon Technologies AG, 10.09.2007

[16] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 32; Bundesamt für Sicherheit in der Informationstechnik, Version 1, 02.07.2001, Final Interpretation 065, 31.07.2001

[17] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (BGBI. I S.876 ff) und Erstes Gesetz zur Änderung des Signaturgesetzes vom 04. Januar 2005 (BGBl. I Nr. 1 2005, S.2f)

[18] Verordnung zur digitalen Signatur (Signaturverordnung) vom 16. November 2001

[19] http://www.commoncriteriaportal.org/public/expert/index.php?menu=5

11 Acronyms

CC Common Criteria

EAL Evaluation Assurance Level

IT Information Technology

PP Protection Profile

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSFI TSF Interface

TSP TOE Security Policy