SIEMENS

CardOS® V4.3B Re_Cert

Security Target
CardOS V4.3B Re_Cert with
Application for Digital Signature

Edition 11/2006

SIEMENS

Siemens AG
MED GS SEC
Charles-de-Gaulle-Str. 2

D-81737 Munich
Germany

Disclaimer of Liability

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcomed.

Subject to change without notice
© Siemens AG 2006

CardOS is a registered trademark of Siemens AG.

Contents

Document History

Version	Release Date	Changed Chapter(s)	Remarks	Author	Sent to Receiver on Date
0.01	11.09.06		First version	Ulrike Ludwig Siemens	T-Systems (Igor Furgel, Evaluator) on 11.09.06
0.02	16.10.06			Ulrike Ludwig Siemens	T-Systems (Igor Furgel, Evaluator) on 16.10.06
0.03	16.10.06		Changes proposed by ser_ase_siicnV43B-642P_v091.doc Deleted SHA-1 from chap. 6.1.4	Ulrike Ludwig Siemens	T-Systems (Igor Furgel, Evaluator) on 16.10.06
1.00	28.11.06		Changes proposed by Review_ST_10.pdf	Ulrike Ludwig Siemens	T-Systems, Igor Furgel, Evaluation, Klaus-Werner Schröder, Certification on 28.11.06

1 ST Introduction

1.1 ST Identification

Title:	Security Target CardOS V4.3B Re_Cert
Authors:	Siemens AG, Med GS ESY SEC
CC Version:	2.3 Final
General Status:	draft
Version Number:	1.0
Registration:	T-Systems-DSZ-CC-04181

The TOE can be based on the Infineon SLE66CX322P or SLE66CX642P as ICC platform.

1.2 ST Overview

The TOE defined by this Security Target is Software implementing a Secure Signature Creation Device (SSCD) basing on a Card residing Security Controller Chip, that allows to generate cryptographically strong Signatures over previously internally or externally calculated hash-values. The TOE is able to protect the secrecy of the internally generated and stored Signature Creation Data (SCD, i.e. secret key) and restricts the usage access to the authorised Signatory only.

This ST provides

- an introduction, see this section,
- the TOE description in section 2,
- the TOE security environment in section 3,
- the security objectives in section 4,
- the security and assurance requirements in section 5,
- the TOE summary specification (TSS) in section 6,
- the PP claim in section 7,
- the rationale in section 8 and
- the references in section 9

1.3 CC Conformance

This ST claims to be to CC Part 2 [9] extended, CC Part 3 [10] conformant, and EAL4 augmented.

The assurance level EAL4 within this ST is augmented by

- AVA_MSU.3 (Analysis and testing for insecure states) and
- AVA_VLA.4 (Highly resistant) as stated in [10].

The minimum strength level for the TOE security functions (TSF) is 'SOF high' (Strength of Functions High).

The ST does not claim any PP conformance but is derived from the SSCD-PP type 3 [16].

2 TOE Description

2.1 TOE Characteristics

The TOE is the software part of a secure signature-creation device (SSCD) 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 which can run on the security processor chip SLE66CX322P or SLE66CX642P from Infineon consists of i) configured software (OS and signature application) used to implement the secure signature-creation device (SSCD) and ii) the pertaining guidance documentation ‘User Guidance CardOS V4.3B Re_Cert ’ [21] and ‘Administrator Guidance CardOS V4.3B Re_Cert ’ [20].

The chip SLE66CX322P is certified for several production sites (e.g. Dresden in Germany (production line indicator ‘2’) and Corbeil Essonnes (called Altis) in France (production line indicator ‘5’)) (see German IT-Security Certificate [25] and Assurance Maintenance Reports [26] - [28].
The chip SLE66CX642P is certified for the production site Dresden (see German IT-Security Certificate [22], Infineon Smart Card IC (Security Controller) SLE66CX642P with RSA2048 m1485b16 from Infineon Technologies AG, Bonn, 12 August 2005).

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

(1) to generate the SCD and the correspondent signature-verification data (SVD) and
(2) to create qualified electronic signatures
    (a) after allowing for the data to be signed (DTBS) to be displayed correctly where the display function is provided by the TOE environment
    (b) using appropriate hash functions that are, according to [4], agreed as suitable for qualified electronic signatures
    (c) after appropriate authentication of the signatory by the TOE
    (d) using an appropriate cryptographic signature function that employs appropriate cryptographic parameters agreed as suitable according to [4].

The TOE implements the IT security functionality realised in software which is necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control. The interface for the user authentication is provided by the trusted TOE environment.

The TOE protects the SCD during the whole life cycle as to be solely used in the signature-creation process by the legitimate signatory. The TOE will be initialised for the signatory's use by

(1) generating a SCD/SVD pair
(2) personalisation for the signatory by means of the signatory’s reference authentication data (RAD).

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

The human interface for user authentication is implemented in the trusted TOE environment and used for the input of VAD for authentication by knowledge. The TOE holds RAD to check the provided VAD.

Figure 1 shows the ST scope from the structural perspective. The TOE comprises the operating system (OS), the SCD/SVD generation, SCD storage and use, and signature-creation functionality. The SCA and the CGA (and possibly other applications) are part of the immediate environment of the TOE. They communicate with the TOE in a trusted environment.

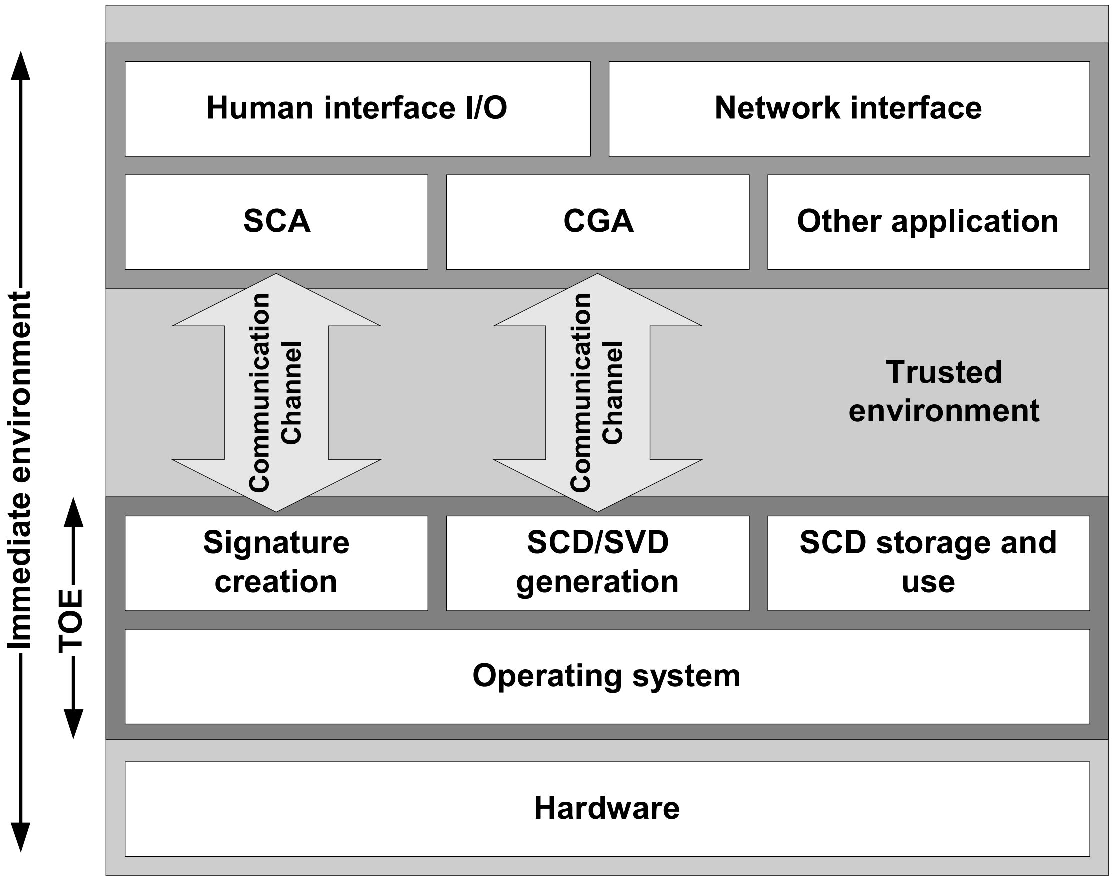

Figure 1: Scope of the SSCD, structural view

The physical interface of the TOE is provided by a connection according to ISO 7816 part 3 [12]. This interface is used to transmit an APDU command to the TOE and receive the corresponding response APDU from the TOE as specified in ISO 7816 part 4 [13] and part 8 [14].

The TOE life cycle is shown in Figure 2. Basically, it consists of a development phase and the operational phase.

This document refers to the operational phase which starts with personalisation including SCD/SVD generation. This phase represents installation, generation, and start-up in the CC terminology. The main functionality in the usage phase is signature-creation including all supporting functionality (e.g., SCD storage and SCD use).

After fabrication, the TOE is initialised and personalised for the signatory, i.e. the SCD/SVD key pair is generated and the RAD used for authentication of the signatory is imported.

The main functionality in the usage phase is signature-creation including supporting functionality like secure SCD storage and use. The TOE protects the SCD during the relevant life cycle phases. Only the legitimate signatory can use the SCD for signature-creation by means of user authentication and access control. The SVD corresponding to the signatory’s SCD will be included in the certificate of the signatory by the certificate-service provider (CSP).

The life cycle ends with the life cylce phase DEATH in which the SCD is permanently blocked.

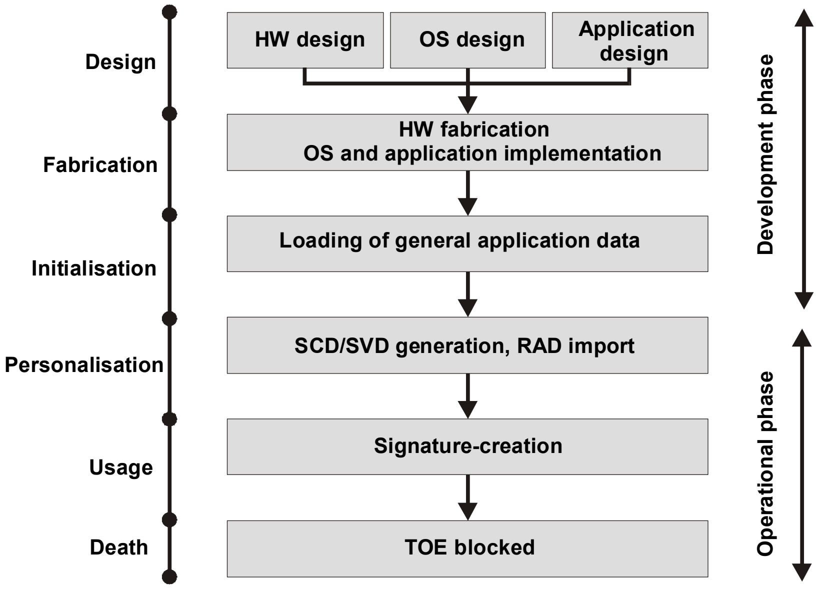

Figure 2: SSCD life cycle

2.2 CardOS V4.3B Features

As described in section 2.1, the TOE comprises the OS and the signature application. This subsection does not extend the TOE description but provides a more general overview of the OS identified as CardOS V4.3B.

CardOS V4.3B is a multifunctional smart card operating system (OS) supporting active and passive data protection. The operating system is designed to meet the most advanced security demands.

CardOS V4.3B complies with the ISO standard family ISO 7816 part 3, 4, 5, 8 and 9.

CardOS V4.3B with application SigG is designed to meet the requirements of the German Digital Signature Act ([2], [3]).

The versatile and feature rich operating system supports rapid application development on smart cards.

A patented scheme for initialisation/personalisation provides for cost efficient mass production by card manufacturers.

General features

- CardOS V4.3B runs on the Infineon SLE66 chip family. The SLE66CX322P and SLE66CX642P chips with embedded security controller for asymmetric cryptography and true random number generator have successfully been certified against the Common Criteria EAL5+ security requirements (see [25], [26], [27], [28] and [22]).
- Shielded against all presently known security attacks
- All commands are compliant with ISO 7816-4, -8 and –9 standards.
- PC/SC- compliance and CT-API

- Cleanly structured security architecture and key management
- Customer and application dependent configurability of card services and commands
- Extensibility of the operating system using loadable software components (packages)

File system

CardOS V4.3B offers a dynamic and flexible file system, protected by chip specific cryptographic mechanisms:

- Arbitrary number of files (EFs, DFs)
- Nesting of DFs limited by memory only
- Dynamic memory management aids in optimum usage of the available EEPROM
- Protection against EEPROM defects and power failures

Access control

- Up to 126 distinct programmer definable access rights
- Access rights may be combined with arbitrary Boolean expressions
- Any command or data object may be protected with an access condition scheme of its own
- All security tests and keys are stored as so-called basic security objects in the DF bodies (no reserved file IDs for key- or PIN files)
- Security structure may be refined incrementally after file creation without data loss

Cryptographic Services

- Implemented algorithms: RSA with 1024 up to 2048 bit key length (PKCS#1 padding), SHA-1, Triple-DES (CBC), DES (ECB, CBC), MAC, Retail-MAC
- Protection against Differential Fault Analysis (”Bellcore-Attack”)
- Protection of DES and RSA against SPA and DPA
- Support of ”Command Chaining” following ISO 7816-8
- Asymmetric key generation “on chip” using the onboard true random number generator
- Digital Signature functions “on chip”
- Connectivity to external Public Key certification services

Secure Messaging

- Compatible with ISO 7816-4
- may be defined for every command and every data object (files, keys) independently.

3 TOE Security Environment

This chapter defines the assets, subjects and threat agents used for the definition of the assumptions, threat and organisational security policies in the following subsections.

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.
3. DTBS and DTBS-representation: set of data, or its representation which is intended to be signed.
4. VAD: PIN, PUK (optional) and Transport-PIN code entered by the End User to perform authentication attempts.
5. RAD: Reference PIN, PUK (optional) and Transport-PIN code used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)[1]
6. Signature-creation function of the SSCD using the SCD: (The quality of the function must be maintained so that it can participate in the legal validity of electronic signatures)
7. Electronic signature: (Unforgeability of electronic signatures must be assured).

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 attack potential** and **knows no secrets**.

Application note:
Throughout this document and the evaluation documentation the following synonyms will be used:

Subjects and Threat agents defined in the PP [16]	Synonyms used in this evaluation
S.User	User
S.Admin	Administrator
S.Signatory	Signatory
S.OFFCARD	Attacker

[1] The TOE does not support biometric authentication. Therefore the authors changed this asset definition by deleting the term “biometric authentication references”, see also section 3 [16].

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 in a trustworthy environment. The SCA generates and sends the DTBS-representation of data the Signatory wishes to sign in a form appropriate for signing by the TOE.

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 attacker can store, copy, the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE.

T.SCD_Derive *Derive the signature-creation data*

An attacker derives the SCD from public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.

T.Sig_Forgery *Forgery of the electronic signature*

An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.Sig_Repud *Repudiation of signatures*

If an attacker can successfully threaten any of the assets, then the non repudiation of the electronic signature is compromised. This results in the signatory being 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.

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 certificate 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 section has been taken from [16] 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.

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 in the TOE.

OT.Tamper_Resistance *Tamper resistance*

The TOE prevents or resists physical tampering with specified system devices and components.

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 negligibly low.

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 can not 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,
(c) the advanced signature of the CSP.

OE.SVD_Auth_CGA *CGA ensures the integrity and authenticity of the SVD*

The CGA ensures the integrity and authenticity of the SVD received from the TOE. The CGA ensures the correspondence between the SVD received from the TOE 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
(c) attaches the signature produced by the TOE to the data or provides it separately.

OE.SCA_Trusted_Env *Trusted environment*

The environment of the TOE protects

(a) the confidentiality and integrity of the VAD entered by the user via the SCA human interface and sent to the TOE and
(b) the integrity of the DTBS sent by the SCA to the TOE.

5 IT Security Requirements

This chapter provides 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” (except FPT_EMSEC.1 which is explicitly stated) are drawn from Common Criteria part 2 [9]. Some security functional requirements represent extensions to [9]. Operations for assignment, selection and refinement have been made. Operations are identified by an underlined italic font, e.g. *SHA-1*.

The TOE security assurance requirements given in section 5.2 “TOE Security Assurance Requirement” are drawn from the security assurance components from Common Criteria part 3 [10].

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.

The original text for the elements taken from CC part 2 [9] for each in this ST performed operation is additionally stated in footnotes.

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 *RSA*[2] and specified cryptographic key sizes *1024 up to 2048 bit in 8 bit steps*[3] that meet the following:

Geeignete Algorithmen [4][4].

5.1.1.2 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 The TSF shall perform *digital signature-generation*[5] in accordance with specified cryptographic algorithms *RSA*[6] and cryptographic key sizes *1024 up to 2048 bit in 8 bit steps*[7] that meet the following:

(1) *RSA and PKCS#1, v. 1.5, BT 1 [6]*

(2) *Geeignete Algorithmen [4]*[8]

[2] [assignment: *cryptographic key generation algorithm*]
[3] [assignment: *cryptographic key sizes*]
[4] [assignment: *list of standards*]
[5] [assignment: *list of cryptographic operations*]
[6] [assignment: *cryptographic algorithm*]
[7] [assignment: *cryptographic key sizes*]
[8] [assignment: *list of standards*]

5.1.2 User data protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the _Signature-creation SFP_[9] on _signing of DTBS-representation by Signatory_[10].

5.1.2.2 Security attribute based access control (FDP_ACF.1)

The following table lists the subjects and objects controlled under the Signature-creation SFP and the SFP-relevant security attributes:

Subject or object the attribute is associated with	Attribute	Status
General attribute		
User	Role	Administrator, Signatory
Signature-creation attribute		
SCD	SCD operational	no, yes

FDP_ACF.1.1 The TSF shall enforce the _Signature-creation SFP_[11] to objects based on the following: _General attribute and Signature creation attribute_[12].

Application Note: This element is changed as a result of Interpretation 103.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

A User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures with the SCD for DTBS sent by the SCA if the security attribute "SCD operational" is set to "yes".[13]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: _none_[14].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rule:

(a) _A User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures with the SCD for DTBS sent by the SCA if the security attribute "SCD operational" is set to "no"._

(b) _A User with the security attribute "role" set to "Administrator" is not allowed to create electronic signatures with the SCD._[15]

[9] [assignment: *access control SFP*]

[10] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

[11] [assignment: *access control SFP*]

[12] [assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

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

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

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

5.1.2.3 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 *deallocation of the resource from*[16] the following objects: *SCD, VAD, RAD*[17].

5.1.2.4 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*[18] on all objects, based on the following attributes: *integrity checked persistent stored data*[19].

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*[20].

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 (Transport PIN) and 3 up to 15 (PIN and PUK)*[21] unsuccessful authentication attempts occur related to *consecutive failed authentication attempts*[22].

Application Note: This element is changed as a result of Interpretation 111.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *block RAD*[23].

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*[24].

[16] [selection: *allocation of the resource to, deallocation of the resource from*]
[17] [assignment: *list of objects*]
[18] [assignment: *integrity errors*]
[19] [assignment: *user data attributes*]
[20] [assignment: *action to be taken*]
[21] [selection: [assignment: *positive integer number*], *"an administrator configurable positive integer within*[assignment: *range of acceptable values*]*"*]
[22] [assignment: *list of authentication events*]
[23] [assignment: *list of actions*]
[24] [assignment: *list of security attributes*]

5.1.3.3 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow *the identification of the user*[25] on behalf of the user to be performed before the user is authenticated.

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

5.1.3.4 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow *no TSF-mediated action*[26] 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*[27] the *signature-creation function*[28] to *Signatory*[29].

5.1.4.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the *Signature-creation SFP*[30] to restrict the ability to *modify*[31] the security attributes *SCD operational*[32] to *Signatory*[33].

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.

[25] [assignment: *list of TSF mediated actions*]
[26] [assignment: *list of TSF-mediated actions*]
[27] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
[28] [assignment: *list of functions*]
[29] [assignment: *the authorised identified roles*]
[30] [assignment: access control SFP, information flow control SFP]
[31] [selection: *change_default, query, modify, delete,* [assignment: *other operations*]]
[32] [assignment: *list of security attributes*]
[33] [assignment: *the authorised identified roles*]

5.1.4.4 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the *Signature-creation SFP*[34] to provide *restrictive*[35] default values for security attributes that are used to enforce the SFP.

Application Note: This element is changed as a result of Interpretations 201 and 202.
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*[36] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.5 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to *modify or unblock*[37] the *RAD*[38] to *Signatory*[39].

5.1.4.6 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

(1) *Modifying the SCD operational attribute*

(2) *Creation of RAD*

(3) *Modifying or unblocking of RAD*[40].

.

5.1.4.7 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles

1. *Administrator*
2. *Signatory*[41].

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 and before the use of the random number generator*[42] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

[34] [assignment: *access control SFP, information flow control SFP*]
[35] [selection: *choose one of: restrictive, permissive,* [assignment: *other property*]]
[36] [assignment: *the authorised identified roles*]
[37] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[38] [assignment: *list of TSF data*]
[39] [assignment: *the authorised identified roles*]
[40] [assignment: *list of security management functions to be provided by the TSF*]
[41] [assignment: *the authorised identified roles*]
[42] [selection: *during initial start-up, periodically during normal operation, at the request of an authorised user,*assignment [*other conditions*]]

5.1.5.2 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit *information about IC power consumption*[43] in excess of *unintelligible limits*[44] enabling access to *RAD and SCD*[45].

FPT_EMSEC.1.2 The TSF shall ensure *S.User and S.OFFCARD*[46] are unable to use the following interface *physical contacts of the underlying IC hardware*[47] to gain access to *RAD and SCD*[48].

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:

(1) *Failures during random number generation*

(2) *Failures during cryptographic operations*

(3) *Memory failures during TOE execution*[49].

Application Note: Out of range failures of temperature, clock and voltage sensors are detected by the underlying hardware, which preserves a secure state.

5.1.5.4 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist *tampering scenarios by intrusion of physical or mechanical means*[50] to the *underlying IC hardware*[51] by responding automatically such that the TSP is not violated.

[43] [assignment: *types of emissions*]
[44] [assignment: *specified limits*]
[45] [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*]
[46] [assignment: *type of users*]
[47] [assignment: *type of connection*]
[48] [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*]
[49] [assignment: *list of types of failures in the TSF*]
[50] [assignment: *physical tampering scenarios*]
[51] [assignment: *list of TSF devices/elements*]

5.2 TOE Security Assurance Requirements

Table 5.1 Assurance Requirements: EAL4+ (the augmentation is done within the Family AVA_MSU and AVA_VLA, typographically indicated by the bold face setting).

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**

These Security Assurance Requirements are taken from Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Requirements, Version 2.3 [10]. No additional operations are performed on these Assurance Requirements.

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 *IT environment*[52] shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *qualified certificate*[53] that meets the following:

Geeignete Algorithmen [4][54].

5.3.1.2 Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/ CGA The *IT environment*[52] shall perform *import the SVD*[55] in accordance with a specified cryptographic key access method *import in a trusted environment*[56] that meets the following: *none*[57].

5.3.2 Signature creation application (SCA)

5.3.2.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ SCA Hash The *IT environment*[52] shall perform *hashing the DTBS*[58] in accordance with specified cryptographic algorithms *SHA-1 up to SHA-512*[59]*, RIPEMD-160*[60] and cryptographic key sizes *none*[61] that meet the following: *Secure Hash Standard [7]*[62]*and RIPEMD-160 [23]*[63].

[52] Term “TSF” refined according to Final Interpretation 058
[53] [assignment: *cryptographic key distribution method*]
[54] [assignment: *list of standards*]
[55] [assignment: *type of cryptographic key access*]
[56] [assignment: *cryptographic key access method*]
[57] [assignment: *list of standards*]
[58] [assignment: l*ist of cryptographic operations*]
[59] [assignment: *cryptographic algorithm*]
[60] [assignment: *cryptographic algorithm*]
[61] [assignment: *cryptographic key sizes*]
[62] [assignment: *list of standards*]
[63] [assignment: *list of standards*]

5.4 Security Requirements for the Non-IT Environment

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

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

R.TRP_Environment *Trusted environment for the TOE and local user*

The environment, in which the TOE is used, shall keep confidentiality and integrity of the VAD and integrity of the DTBS.

R.CGA_Environment *Trusted environment of the CGA*

The CGA environment ensures the integrity and authenticity of the SVD received from the TOE and used for the qualified certificate of the signatory.

6 TOE Summary Specification

6.1 TOE Security Functions

This section provides a description of the TOE security functions (TSF) which instantiated the TSFR of section 5.1.

6.1.1 SF1 User Identification and Authentication

This TSF is responsible for the identification and authentication of the Administrator and Signatory (FMT_SMR.1).

This implies that the TOE allows identification of the User before the authentication takes place (FIA_UAU.1). The TOE does not allow the execution of any TSF-mediated actions before the user is identified (FIA_UID.1), authenticated and associated to one of the two roles.

The Administrator is successfully implicitly authenticated within the lifecycle phase Administration. This lifecycle starts after changing the original Start_Key with a confidential command sequence received by the TOE software developer and then switching the TOE's life cycle from the Manufacturing to the Aministration phase which requires the knowledge of the Start_Key and ends by changing into the lifecycle Operational.

Within the lifecycle Operational, the Signatory is successfully authenticated after transmitting the correct VAD to the TOE, e.g. the user has to transmit the correct PIN to be associated with the role Signatory. The following types of VAD/RAD are defined for the TOE:

- PIN to authenticate the user as Signatory
- PUK (optional) to unblock the blocked PIN (and Transport-PIN) by the Signatory
- Transport-PIN for the first setting of the PIN (and PUK). The Transport-PIN is used to secure the TOE delivery process. After entering the correct Transport-PIN the Signatory has to set his individual PIN (and PUK) value. Thereafter the PIN (and PUK) will be unblocked by the TOE. If the PUK value is created by the Administrator, the PUK is already usable (unblocked) after card (and PUK-letter) delivery to the Signatory.

If the TOE is configured to be used for unlimited mass signature generation, it can also contain two different PINs, whose correct values both have to be presented and verified successfully before signing.

The TOE will check that the provided VAD is equal to the stored and individual value of the corresponding RAD (FIA_ATD.1). The number of unsuccessful consecutive authentication attempts by the user is limited to a value depending on the RAD length. Thereafter SF1 will block the RAD (FIA_AFL.1).

The ability to modify or unblock the RAD is restricted to the Signatory (FMT_MTD.1). The Signatory has to provide

- the correct PIN to change resp. modify the PIN
- the correct PUK (optional) to change resp. modify the PUK and to unblock the blocked PIN (and Transport-PIN)
- the correct Transport-PIN to unblock the PIN (and PUK) before the first use (FMT_SMF.1.1 (3)).

The ability to initially create the Transport-PIN is restricted to the Administrator. The individual PIN (and PUK) value is set by the Signatory after successful authentication with the Transport-PIN (FMT_SMF.1.1 (2)).
The PUK value might also be created by the Administrator and can in this case also be used to unblock the Transport-PIN, if it has been blocked by too many unsuccessful authentication attempts. If, however, the Transport-PIN is blocked after its successful use, it cannot be unblocked anymore.

The successful authentication with the Transport-PIN which is possible only once, also changes the value of the attribute “SCD operational” from “no” to “yes”, see also SF2 Access Control.
It is important that an attacker can not guess the RAD values by measuring or probing physical observables like TOE power consumption or electromagnetic radiation (FPT_EMSEC.1). Further protection functionality is covered by SF5 Protection.

6.1.2 SF2 Access Control

This TSF is responsible for the realisation of Signature-creation SFP. The security attributes used for these policies are stated in 5.1.2.2. Generally, this access control policy is assigned to user roles. The identification, authentication and association of users to roles is realised by SF1 User Identification and Authentication (FMT_SMR.1).

SF2 controls the access to the signature creation functionality of the TOE. The TOE allows the generation of a signature if and only if (FDP_ACC.1, FDP_ACF.1.1 and FMT_MOF.1):

- the security attribute “SCD operational” is set to “yes”.
- the signature request is sent by an authorised signatory, see also SF1 User Identification and Authentication.

After the generation of the SCD/SVD key pair, the security attribute “SCD operational” is set to “no” (FMT_MSA.3) by the Administrator. The Administrator is able to set other default values. Thereafter only the Signatory is allowed to modify the security attribute “SCD operational” (FMT_MSA.1 and FMT_SMF.1 (1)). The security attribute “SCD operational” is set to “yes” by the TOE after the Signatory has successfully authenticated himself with the Transport-PIN and unblocked the PIN, see also SF1 User Identification and Authentication.

Only the signatory is allowed to modify or unblock the RAD in form of the PIN (FMT_MTD.1 and FMT_SMF.1(3)), see also SF1 User Identification and Authentication.
The Transport-PIN cannot be modified and can be used only once. If the value of the optional PUK is initialized by the Administrator the Transport-PIN can be unblocked, if it has been blocked by too many unsuccessful authentication attempts. If, however, the Transport-PIN is blocked after its successful use, it cannot be unblocked anymore. If the Transport-PIN is initialized by the signatory it can never be unblocked. The optional PUK can always be modified but unblocked never (if initialized by Administrator) or only once (by Transport-PIN).

The mass signature module with two signatory PINs can only be used for the generation of mass signatures, if both signatorys are present to enter their respective PINs. The personal PIN (and PUK) of each signatory can only be set by each signatory after the corresponding Transport PIN entry. The Transport-PINs cannot be modified or unblocked and can be used only once. Each signatory is allowed to modify or unblock the RAD in form of his personal PIN.

6.1.3 SF3 SCD/SVD Pair Generation

This TSF is responsible for the correct generation of the SCD/SVD key pair which is used by the Signatory to create signatures.

The TOE generates RSA signature key pairs with a module length of 1024 up to 2048 bit in 8 bit steps. The key pairs fulfil the corresponding requirements of [4] for RSA key pairs (FMT_MSA.2 and FCS_CKM.1).For the generation of primes used for the key pair a GCD (Greatest Common Devisor) test and enough rounds of the Rabin Miller Test are performed. The TOE uses the random number generator of the underlying hardware for the generation of the SCD/SVD key pair. The generation is furthermore protected against electromagnetic emanation, SPA and timing attacks (FPT_EMSEC.1), see also SF5 Protection.

6.1.4 SF4 Signature Creation

This TSF is responsible for signature creation using the SCD of the Signatory. Before a signature is generated by the TOE, the Signatory has to be authenticated successfully, see SF1 User Identification and Authentication.
Before mass signatures, which require the entry of two PINs, are generated by the TOE, both Signatorys have to be authenticated successfully, see SF1 User Identification and Authentication.

Technically, SF4 generates RSA signatures for hash values with PKCS#1 padding (block type 1) using the SCD of the Signatory. The signatures generated by this TSF meet the following standards:

[6] RSA Laboratories, PKCS #1: RSA Encryption Standard, An RSA Laboratories Technical Note Version 1.5, Revised November 1st, 1993

[7] FIPS PUB 180-2: Secure Hash Standard, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2002, August 1,

[4] Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV, Veröffentlicht am 23. März 2006 im Bundesanzeiger Nr. 58, S. 1913-1915, Vom 2. Januar 2006, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

The TSF supports RSA key length form 1024 to 2048 bit in 8 bit steps (FMT_MSA.2 and FCS_COP.1).

The hash value used for the signature creation is

- calculated over the DTBS in the TOE IT environment and sent to the TOE or
- completely calculated by means of SF4 for DTBS sent to the TOE (only possible with SHA-1)

under the control of the Signature-creation SFP, see SF2 Access Control.

The signature creation process is implemented in a way which does not disclose the SCD by measuring the IC power consumption of the TOE during the signature calculation (FPT_EMSEC.1). It is furthermore not possible to gain unauthorised access to the SCD using the physical contacts of the underlying hardware.
The certificates of the SLE66CX322P and SLE66CX642P (Common Criteria level EAL 5+) cover also the RSA 2048 bit functionality for signature creation (see [25] and [22]).

6.1.5 SF5 Protection

This TSF is responsible for the protection of the TSF, TSF data and user data.

The TOE runs a suite of tests to demonstrate the correct operation of the underlying platform (FPT_AMT.1). The following tests are performed by the TOE during initial start-up:

- After erasure of RAM and XRAM, the state of the EEPROM is tested and, if not yet initialised, this will be done.
- The EEPROM heap is checked for consistency. If it is not valid the TOE will preserve a secure state (lifecycle DEATH).
- The backup buffer will be checked and its data will be restored to EEPROM, if they were saved because of a command interruption.

The TOE will furthermore run tests during the generation of the SCD/SVD key pair (SF3 SCD/SVD Pair Generation) and during signature creation (SF4 Signature Creation). For tests during signature creation the code of the Infineon RSA2048 Library (Crypto Library for SLE 66CX322P and SLE66CX642P) is used. The correct operation of SF3 is demonstrated by performing the following checks:

- The TOEs lifecycle phase is checked. Only Administrator can perform SCD/SVD pair generation.

- Before command execution the correct functioning of the Random Number Generator (RNG) and of the Active Shield is tested.
- All command parameters are checked for consistency.
- Access rights are checked.
- The ‘generation allowed bit’ is checked (key pair generation allowed only once).

If a critical failure occurs during these tests, the TOE will preserve a secure state (FPT_FLS.1). This comprises the following types of failures:

- Random number generation failures, e.g during key pair generation
- Cryptographic operation failures, e.g. during signature creation
- Memory failures during TOE execution
- Out of range failures of temperature, clock and voltage sensors

In case the underlying IC hardware (environment) has detected a physical and mechanical tampering attempt, the TOE will react and responds automatically in form of a continuously generated reset and the TOE functionality will be blocked (FPT_PHP.3).

SF5 actively destructs temporarily stored SCD, VAD and RAD immediately after their use - as soon as these data are dispensable (FDP_RIP.1).
The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data":

- SCD
- RAD
- SVD

If the integrity of SCD, RAD or SVD is violated, the TOE will prohibit the usage of the altered data and inform the Signatory about the integrity error by means of an error code (FDP_SDI.2/ Persistent).

6.2 Assurance measures

TOE implements the assurance measures exactly drawn from the assurance requirements referenced in section 5.2. Naming of each assurance measure is derived from the name of the according assurance requirement. The TOE implements the following assurance measures by providing the appropriate documents and activities:

Table 6.1-: Assurance Measures

Assurance Measures	Remarks
ACM_AUT.1M	configuration management documentation
ACM_CAP.4M	configuration management documentation
ACM_SCP.2M	configuration management documentation
ADO_DEL.2M	parts of delivery documentation
ADO_IGS.1M	secure installation, generation and start-up procedures
ADV_FSP.2M	fully defined external interfaces
ADV_HLD.2M	high-level design (security enforcing)
ADV_IMP.1M	parts of the implementation representation
ADV_LLD.1M	low-level design
ADV_RCR.1M	correspondence analysis between TOE summary specification and fully defined external interfaces, functional specification and high-level design, high-level design and low-level design, low-level design and implementation representation
ADV_SPM.1M	informal security policy model
AGD_ADM.1M	administrator guidance
AGD_USR.1M	user guidance
ALC_DVS.1M	development security documentation
ALC_LCD.1M	life-cycle description
ALC_TAT.1M	description of Tools and techniques
ATE_COV.2M	test coverage analysis
ATE_DPT.1M	depth of testing analysis
ATE_FUN.1M	test documentation
ATE_IND.2M	the TOE suitable for testing
AVA_MSU.3M	administrator and user guidance, misuse analysis
AVA_SOF.1M	strength of function claims analysis
AVA_VLA.4M	vulnerability assessment

6.3 SOF Claim

According to the CEM [11] a Security Target shall identify all mechanisms which can be assessedaccording to the assurance requirement AVA_SOF.1.

The following table lists the TSF, the corresponding SOF claim if applicable and a reference to the permutational or probabilistic mechanisms.

Table 6.1-: SOF claim

TSF	SOF Claim	Probabilistic or permutational mechanisms
SF1 User Identification and Authentication	SOF-high	PIN, PUK, Transport-PIN
SF2 Access Control	–	–
SF3 SCD/SVD Pair Generation	SOF-high	Random number generator, Prime number test
SF4 Signature Creation	SOF-high[64]	Signature Creation
SF5 Protection	–	–

[64] This TSF is claimed to be SOF-high because it uses mechanisms approved by [4]. The scope of the evaluation is to show the functional correctness of the implementation of these mechanisms. The cryptographic strength is not assessed in the scope of the evaluation.

7 PP Claims

7.1 PP Reference

The Security Target does not claim any PP conformance.

7.2 PP Refinements

The Security Target does not state any PP refinements, see also section 7.1.

7.3 PP Additions

The Security Target does not state any PP additions, see also section 7.1.

8 Rationale

8.1 Security Objectives Rationale

8.1.1 Security Objectives Coverage

Table 8.1-: Security Environment to Security Objectives Mapping

Threats - Assumptions - Policies / Security objectives	OT.EMSEC_Design	OT.lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_Resistance	OT.SCD_Unique	OT.Sigy_SigF	OT.Sig_Secure	OE.CGA_Qcert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend	OE.SCA_Trusted_env
T.Hack_Phys	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	
T.Sig_Repud	x	x	x	x	x	x	x	x	x	x		x	x
A.CGA									x	x			
A.SCA												x	x
P.CSP_Qcert				x					x				
P.Qsign							x	x	x			x	
P.Sigy_SSCD			x			x	x						

8.1.2 Security Objectives Sufficiency

8.1.2.1 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 and 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 ensures 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, OT.SCD_Unique ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature and by OT.SCD_Secrecy which preserves the secrecy of the SCD.

8.1.2.2 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_Resistance counters the threat T.Hack_Phys by resisting tamper attacks detected by the underlying hardware.

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 then does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The TOE IT environment addresses T.DTBS_Forgery by means of OE.SCA_Data_Intend and OE.SCA_Trusted_Env.

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 or 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) 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. OE.SCA_Trusted_Env 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 (Data intended to be signed), OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OE.SVD_Auth_CGA (CGA ensures the integrity and authenticity of the SVD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), 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 ensures that the methods used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation are appropriate for the cryptographic methods employed to generate the electronic signature. The combination of OE.CGA_QCert,

OT.SCD_SVD_Corresp 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), OE.SVD_Auth_CGA (CGA ensures the integrity and authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signature-creation data), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_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 (Data intended to be signed) and OE.SCA_Trusted_Env (Integrity of the DTBS-representation).
OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert and OE.SVD_Auth_CGA ensure the integrity and authenticity of the SVD.
OE.CGA_Qcert, OT.SCD_SVD_Corresp and OE.SVD_Auth_CGA ensure that the SVD in the certificate corresponds 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_Secrecy, 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 OE.SCA_Trusted_Env 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.SCD_SVD_Corresp by ensuring the correspondence between the SVD and SCD stored in the TOE. The export of the SVD is addressed by OE.SVD_Auth_CGA. The trusted environment of the CGA ensures the integrity and authenticity of the SVD send by the TOE. The CGA furthermore ensures the correspondence between the SVD received by the CGA and the SVD identified in the qualified certificate.

8.1.2.3 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. The confidentiality and integrity of the VAD as well as the integrity of the DTBS sent to the TOE is addressed by OE.SCA_Trusted_Env (Trusted environment of SCA) which provides a trusted environment.

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 ensures the integrity and authenticity of the SVD) which ensures the integrity and authenticity of the SVD received from the TOE.

8.2 Security Requirements Rationale

8.2.1 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.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_Resistance	OT.SCD_Unique	OT.Sigy_SigF	OT.Sig_Secure
FCS_CKM.1				x		x		
FCS_COP.1								x
FDP_ACC.1							x	
FDP_ACF.1							x	
FDP_RIP.1			x				x	
FDP_SDI.2/Persistent			x	x			x	x
FIA_AFL.1							x	
FIA_ATD.1							x	
FIA_UAU.1							x	
FIA_UID.1							x	
FMT_MOF.1			x				x	
FMT_MSA.1			x				x	
FMT_MSA.2							x	
FMT_MSA.3			x				x	
FMT_MTD.1							x	
FMT_SMF.1[65]			x				x	
FMT_SMR.1			x				x	
FPT_AMT.1		x	x					x
FPT_EMSEC.1	x							
FPT_FLS.1			x		x			
FPT_PHP.3					x			

[65] See the note in section 5.1.4.6.

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	OE.SCA_Trusted_Env
FCS_CKM.2/CGA	x				
FCS_CKM.3/CGA	x				
FCS_COP.1/SCA HASH			x		
R.Sigy_Name	x				
R.TRP_Environment		x			x
R.CGA_Environment				x	

Table 8.4: Assurances Requirement to Security Objective Mapping

Objectives	Security Assurance Requirements
OT.Lifecycle_Security	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1,ADO_DEL.2, ADO_IGS.1
OT.SCD_Secrecy	ADO_IGS.1, ADV_IMP.1, AGD_ADM.1, AVA_SOF.1, AVA_VLA.4
OT.Sigy_SigF	AVA_MSU.3, AVA_SOF.1, AVA_VLA.4
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

8.2.2 Security Requirements Sufficiency

8.2.2.1 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.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 function FPT_AMT.1 provides failure detection throughout the lifecycle.

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 assurance requirements ADO_IGS and AGD_ADM which ensure that only authorised users can initialise the TOE and create the SCD. The authentication and access management functions specified by FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1 and FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.

The security functions specified by FDP_RIP.1 ensure that residual information on SCD is destroyed after the SCD has been used for signature creation. 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 as to retain the correspondence.

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.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, FDP_ACF.1, FMT_MTD.1, FMT_SMF and FMT_SMR.1 ensure that the signature process is restricted to the signatory.
The security functions specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, and FMT_MSA.3 ensure that the access to the signature generation functions remain under the sole control of the signatory, as well as FMT_MSA.1 provides that the control of corresponding security attributes is under signatory's control.
FDP_SDI.2/Persistent ensures the integrity of stored data.
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 which ensures the cryptographic robustness of the signature algorithms and by AVA_VLA.4 by requesting that these resist attacks with a high attack potential. The security function specified by FPT_AMT.1 ensures that the security functions are performing correctly. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE.

OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to react on (and therefore resist) physical attacks. In case a tampered HW is detected by the underlying hardware the TOE switches into a secure state by FPT_FLS.1.

8.2.2.2 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. The requirement R.Sigy_Name ensures that the identity of the certificate requesting person is verified and that it holds the SSCD which implements the SCD corresponding to the SVD to be included in the qualified certificate.

OE.HI_VAD (Protection of the VAD) The non-IT requirement R.TRP_Environment covers also the confidentiality and integrity of the VAD of the TOE.

OE.SCA_Data_Intend (Data intended to be signed) is covered by FCS_COP.1/SCA HASH that ensures that the hashing function used by the SCA corresponds to the approved algorithms.

OE.SVD_Auth_CGA (CGA ensures the integrity and authenticity of the SVD) is covered by the non-IT requirement R.CGA_Environment that ensures that the SVD used for the qualified certificate of the signatory corresponds to the SVD received from the TOE by means of a trusted environment.

OE.SCA_Trusted_Env (Trusted environment) is coverted by the non-IT requirement R.TRP_Environment, which ensures the confidentiality and integrity of the VAD and the integrity of the DTBS.

8.3 Dependency Rationale

8.3.1 Functional and Assurance Requirements Dependencies

The assurance requirements dependencies for the TOE are completely fulfilled. The functional requirements dependencies for the TOE and the TOE environment are not completely fulfilled (see section 6.4.2 for justification).

Table 8.5 Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FCS_CKM.1	FCS_COP.1, FMT_MSA.2, unsupported dependencies, see sub-section 8.3.2 for justification
FCS_COP.1/	FCS_CKM.1, FMT_MSA.2, unsupported dependencies, see sub-section 8.3.2 for justification
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
FIA_AFL.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1[66]
FMT_MSA.1	FDP_ACC.1, FMT_SMF.1[66], FMT_SMR.1
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1, FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1[66]
FMT_SMR.1	FIA_UID.1
FPT_FLS.1	ADV_SPM.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

[66] See the note in section 5.1.4.6.

Requirement	Dependencies
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 (GGA)	
FCS_CKM.2/CGA	unsupported dependencies, see sub-section 8.3.2 for justification
FCS_CKM.3/CGA	unsupported dependencies, see sub-section 8.3.2 for justification
Functional Requirements for Signature creation application (SCA)	
FCS_COP.1/ SCA HASH	Unsupported dependencies, see sub-section 8.3.2 for justification

8.3.2 Justification of Unsupported Dependencies

The following tables includes the unsupported dependencies and the corresponding justification.

Requirement	Unsupported dependencies
FCS_CKM.1	It is not possible to delete the SCD (FCS_CKM.4) by means of the TSF. But the TOE blocks the SCD after the defined number of consecutive authentication attempts or if the signature application is terminated. When the SCD is blocked, it is not possible to unblock, use or readout the SCD.
FCS_COP.1	FCS_CKM.4 is not supported by the TOE, see argumentation for FCS_CKM.1.
FCS_CKM.2/ CGA	The CGA generates qualified electronic certificates including the SVD imported from the TOE. The requirement 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 out of scope for this ST.
FCS_CKM.3/ CGA	The CGA imports SVD in a trusted environment. The requirement 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 out of scope for 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.

8.3.3 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 externally 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.

8.3.3.1 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 to 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.

8.4 Security Requirements Grounding in Objectives

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

Table 8.6 : Assurance Requirement to Security Objective Mapping

Requirement	Security Objectives
Security Assurance Requirements	
ACM_AUT.1	EAL 4
ACM_CAP.4	EAL 4
ACM_SCP.2	EAL 4
ADO_DEL.2	EAL 4
ADO_IGS.1	EAL 4
ADV_FSP.2	EAL 4
ADV_HLD.2	EAL 4
ADV_IMP.1	EAL 4
ADV_LLD.1	EAL 4
ADV_RCR.1	EAL 4
ADV_SPM.1	EAL 4
AGD_ADM.1	EAL 4
AGD_USR.1	EAL 4
ALC_DVS.1	EAL4, OT.Lifecycle_Security
ALC_LCD.1	EAL4, OT.Lifecycle_Security
ALC_TAT.1	EAL4, OT.Lifecycle_Security
ATE_COV.2	EAL 4
ATE_DPT.1	EAL 4
ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_MSU.3	OT.Sigy_SigF
AVA_SOF.1	EAL 4, OT.SCD_Secrecy, OT.Sigy_SigF
AVA_VLA.4	OT.SCD_Secrecy, OT.Sig_Secure,
Security Objectives for the Environment	
R.Administrator_Guide	AGD_ADM.1
R.Sigy_Guide	AGD_USR.1
R.Sigy_Name	OE.CGA_Qcert
R.TRP_Environment	AGD_ADM.1, AGD_USR.1
R.CGA_Environment	AGD_ADM.1

8.5 TOE Summary Specification Rationale

8.5.1 Security Function Coverage

This chapter covers the mapping between TSFR and TSF.

Table 8.7 : TOE Security Requirement to TOE Security Function Mapping

TOE Security Functional Requirement / TOESecurity Function	SF1 User Identification and Authentication	SF2 Access Control	SF3 SCD/SVD Pair Generation	SF4 Signature Creation	SF5 Protection
FCS_CKM.1			x		
FCS_COP.1				x	
FDP_ACC.1		x			
FDP_ACF.1		x			
FDP_RIP.1					x
FDP_SDI.2/Persistent					x
FIA_AFL.1	x				
FIA_ATD.1	x				
FIA_UAU.1	x				
FIA_UID.1	x				
FMT_MOF.1		x			
FMT_MSA.1		x			
FMT_MSA.2			x	x	
FMT_MSA.3		x			
FMT_MTD.1	x	x			
FMT_SMF.1[67]	x	x			
FMT_SMR.1	x	x			
FPT_AMT.1					x
FPT_EMSEC.1	x		x	x	
FPT_FLS.1					x
FPT_PHP.3					x

8.5.2 TOE Security Function Sufficiency

Each TSFR is implemented by at least one TSF. How and whether the TSF actually implement the TSFR is described in section 6.1.

[67] See the note in section 5.1.4.6.

8.5.3 Assurance Measures Rationale

Each TOE security assurance requirement is implemented by exactly one assurance measure. The content and application of these assurance measures exactly accord with the assurance components of CC part 3 [10] with the same identifier, respectively, and CEM [11].

Table 8.8: Mapping TOE Assurance Requirements to TOE Assurance Measures

TOE Security Assurance Requirements	TOE Assurance Measures
ACM_AUT.1	ACM_AUT.1M
ACM_CAP.4	ACM_CAP.4M
ACM_SCP.2	ACM_SCP.2M
ADO_DEL.2	ADO_DEL.2M
ADO_IGS.1	ADO_IGS.1M
ADV_FSP.2	ADV_FSP.2M
ADV_HLD.2	ADV_HLD.2M
ADV_IMP.1	ADV_IMP.1M
ADV_LLD.1	ADV_LLD.1M
ADV_RCR.1	ADV_RCR.1M
ADV_SPM.1	ADV_SPM.1M
AGD_ADM.1	AGD_ADM.1M
AGD_USR.1	AGD_USR.1M
ALC_DVS.1	ALC_DVS.1M
ALC_LCD.1	ALC_LCD.1M
ALC_TAT.1	ALC_TAT.1M
ATE_COV.2	ATE_COV.2M
ATE_DPT.1	ATE_DPT.1M
ATE_FUN.1	ATE_FUN.1M
ATE_IND.2	ATE_IND.2M
AVA_MSU.3	AVA_MSU.3M
AVA_SOF.1	AVA_SOF.1M
AVA_VLA.4	AVA_VLA.4M

8.5.4 Mutual Supportiveness of the Security Functions

The supportiveness of the TSF is already considered in the description of the TSF in section 6 by using references. The following table summarises the mutual supportiveness between the TSF.

Table 8.9: Mutual Supportiveness of the Security Functions

TSF	Supportiveness of the Security Functions
SF1 User Identification and Authentication	The TSF is furthermore supported by SF5 to ensure that the RAD can not be easily guessed by measurement of power consumption or electromagnetic radiation.
SF2 Access Control	The TSF is supported by SF1 which is responsible for the user identification and authentication before security attributes can be accessed.
SF3 SCD/SVD Pair Generation	SF5 ensures that the SCD/SVD generation is protected against electromagnetic emanation, SPA and timing attacks.
SF4 Signature Creation	Before this TSF can be used for signature creation, SF1 is responsible for the signators identification and authentication before SF2 allows the access to the SCD. SF5 ensures that the signature generation is protected against electromagnetic emanation, DPA and timing attacks.
SF5 Protection	SF5 supports all other TSF by testing and protecting the TOE.

8.6 Rationale for Extensions

The additional family FPT_EMSEC TOE Emanation was defined in the SSCD type 3 PP [16]. The developer decided to inherit FPT_EMSEC TOE Emanation from [16]. The rationale for the extension is transferable and reproduced here for clarity reasons. 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 externally 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.
For further details refer to section 6.6 [16]. This ST does not define or use other extensions to CC part 2 [9].

8.7 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.

8.8 Rationale for Assurance Level 4 Augmented

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

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

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

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

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

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

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

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

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

8.9 PP Claims Rationale

The Security Target does not include a PP claim, see also section 7.

9 References

9.1 Bibliography

[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] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (BGBl. I S.876 ff)

[3] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16.November 2001 (BGBl. I S. 3074ff)

[4] Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV, Veröffentlicht am 23. März 2006 im Bundesanzeiger Nr. 58, S. 1913-1915, Vom 2. Januar 2006, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

[5] Algorithms and Parameters for Secure Electronic Signatures, V.2.1 Oct 19th 2001, Algorithms group working under the umbrella of European Electronic Signature Standardisation Initiative Steering Group

[6] RSA Laboratories, PKCS #1: RSA Encryption Standard, An RSA Laboratories Technical Note Version 1.5, Revised November 1st, 1993

[7] FIPS PUB 180-2: Secure Hash Standard, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2002, August 1,

[8] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.3, August 2005, CCMB-2005-08-001

[9] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.3, August 2005, CCMB-2005-08-002

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

[11] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004

[12] ISO/IEC 7816-3: 1997 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols, International Standard

[13] ISO/IEC 7816-4: 1995 Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry command for interchange

[14] ISO/IEC 7816-8:1998 Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands

[15] ISO/IEC 7816-8:1998 Identification cards – Integrated circuit(s) cards with contacts – Part 9: Additional interindustry commands and security attributes

[16] Protection Profile – Secure Signature-Creation Device (SSCD-PP) Type 3, Version 1.05, EAL 4+ BSI-PP-0006-2002T, 03.04.2002

[17] Protection Profile – Secure Signature-Creation Device (SSCD-PP) Type 3, Version 1.05, EAL 4+ BSI-PP-0006-2002T, 03.04.2002

[18] Certification report for Infineon Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a24, m1484a27 and m1484b14

[19] Security and Chip Card ICs, SLE66CxxxP, Data Book, August 2004, Infineon

[20] Administrator Guidance CardOS V4.3B Re_Cert with Application for Digital Signature Siemens AG, MED GS SEC, Version 1.2, Edition 11/2006

[21] User Guidance CardOS V4.3B Re_Cert with Application for Digital Signature Siemens AG, MED GS SEC, Version 1.2, Edition 11/2006

[22] Certification report for Infineon Smart Card IC (Security Controller) SLE66CX642P / m1485b16 with RSA 2048 V1.30 and specific IC Dedicated Software from Infineon Technologies, certification file BSI-DSZ-CC-0315-2005, 12.08.2005, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[23] RIPEMD-160: A Strengthened Version of RIPEMD, Hans Dobbertin, Antoon Bosselaers Bart, April 1996

[24] Certification report for Infineon Smart Card IC (Security Controller) SLE66CX322P with RSA2048/m1484f18

[25] Certification report for Infineon Smart Card IC (Security Controller) SLE66CX322P/m1484b14 and m1484f18 with RSA 2048 V1.30 and Specific IC Dedicated Software from Infineon Technologies AG, Certification ID BSI-DSZ-CC-0266-2005, 22.04.2005, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[26] Assurance Continuity Maintenance Report BSI-DSZ-CC-0266-2005-MA-01 for Infineon Smart Card IC (Security Controller) SLE66CX322P/m1484b14 and m1484f18 with RSA 2048 V1.30 and Specific IC Dedicated Software from Infineon Technologies AG, 07.06.2005, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[27] Assurance Continuity Maintenance Report BSI-DSZ-CC-0266-2005-MA-02 for Infineon Smart Card IC (Security Controller) SLE66CX322P/m1484b14 and m1484f18 with RSA 2048 V1.30 and Specific IC Dedicated Software from Infineon Technologies AG, 16.05.2006, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[28] Assurance Continuity Maintenance Report BSI-DSZ-CC-0266-2005-MA-03 for Infineon Smart Card IC (Security Controller) SLE66CX322P/m1484b14 and m1484f18 with RSA 2048 V1.30 and Specific IC Dedicated Software from Infineon Technologies AG, 25.07.2006, Bundesamt für Sicherheit in der Informationstechnik (BSI)

9.2 Acronyms

CC	Common Criteria
CGA	Certification Generation Application
DTBS	Data to be signed
EAL	Evaluation Assurance Level
IT	Information Technology
PIN	Personal Identification Number
PP	Protection Profile
PUK	Personal Unblocking Key
RAD	Reference Authentication Data
SCA	Signature Creation Application
SCD	Signature Creation Data
SDO	Signed Data Object
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
SSCD	Secure Signature Creation Device
ST	Security Target
SVD	Signature Verification Data
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
VAD	Verification Authentication Data