SIEMENS

CardOS® V4.2B FIPS

Security Target
CardOS V4.2B FIPS with
Application for Digital Signature

Edition 07/2007

SIEMENS

Siemens AG
DS1
Charles-de-Gaulle-Str. 2

D-81737 Munich
Germany

Contents

1 ST Introduction

1.1 ST Identification

Title: Security Target CardOS V4.2B FIPS with Application for Digital Signature
Authors: Siemens AG, Med GS SEC DS1
CC Version: 2.3 Final
General Status: Final
Version Number: Version 1.2, (23.07.2007)
Registration: BSI-DSZ-CC-0476

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 a Secure Signature Creation Device (SSCD) based on a Chip Card allowing to generate cryptographically strong Signatures over previously and 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

The ST is CC Part 2 [9] extended, CC Part 3 [10] conformant and the assurance level for this ST is EAL4 augmented.

The augmentation of EAL4 is given 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 claims to be conformant to the SSCD-PP type 3 [16].

2 TOE Description

2.1 TOE Characteristics

The TOE is 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 consists of i) configured software (OS, packages and signature application) ii) the underlying hardware (SLE66CX322P/ SLE66CX642P from Infineon) used to implement the secure signature-creation device (SSCD) and iii) the pertaining guidance documentation 'Administrator Guidance CardOS V4.2B_FIPS' [21] 'User Guidance CardOS V4.2B_FIPS' [22].

Therefore the TOE is considered to be a product.

Table 1: Components of the TOE

No.	Type	Term	Version	Date	Form of delivery
1	Software (Operating System)	CardOS V4.2B	C809	05.07.05	loaded in ROM / EEPROM
2	Software Application Digital Signature (Application / Data Structure)	***Pre-loaded variant*** V42B_FIPS_InitScript.py	1.1	May 24 2007	Personalization Script Files in Python format, after whose execution the ADS will be loaded in EEPROM
		V42B_FIPS_InitScript_DF_DS_x.py	1.0	May 15 2007	
		V42B_FIPS_PersScript.py	1.1	May 24 2007	
		V42B_FIPS_PersScript_DF_DS_x .py	1.1	May 24 2007	
		V42B_FIPS_CAScript.py	1.1	May 24 2007	
		V42B_FIPS_CAScript_DF_DS_x.py	1.0	May 15 2007	
		V42B_FIPS_RAScript.py	1.1	May 24 2007	
		V42B_FIPS_RAScript_DF_DS_x.py	1.2	Jun 04 2007	
		Post-loaded variant: V42B_FIPS_InitScript_Post.py	1.1	May 24 2007	
		V42B_FIPS_LRAScript_Post.py	1.1	May 24 2007	
		V42B_FIPS_LRAScript_Post_DF_DS_x.py	1.1	May 24 2007	
		All variants: V42B_FIPS_Default_1024.py V42B_FIPS_Default_1280.py V42B_FIPS_Default_1536.py V42B_FIPS_Default_1752.py V42B_FIPS_Default_1880.py	1.0	May 21 2007	
		cardlib.py	1.0	22.06.2007	Cardlib Script Files in Python format (necessary for execution of the Personalization Scripts)
		Apdu.py	1.14		
		Chips.py	1.2		
		codeLen.py	1.6		
		Constants.py	1.33		
		CsfParser.py	1.9		
		DevInifile.py	1.10		
		DirectInterface.py	1.16		
		EchoAPDU.py	1.9		
		EchoInterface.py	1.7		
		Exceptions.py	1.4		

No.	Type	Term	Version	Date	Form of delivery
		__init__.py	1.0		
		ExpandedRules.py	1.2		
		Interface.py	1.13		
		InterfaceToCard.py	1.16		
		Iso.py	1.26		
		locate.py	1.39		
		m_classes.py	1.29		
		m_functions.py	1.17		
		m3constants.py	1.1		
		m4lib.py	1.0		
		MAC.py	1.0		
		MAC3.py	1.0		
		makeOptions.py	1.2		
		OsVersionCNS.py	1.5		
		OsVersionHPC1.py	1.15		
		OsVersionM3.py	1.3		
		OsVersionM4.py	1.33		
		OsVersionM401.py	1.2		
		OsVersionM401a.py	1.2		
		OsVersionM401x.py	1.2		
		OsVersionM401y.py	1.3		
		OsVersionM403.py	1.25		
		OsVersionM410.py	1.15		
		OsVersionM420.py	1.4		
		OsVersions.py	1.11		
		OsVersionV42B.py	1.7		
		OsVersionV42BCNS.py	1.2		
		OsVersionV42CNS.py	1.2		
		OsVersionV43.py	1.4		
		OsVersionV43B.py	1.4		
		OsVersionV43BCNS.py	1.3		
		OsVersionV43CNS.py	1.2		
		Pcsc.py	1.13		
		setBaudRate.py	1.1		
		SM.py	1.24		
		tracer.py	1.4		
		translateAddr.py	1.2		
		xd.py	1.3		
		romkeys.py (Default keys)	1.26.1.0		
		reader.ini (Card Reader configuration file)	1.0	23.11.2006	Config File
		M3_Crypto.dll	1.2	02.05.2006	Crypto Library components (used for SM calculation)
		Des_crypt.dll	1.2	02.05.2006	
		rsa_crypt.dll	1.1	25.02.2003	
		m3lib.pyd	1.5	27.08.2003	
		Python-2.3.4.exe	2.3.4		Python Programming Language
		Python Cryptography Toolkit	2.0.1		Python CryptoLibrary (used for SM calculation)

No.	Type	Term	Version	Date	Form of delivery
3	Software CommandSet_ Extension Package	V42B_CommandSet_Ext_Package.csf	1.2	Jun 15 2007	Personalization Script Files in CSF format, after whose execution the resp. code will be loaded and activated in EEPROM
4	Software CAT Package	V42B_CAT_Package.csf	1.2	Jun 15 2007	
5	Software DRNG Package	V42B_DRNG_Package.csf	1.3	Jun 15 2007	
6	Software WIPE Package	V42B_WIPE Package.csf	1.1	Jun 06 2007	
7	Software HMAC Package (optional)	V42B_HMAC_Package.csf	1.2	Jun 15 2007	
9	Documentation	CardOS V4.2B User's Manual	1.0	09/2005	Paper form or PDF-File
10	Documentation	CardOS V4.2B Packages & Release Notes	1.0	05/2007	Paper form or PDF-File
11	Documentation	CardOS V4.2B CAT_DRNG_WIPE Packages & Release Notes	1.0	05/2007	Paper form or PDF-File
12	Documentation	Administrator Guidance CardOS V4.2B FIPS	1.4	07/2007	Paper form or PDF-File
13	Documentation	User Guidance CardOS V4.2B FIPS	1.4	06/2007	Paper form or PDF-File
14	Documentation	ADS_Description CardOS V4.2B FIPS	1.0	05/2007	Paper form or PDF-File
15					
16	Hard-ware (Chip) 32K	Infineon SLE66CX322P	m1484b14 and m1484f18		Module
	Hard-ware (Chip) 64K	Infineon SLE66CX642P	m1485b16		Module
	Firmware RMS	RMS	Version 1.5		loaded in reserved area of User ROM
	Software crypto library	RSA2048 crypto library	Version 1.30		loaded in ROM
17	Software STS	STS Self Test Software	V53.10.13		Stored in Test ROM on the IC

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 [17] German IT-Security Certificate and Assurance Maintenance Reports [25] - [27]. The chip SLE66CX642P is certified for the production site Dresden (see German IT-Security Certificate [24]).

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 (i) displayed correctly and (ii) hashed with appropriate hash functions that are, according to 'Algorithms and Parameters for Secure

Electronic Signatures' [4] and 'Geeignete Algorithmen' [28] agreed as suitable for qualified electronic signatures, where the display and hash functions are provided by the TOE environment

(b) after appropriate authentication of the signatory by the TOE.
(c) using appropriate cryptographic signature function that employs appropriate cryptographic parameters agreed as suitable according to 'Algorithms and Parameters for Secure Electronic Signatures' [4] and 'Geeignete Algorithmen' [28].

The TOE implements all IT security functionality which is necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control. The 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 verification authentication data of the Transport-PIN (VAD).

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 underlying hardware, 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 via a trusted path or trusted channel, whenever authenticity, and/or confidentiality of the transferred data is required..

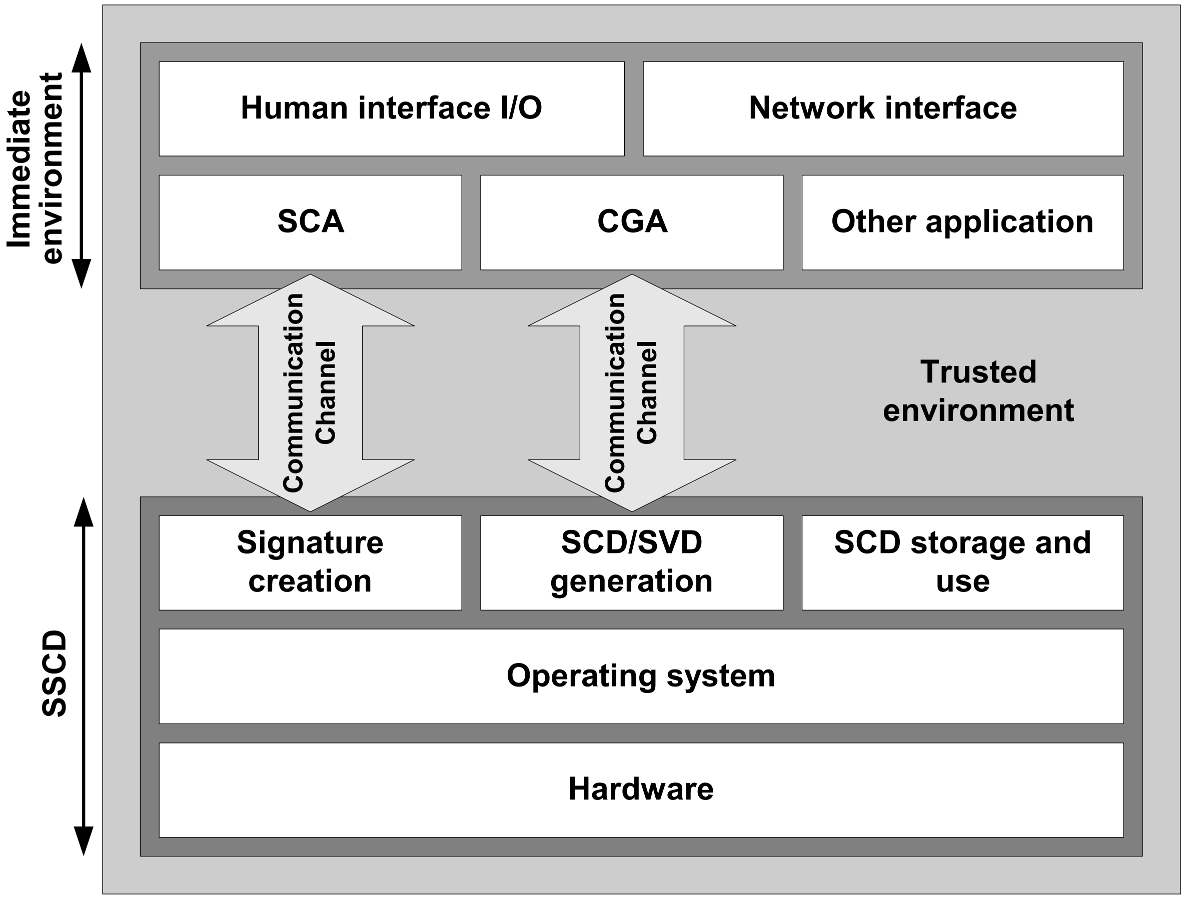

Figure 1: Scope of the SSCD, structural view

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.

After fabrication, the TOE is initialised and personalised for the signatory, i.e. the SCD/SVD key pair is generated and the Transport PIN RAD used for the first 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 cycle phase DEATH in which the SCD is permanently blocked.

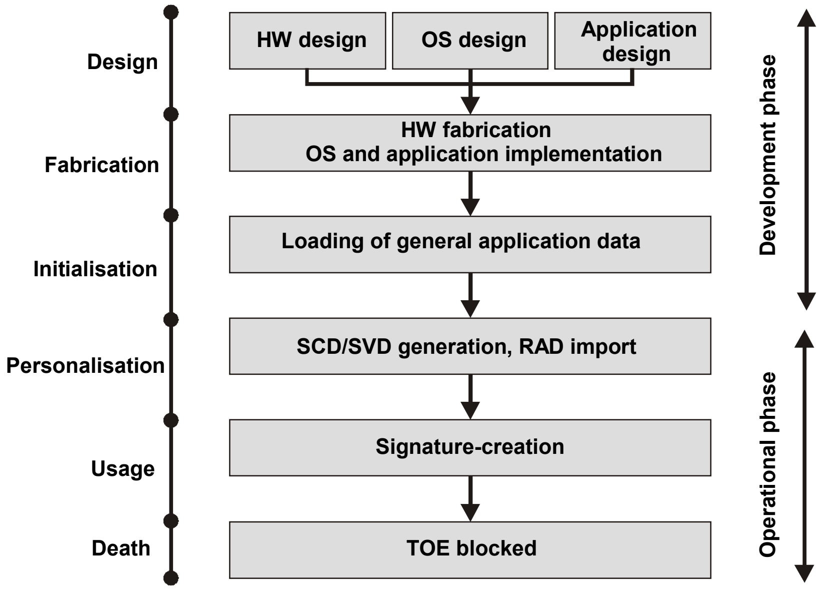

Figure 2: SSCD life cycle

2.2 General Features of the CardOS V4.2B operating system

As described in section 2.1, the TOE comprises the underlying hardware, 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 V4.2B .

CardOS V4.2B 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 V4.2B complies with the ISO standard family ISO 7816 part 3, 4, 5, 8 and 9.

CardOS V4.2B with application Digital Signature and FIPS packages is designed to meet the requirements of the German Digital Signature Act ([29], [30]).

The CardOS V4.2B DRNG Package implements the functionality of a high quality 'Deterministic Random Number Generator'.

The CardOS V4.2B CAT Package implements the functionality of 'Cryptographic Algorithm Tests' via 'Known Answer Tests' for the algorithms RSA, RSA_SIG, RSA2_SIG, 3DES, MAC3, SHA-1 and for the DRNG.

The CardOS V4.2B WIPE Package implements the possibility to delete a complete DF-tree, without prior deletion of sub-elements, after aquisition of the corresponding access right.

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

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

General features

- CardOS V4.2B runs on the Infineon SLE66 chip family. The SLE66CX322P and SLE66CX642P chips with embedded security controller for asymmetric cryptography and with a true random number generator have successfully been certified against the Common Criteria EAL5+ security requirements (see [17], [25], [26], [27] and [24]).
- 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 V4.2B 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 to so-called Logical Tests.
- 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 up to 2048 bit key length (PKCS#1 padding) (the TOE uses only 1024 up to 1752 bit RSA keys (with ext. APDU mode up to 1880)), 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 a deterministic 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 (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 during transmission to the TOE).
4. VAD: PIN, PUK and Transport PIN code entered by the End User to perform a signature operation resp. the changing and unblocking of the PIN (confidentiality and authenticity of the VAD as needed by the authentication method employed)[1]
5. RAD: Reference PIN, PUK and Transport PIN code used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)[2]
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**.

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

2 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].

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

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.

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] with some necessary modifications.

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 uses 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 negligibly 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 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 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 and
(c) attaches the signature produced by the TOE to the data or provides it separately.

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].
Where operations for assignment, selection and refinement have been made, all these operations are typographically accentuated by underlining these passages (e.g. RSA).
Operations that were already carried out within the PP [16] are only underlined (e.g. RSA), whereas those operations that are carried out or changed later on are underlined and also italicised, (e.g. *RSA*).
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.

Whenever in this and the following sections the signature key length is specified as ‘1024 up to 1752 bit’, 1752 is the max. length that can be used with normal APDU mode, i.e. with an Input Buffer of 255 bytes. If extended APDU mode is used (Input Buffer adjustable up to 1024) a key length up to 1880 bytes is possible.

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*[3] and specified cryptographic key sizes *1024 up to 1752 bit in 8 bit steps*[4] that meet the following:

Geeignete Algorithmen [28][5].

Refinement:
The already within [16] executed operation ‘List of approved algorithms and parameters’ is replaced with the concrete statement of references.

3 [assignment: cryptographic key generation algorithm]
4 [assignment: cryptographic key sizes]
5 [assignment: list of standards]

5.1.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in case of regeneration of a new SCD in accordance with a specified cryptographic key destruction method *key overwriting*[6] that meets the following: *none*[7].

Application note:

The cryptographic key SCD will be destroyed on demand of the Administrator. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.
The SCD key data are physically overwritten when the new key is generated.

5.1.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP	The TSF shall perform SCD / SVD correspondence verification[8] in accordance with a specified cryptographic algorithm *RSA*[9] and cryptographic key sizes *1024 up to 1752 bit in 8 bit steps*[10] that meet the following: *RSA and PKCS#1, v. 1.5, BT 1 [6]*[11].
FCS_COP.1.1/ SIGNING	The TSF shall perform digital signature-generation[8] in accordance with a specified cryptographic algorithm *RSA*[9] and cryptographic key sizes *1024 up to 1752 bit in 8 bit steps*[10] that meet the following: (1) *RSA and PKCS#1, v. 1.5, BT 1* [6] (2) *Geeignete Algorithmen* [28][11]

Refinement:
The already within [16] executed operation 'List of approved algorithms and parameters' is replaced with the concrete statement of references.

5.1.2 User data protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1/ Initialisation SFP	The TSF shall enforce the Initialisation SFP[12] on generation of SCD/SVD pair by User[13].
FDP_ACC.1.1/ Personalisation SFP	The TSF shall enforce the Personalisation SFP[12] on creation of RAD by Administrator[13].
FDP_ACC.1.1/ Signature-creation SFP	The TSF shall enforce the Signature-creation SFP[12] on 1. sending of DTBS-representation by SCA, 2. signing of DTBS-representation by Signatory[13].
FDP_ACC.1.1/ SVD Transfer SFP	The TSF shall enforce the SVD Transfer SFP[12] on export of SVD by User[13].

6 [assignment: cryptographic key destruction method]
7 [assignment: list of standards]
8 [assignment: list of cryptographic operations]
9 [assignment: cryptographic algorithm]
10 [assignment: cryptographic key sizes]
11 [assignment: list of standards]
12 [assignment: access control SFP]
13 [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

5.1.2.2 Security attribute based access control (FDP_ACF.1)

The following table lists the subjects and objects controlled by the SFPs of section 5.1.2.1 and the SFP-relevant security attributes:

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

Table 2: Security attributes of the different SFP

Initialisation SFP

FDP_ACF.1.1/ Initialisation SFP — The TSF shall enforce the Initialisation SFP[14] to objects based on General attribute and Initialisation attribute[15].

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[16].

FDP_ACF.1.3/ Initialisation SFP — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[17].

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[18].

Application note:
The generation of the SCD/SVD pair is only possible for the Administrator (restricted by “SCD / SVD management”. See also FMT_MSA.1.1 / Administrator).

14 [assignment: access control SFP]
15 [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]
16 [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
17 [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
18 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

Personalisation SFP

FDP_ACF.1.1/ Personalisation SFP	The TSF shall enforce the Personalisation SFP[14] to objects based on General attribute[15].
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[16].
FDP_ACF.1.3/ Personalisation SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[17].
FDP_ACF.1.4/ Personalisation SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: none[18].

Signature-creation SFP

FDP_ACF.1.1/ Signature-creation SFP	The TSF shall enforce the Signature-creation SFP[14] to objects based on General attribute and Signature-creation attribute group[15].
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"[16].
FDP_ACF.1.3/ Signature-creation SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[17].
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". (c) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS not sent by an authorised SCA with SCD by the Signatory whose security attribute "SCD operational" is set to "no". (d) User with the security attribute "role" set to "Administrator is not allowed to create electronic signatures for any DTBS with SCD whose security attribute "SCD operational" is set to any status[18].

Application note:
The corresponding TSFR of the PP [16], section 5.1.2.2 was refined for reasons of clarity regarding all possible combinations of relevant security attributes. The following table is added for additional support.

DTBS	Administrator SCD operational “no”	Administrator SCD operational “yes”	Signatory SCD operational “no”	Signatory SCD operational “yes”
sent by an authorised SCA “no”	not allowed[19]	not allowed[19]	not allowed[20]	not allowed[21]
sent by an authorised SCA “yes”	not allowed[19]	not allowed[19]	not allowed[22]	**allowed[23]**

Table 3: Additional support for the refinement of Signature-creation SFP

SVD Transfer

FDP_ACF.1.1/ SVD Transfer SFP — The TSF shall enforce the SVD Transfer SFP[14] to objects based on General attribute[15].

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[16].

FDP_ACF.1.3/ SVD Transfer SFP — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[17].

FDP_ACF.1.4/ SVD Transfer SFP — The TSF shall explicitly deny access of subjects to objects based on the rule: none[18].

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[24] 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[25] 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[26].

[19] See FDP_ACF.1.4/ Signature-creation SFP, point (d).
[20] See FDP_ACF.1.4/ Signature-creation SFP, point (c).
[21] See FDP_ACF.1.4/ Signature-creation SFP, point (a).
[22] See FDP_ACF.1.4/ Signature-creation SFP, point (b).
[23] See FDP_ACF.1.2/ Signature-creation SFP.
[24] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[25] [assignment: access control SFP and/or information flow control SFP]

Application note:
An SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature and 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[27] the following objects: SCD, VAD, RAD[28].

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 persistently stored by TOE).

FDP_SDI.2.1/ Persistent	The TSF shall monitor user data stored within the TSC for integrity error[29] on all objects, based on the following attributes: integrity checked persistent stored data[30].
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[31].

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[29] on all objects, based on the following attributes: integrity checked stored data[30].
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[31].

5.1.2.7 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ SVD Transfer	The TSF shall enforce the SVD Transfer SFP[32] to be able to transmit[33] user data in a manner protected from modification and insertion[34] errors.

[26] [assignment: additional importation control rules]
[27] [selection: allocation of the resource to, deallocation of the resource from]
[28] [assignment: list of objects]
[29] [assignment: integrity errors]
[30] [assignment: user data attributes]
[31] [assignment: action to be taken]
[32] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[33] [selection: transmit, receive]
[34] [selection: modification, deletion, insertion, replay]

FDP_UIT.1.2/ SVD Transfer	The TSF shall be able to determine on receipt of user data, whether modification and insertion[35] has occurred.
FDP_UIT.1.1/ TOE DTBS	The TSF shall enforce the Signature-creation SFP[32] to be able to receive[33] the DTBS-representation in a manner protected from modification, deletion and insertion[34] errors.
FDP_UIT.1.2/ TOE DTBS	The TSF shall be able to determine on receipt of user data, whether modification, deletion and insertion[35] 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 (PIN and PIN_T), resp. 10[36] (PUK)* unsuccessful authentication attempts occur related to consecutive failed authentication attempts[37].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall block RAD[38].

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[39].

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.[40]

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

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

Application note:
“Local user” mentioned in component FIA_UAU.1.1 is the user using the trusted path provided between the SCA in the TOE environment and the TOE as indicated by FTP_TRP.1/SCA and FTP_TRP.1/TOE.

35 [selection: modification, deletion, insertion, replay]
36 [selection: [assignment: positive integer number], “an administrator configurable positive integer within [assignment: range of acceptable values]”] (due to FI 111)
37 [assignment: list of authentication events]
38 [assignment: list of actions]
39 [assignment: list of security attributes]
40 [assignment: list of TSF mediated actions]

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.[41]

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[42] the signature-creation function[43] to Signatory[44].

5.1.4.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/ Administrator The TSF shall enforce the Initialisation SFP[45] to restrict the ability to modify[46] the security attributes SCD / SVD management[47] to Administrator[48].

FMT_MSA.1.1/ Signatory The TSF shall enforce the Signature-creation SFP[45] to restrict the ability to modify[46] the security attributes SCD operational[47] to Signatory[48].

Application Note:
The security attribute “SCD operational” is set from “no” to “yes” after successful verification of the PIN_T which is only known by the 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[49] to provide restrictive[50] 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 first generation of the SCD.

41 [assignment: list of TSF-mediated actions]
42 [selection: determine the behaviour of, disable, enable, modify the behaviour of]
43 [assignment: list of functions]
44 [assignment: the authorised identified roles]
45 [assignment: access control SFP, information flow control SFP]
46 [selection: change_default, query, modify, delete, [assignment: other operations]]
47 [assignment: list of security attributes]
48 [assignment: the authorised identified roles]
49 [assignment: access control SFP, information flow control SFP]
50 [selection: choose one of: restrictive, permissive, [assignment: other property]]

FMT_MSA.3.2 The TSF shall allow the Administrator[51] to specify alternative initial values to override the default values when an object or information is created.

Application note:
The Administrator is required by the guidance not to override the default value.
The security attribute of the SCD "**SCD operational**" which has been set to "**yes**" after the **first** authentication of the Signatory by Transport-PIN, must not be reset to "**no**" after re-generation of the SCD. The new SCD is immediately operational.

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*[52] the RAD[53] to Signatory[54].

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/SVD management attribute*

(2) *Modifying the SCD operational attribute*

(3) *Creation of RAD*

(4) *Changing or unblocking of RAD*[55].

Application note:
This TSFR is not taken from [16] but has been introduced due to [9].

5.1.4.7 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles

1. Administrator and
2. Signatory[56].

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*[57] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

[51] [assignment: the authorised identified roles]
[52] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[53] [assignment: list of TSF data]
[54] [assignment: the authorised identified roles]
[55] [assignment: list of security management functions to be provided by the TSF]
[56] [assignment: the authorised identified roles]
[57] [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*[58] in excess of *unintelligible limits*[59] enabling access to RAD and SCD[60].

FPT_EMSEC.1.2 The TSF shall ensure *S.User and S.OFFCARD*[61] are unable to use the following interface *physical contacts of the underlying IC hardware*[62] to gain access to RAD and SCD[63].

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*[64]

(4) *Out of range failures of temperature, clock and voltage sensors*[65].

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 scenarios by intrusion of physical or mechanical means*[66] to the *underlying IC hardware*[67] by responding automatically such that the TSP is not violated.

5.1.5.6 TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up and at the conditions* [68]

(1) *Generation of the SCD/SVD key pair according to FCS_CKM.1*

(2) *Signature-creation according to FCS_COP.1/SIGNING*[69]

(3) *VAD verification*

---

58 [assignment: types of emissions]
59 [assignment: specified limits]
60 [assignment: list of types of TSF data] and [assignment: list of types of user data]
61 [assignment: type of users]
62 [assignment: type of connection]
63 [assignment: list of types of TSF data] and [assignment: list of types of user data]
64 [assignment: list of types of failures in the TSF]
65 [assignment: list of types of failures in the TSF]
66 [assignment: physical tampering scenarios]
67 [assignment: list of TSF devices/elements]

(4) *RAD modification*

(5) *RAD unblocking*

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*[70] 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[71].
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**[70] 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[71].

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[72] 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.

68 [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions]
69 [assignment: conditions under which self test should occur]
70 [selection: the TSF, the remote trusted IT product]
71 [assignment: list of functions for which a trusted channel is required]
72 [selection: remote, local]

FTP_TRP.1.2/TOE The TSF shall permit *local users*[73] to initiate communication via the trusted path.

FTP_TRP.1.3/TOE The TSF shall require the use of the trusted path for

(1) *initial user authentication*[74],

(2) *modification of the RAD and*

(3) *unblocking the RAD*[75].

.

73 [selection: the TSF, local users]
74 [selection: initial user authentication, [assignment: other services for which trusted path is required]]
75 [selection: initial user authentication, [assignment: other services for which trusted path is required]]

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 given within section 5.2 of the Protection Profile - Secure Signature-Creation Device (SSCD-PP) Type 3 [16].

The following Final Interpretations are considered within [16] , which is based on Common Criteria Version 2.1.

Final Interpretation	Resulting changes
003	An element is added after ACM_CAP.4.3C
004	The element ACM_SCP.2.1D is changed
004 and 038	The element ACM_SCP.2.1C is replaced
051	The element ADO_IGS.1.1C is changed.
051	The two elements AVA_VLA.4.1D and AVA_VLA.4.2D are changed.
051	The previous four elements AVA_VLA.4.1C to AVA_VLA.4.4C (see CC V2.1 part 3 [34]) are replaced by the six elements AVA_VLA.4.1C to AVA_VLA.4.6C

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* shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method qualified certificate[76] that meets the following: *Geeignete Algorithmen* [28][77].

5.3.1.2 Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/ CGA	The *IT environment* shall perform import the SVD[78] in accordance with a specified cryptographic key access method import through a secure channel[79] that meets the following: (1) *FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES)*, [18] (2) *NIST Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm*, [19]. (3) *ANSI X9.19-1996, Financial Institution Retail Message Authentication* [20][80]

5.3.1.3 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ SVD import	The *IT environment* shall enforce the SVD import SFP[81] to be able to receive[82] user data in a manner protected from modification and insertion[83] errors.
FDP_UIT.1.2/ SVD import	The *IT environment* shall be able to determine on receipt of user data, whether modification and insertion[84] has occurred.

5.3.1.4 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SVD import	The *IT environment* 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 *IT environment* shall permit *the remote trusted IT product* [85] to initiate communication via the trusted channel.
FTP_ITC.1.3/ SVD import	The *IT environment* **or the TOE** shall initiate communication via the trusted channel for import SVD[86].

76 [assignment: cryptographic key distribution method]
77 [assignment: list of standards]
78 [assignment: type of cryptographic key access
79 [assignment:cryptographic key access method]
80 [assignment: list of standards]
81 [assignment: access control SFP(s) and/or information flow control SFP(s)]
82 [selection: transmit, receive]
83 [selection: modification, deletion, insertion, replay]
84 [selection: modification, deletion, insertion, replay]
85 [selection: the TSF, the remote trusted IT product]

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* shall perform hashing the DTBS[87] in accordance with a specified cryptographic algorithm *SHA-1 up to SHA-512, RIPEMD160*[88] and cryptographic key sizes none[89] that meet the following: (1) *FIPS PUB 180-2: Secure Hash Standard* [7] (2) *ISO/IEC 10118-3: 1998 Information technology – Security techniques– Hash functions*[90].

5.3.2.2 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ SCA DTBS	The *IT environment* shall enforce the Signature-creation SFP[91] to be able to transmit[92] user data in a manner protected from modification, deletion and insertion[93] errors.
FDP_UIT.1.2/ SCA DTBS	The *IT environmen* shall be able to determine on receipt of user data, whether modification, deletion and insertion[94] has occurred.

5.3.2.3 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SCA DTBS	The *IT environment* 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 *IT environment* shall permit the TSF[95] to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCA DTBS	The *IT environment* **or the TOE** shall initiate communication via the trusted channel for signing DTBS-representation by means of the SSCD[96].

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 *IT environment* shall provide a communication path between itself and *local users*[97] that is logically distinct from other communication

86 [assignment: list of functions for which a trusted channel is required]
87 [assignment: list of cryptographic operations]
88 [assignment: cryptographic algorithm]
89 [assignment: cryptographic key sizes]
90 [assignment: list of standards]
91 [assignment: access control SFP(s) and/or information flow control SFP(s)]
92 [selection: transmit, receive]
93 [selection: modification, deletion, insertion, replay]
94 [selection: modification, deletion, insertion, replay]
95 [selection: the TSF, the remote trusted IT product]
96 [assignment: list of functions for which a trusted channel is required]

	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 *IT environment* shall permit *local users*[98] to initiate communication via the trusted path.
FTP_TRP.1.3/ SCA	The *IT environment* shall require the use of the trusted path for (1) *initial user authentication*[99], (2) *modification of the RAD and* (3) *unblocking the RAD*[100].

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 ensure the ongoing compliance.

R.Sigy_Guide *Application of User Guidance*

The CSP 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.

97 [selection: remote, local]
98 [selection: the TSF, local users, remote users]
99 [selection: initial user authentication, [assignment: other services for which trusted path is required]]
100 [selection: initial user authentication, [assignment: other services for which trusted path is required]]

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).

The Administrator is implicitly identified and authenticated after the card has changed its lifecycle from MANUFACTURING to ADMINISTRATION until all access conditions are correctly set for the dedicated file containing the digital signature application data (DF_DS).

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 to unblock and change the blocked PIN by the Signatory
- Transport-PIN for the activation of the dedicated file containing the SCD and for the first setting of 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 values. Thereafter the PIN and PUK will be unblocked by the TOE.

Therefore, 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 Transport-PIN (PIN_T) is used to secure the TOE delivery process. It will be verified only once and will be used for the activation of the dedicated file containing the SCD/SVD key pair and for the first setting of PIN and PUK.

The TOE will check that the provided VAD (PIN, PUK and Transport-PIN) 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 three for PIN and Transport-PIN and ten for PUK. Thereafter SF1 will block the corresponding 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 to unblock and change the blocked PIN
- the correct PUK to change resp. modify the PUK (FMT_SMF.1 (4))
- the correct Transport-PIN to unblock 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 (FDP_ACC.1 / Personalisation SFP, FDP_ACF.1 / Personalisation SFP and FMT_SMF.1 (3)). The individual PIN and PUK values are set by the Signatory after successful authentication with the Transport-PIN (FMT_SMF.1.1 (2)).

After the successful verification of the Transport-PIN the value of the attribute “SCD operational” is changed from “no” to “yes”, which is irreversible, 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) (Cf. also 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:

- 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),
- the DTBS are sent by an authorised SCA
(FDP_ACC.1 / Signature creation SFP, FDP_ACF.1 / Signature creation SFP and FMT_MOF.1).

During DTBS import any security attribute associated with the user data will be ignored (FDP_ITC.1 / DTBS).

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 / Signatory and FMT_SMF.1 (2)). The security attribute “SCD operational” is set to “yes” by the TOE after the Transport-PIN which is only known by the Signatory has successfully been verified, 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 (4)), see also SF1 User Identification and Authentication.
The PUK can always be modified but unblocked only once (by Transport-PIN). The Transport-PIN can neither be modified nor unblocked. After the first successful verification of the Transport-PIN the security attribute “SCD operational” cannot be set to “no” again by the TOE, see also SF1 User Identification and Authentication.

The SCD / SVD key-pair generation is only possible for the administrator with the attribute “SCD / SVD management” set to “authorised”.
After the key-pair has been generated the “SCD / SVD management” is set to “not authorised” by the administrator (FDP_ACC.1 / Initialisation SFP, FDP_ACF.1 / Initialisation SFP, FMT_MSA.1 / Administrator and FMT_SMF.1 (1)). Before the generation of a new SCD / SVD key-pair the attribute “SCD / SVD management” has to be set to “authorised”, which can be done only by the administrator.

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 1752 bit. The key pairs fulfil the corresponding requirements of [4] and [28] 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 Divisor) test and enough rounds of the Rabin Miller Test are performed. The TOE uses a deterministic random number generator, implemented as package code, 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.

During key pair generation the correspondence between the generated SCD and SVD is always checked before the key pair is stored persistently (FCS_COP.1/CORRESP), see also SF7 SVD Transfer.

The destruction of the old SCD takes place during regeneration of the new SCD by physical overwriting of the exactly same memory area of the stored SCD, which will be re-used, when the new key is generated (FCS_CKM.4).

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.

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:

[4] 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

[5] ISO/IEC 10118-3: 1998 Information technology – Security techniques– Hash functions - Part 3: Dedicated hash functions

[6] RSA Laboratories, PKCS #1 v2.1: RSA Encryption Standard, RSA Laboratories, June 14th, 2002

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

[28] 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 12. April 2007 im Bundesanzeiger Nr. 69, S. 3759, Vom 22. Februar 2007, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

The TSF supports RSA key lengths of 1024 up to 1752 bit (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 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 [17] and [24]).

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 security assumptions provided by the abstract machine that underlies the TSF (FPT_AMT.1). The following tests are performed during initial start-up (FPT_TST.1):

- The SLE66CX322P/ SLE66CX642P provide a high security initialization software concept. The self test software (STS) is activated by the chip after a cold or warm reset (ISO-reset with I/O=1). It contains diagnostic routines for the chip, see [3] chap. 8.
- 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 hardware sensors will be tested. If the first test fails, another test will be executed. If this fails again the TOE will preserve a secure state (lifecycle DEATH).
- The deterministic random number generator will be tested with a ‘Known Answer Test’ (KAT) according to [31] FIPS PUB 140-2: Security Requirements for Cryptographic Modules. If the test fails, the TOE will preserve a secure state (lifecycle DEATH).

The TOE will furthermore run tests during the generation of the SCD/SVD key pair (SF3 SCD/SVD Pair Generation), during signature creation (SF4 Signature Creation), the verification of VAD, the unblocking and changing the RAD (FPT_TST.1).

The correct operation of the TSF is demonstrated by performing the following checks:

- The TOE’s lifecycle phase is checked.
- Before command execution the functioning of the Deterministic Random Number Generator (DRNG), of the sensors and of the Active Shield is tested.
- Before random numbers are requested from the DRNG, which are used for command execution (e.g. generation of the SCD/SVD key pair) the correct functioning of the DRNG is tested.
- All command parameters are checked for consistency.
- Prerequisites for command execution are checked (see also SF2).
- Before a random number is requested for the generation of the SCD/SVD key pair or for random padding used by Secure Messaging the correct functioning of the deterministic random number generator will be tested according to [31].

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

The TOE is furthermore able to detect physical or mechanical tampering attempts (FPT_PHP.1). This comprises tampering attempts before start-up and during operation. If the underlying IC hardware is attacked by physical or mechanical means the TOE will respond 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 or RAD 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).

The following data (temporarily) stored by TOE have the user data attribute "integrity checked stored data":

- DTBS

If the integrity of the DTBS 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/ DTBS).

6.1.6 SF6 Secure Messaging

This TSF is responsible for the secure messaging between TOE and the external entities.

Secure messaging (SF6) is always used when the TOE establishes at least one of the following three types of communication:

- a communication channel between itself and the CGA. This trusted channel, either initiated by the TOE or the CGA is used for the SVD export (FTP_ITC.1/SVD Transfer) and SVD import (FDP_UIT.1/SVD Transfer).
- a communication channel between itself and SCA. This trusted channel, either initiated by the TOE or the SCA is used for import of the DTBS-representation from the SCA intended to be signed by the TOE (FTP_ITC.1/DTBS import and FDP_UIT.1 / TOE DTBS)
- a communication path (using a trusted channel) between itself and a local user. This trusted channel (used for establishing the trusted path), either initiated by the TOE or the local user, is used for initial user authentication (VAD).

  Application note:
  To obtain a complete trusted path, the SCA (environment) has to protect the data during those parts of the transmission from the user that are not protected by secure messaging (i.e. the trusted channel).

All three of these secure messaging communications represent channels (paths) that are logically distinct from other communication channels (paths) and provide assured identification of its end points and protection of the channel (path) data from modification or disclosure.

The TOE permits the CGA, the SCA and the local user to initiate communication via the trusted channel (path) (FTP_ITC.1/SVD Transfer, FTP_ITC.1/DTBS import and FTP_TRP.1/TOE).

The TOE enforces secure messaging (integrity and confidentiality) for changing the RAD in form of PIN/PUK with entry of the old PIN/PUK data (VAD) (FMT_SMF.1(4)).

The TOE enforces secure messaging (integrity and confidentiality) for unblocking and changing the RAD in form of PIN with entry of the PUK data (VAD) and new PIN data (FMT_SMF.1(4)).

The TOE enforces secure messaging (integrity and confidentiality) for verification of the Transport-PIN data (VAD) needed for the setting of the security attribute “SCD operational” to “yes”.

The secure messaging is done by using card and application individual keys KA and KC, being derived from the card serial number (ICCSN) and a set of global master keys MK_KA and MK_KC . The KA and KC stored in the card are pre-calculated during the personalization phase. The KA and KC used by the terminal will be temporarily calculated (derived) from the appropriate global master keys MK_KA and MK_KC after the ICCSN has been requested from the card.

KA is used to ensure the integrity in the authentic mode (MAC3 resp. Retail-MAC with ANSI Padding) and KC is used to additionally protect the confidentiality in the combined mode (DES3 CBC with ISO-Padding).

6.1.7 SF7 SVD Transfer

The TOE allows the SVD to be exported by the users “Administrator” or “Signatory” (FDP_ACC.1/SVD Transfer SFP and FDP_ACF.1/SVD Transfer SFP). When exporting the SVD the TSF shall export the SVD without the user data’s associated security attributes (FDP_ETC.1/SVD Transfer).

The TOE enforces the SVD to be exported in a manner ensuring these user data to be protected from modification and insertion errors during transmission. Furthermore, the TOE is also able to determine on receipt of user data, whether modification and insertion has occurred (FDP_UIT.1/SVD Transfer). Therefore, the TOE or the CGA initiates communication via the trusted channel (with properties described in SF6 in the previous section) for export SVD (FTP_ITC.1/SVD Transfer).

The TOE can perform a SCD / SVD correspondence verification method with the Signatory being authenticated, with the Signatory not being authenticated and during key pair generation. These methods are in accordance with the cryptographic algorithm RSA with key sizes of 1024 up to 1752 bit (FCS_COP.1/CORRESP):

- SCD / SVD correspondence verification **with** Signatory:
  In the presence of the “Signatory” the “Administrator” prepares a certificate request for the CGA that is signed with the SCD for which the “Signatory” has to enter his PIN (VAD). The signature allows the CGA to verify the authenticity of the SVD.
- SCD / SVD correspondence verification **without** Signatory:
  The TOE provides a command ‘Proof of Correspondence’, which always allows to ensure the correspondence of SVD data sent to the TOE and the SCD stored in the TOE .
- SCD / SVD correspondence verification during key pair generation:
  During key pair generation the correspondence between the generated SCD and SVD is always checked before the key pair is stored persistently.

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 assessed according 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 6.2-: SOF claim

TSF	SOF Claim	Probabilistic or permutational mechanisms
SF1 User Identification and Authentication	SOF-high	PIN, PUK
SF2 Access Control	–	–
SF3 SCD/SVD Pair Generation	SOF-high	Prime number test
SF4 Signature Creation	SOF-high[101]	Signature Creation
SF5 Protection	–	–
SF6 Secure Messaging	SOF-high	Command diversification
SF7 SVD Transfer	SOF-high[101]	Proof / Verification of SCD / SVD correspondence

[101] 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

This Security Target claims conformance to the following protection profile:

- Protection Profile – Secure Signature-Creation Device (SSCD-PP) Type 3, Version 1.05, EAL 4+, CWA 14169:2002 (E), 25.07.2001, [16]

The short term for this protection profile used in this document is SSCD-PP.

7.2 PP Refinements

Refinements were made for the following Security Functional Requirements:

FDP_ACF.1 / Signature Creation SFP (cf. section 5.1.2.2)
The set of rules that explicitly deny access to the controlled objects (stated within element FDP_ACF.1.4 / Signature Creation SFP) are completed to prevent any ambiguity.

Within the following SFRs the term 'List of approved algorithms and parameters' as given by [16] is specified more precisely by stating the concrete list of standards:

FCS_CKM.1.1	(cf. section 5.1.1.1)
FCS_COP.1.1 / Corresp	(cf. section 5.1.1.3)
FCS_COP.1.1 / Signing	(cf. section 5.1.1.3)
FCS_CKM.2.1 / CGA	(cf. section 5.3.1.1)
FCS_COP.1.1 / SCA Hash	(cf. section 5.3.2.1)

7.3 PP Additions

Due to [[9]] the Functional Security Requirement FMT_SMF.1 (cf. 5.1.4.6) has been added as a direct dependency from FMT_MOF.1, FMT_MSA.1 and FMT_MTD.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.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					

8.1.2 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 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.

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

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), 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 are 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_Resistance, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

T.Sig_Repud (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGA_QCert (Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signature-creation data), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed) 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_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.

8.1.2.3 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.

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.

8.2 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.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			
FCS_CKM.4		x		x								
FCS_COP.1/CORRESP					x							
FCS_COP.1/SIGNING												x
FDP_ACC.1/INITIALISATION SFP			x	x								
FDP_ACC.1/PERSONALISATION SFP											x	
FDP_ACC.1/SIGNATURE-CREATION SFP										x	x	
FDP_ACC.1/SVD TRANSFER SFP						x						
FDP_ACF.1/INITIALISATION SFP			x	x								
FDP_ACF.1/PERSONALISATION SFP											x	
FDP_ACF.1/SIGNATURE-CREATION SFP										x	x	
FDP_ACF.1/SVD TRANSFER SFP						x						

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
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[102]			x	x							x	
FMT_SMR.1				x							x	
FPT_AMT.1		x		x								x
FPT_EMSEC.1	x											
FPT_FLS.1				x				x				
FPT_PHP.1							x					
FPT_PHP.3								x				
FPT_TST.1		x										x
FTP_ITC.1/SVD TRANSFER						x						
FTP_ITC.1/DTBS IMPORT										x		
FTP_TRP.1/TOE											x	

[102] 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
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: 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	ADV_IMP.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.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 and FMT_SMF.1 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 users 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, FMT_SMF.1 corresponding to the actual TOE (i.e., FMT_MSA.1/ADMINISTRATOR, FMT_MSA.3), and FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.
The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been used for signature creation and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.
The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_AMT.1 and FPT_FLS.1 test the working conditions of the TOE and guarantee a secure state when integrity is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS is differential fault analysis (DFA).
The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation, AVA_SOF HIGH by requesting strength of function high for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, 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 transferred DTBS-representation to be signed is to be verified , and that the DTBS-representation is not altered by the TOE.. This is provided by the trusted channel integrity verification mechanisms of FDP_ITC.1/DTBS, FTP_ITC.1/DTBS IMPORT, and by FDP_UIT.1/TOE DTBS. The verification that the DTBS-representation has not been altered by the TOE is done by integrity functions specified by FDP_SDI.2/DTBS. The access control requirements of FDP_ACC.1/SIGNATURE CREATION SFP and FDP_ACF.1/SIGNATURE CREATION SFP keep unauthorised parties off from altering the DTBS-representation.

OT.Sigy_SigF (Signature generation function for the legitimate signatory only) is provided by FIA_UAU.1 and FIA_UID.1 that ensure that no signature generation function can be invoked before the signatory is identified and authenticated.
The security functions specified by FDP_ACC.1/PERSONALISATION SFP, FDP_ACC.1/SIGNATURE-CREATION SFP, FDP_ACF.1/PERSONALISATION SFP, FDP_ACF.1/SIGNATURE-CREATION SFP, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1 ensure that the signature process is restricted to the signatory.
The security functions specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, and FMT_MSA.3 ensure that the access to the signature generation functions remain under the sole control of the signatory, as well as

FMT_MSA.1/SIGNATORY provides that the control of corresponding security attributes is under signatory's control.
The security functions specified by FDP_SDI.2 and FTP_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 and by AVA_VLA.4 by requesting that these resist attacks with a high attack potential. 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 users can export the SVD to the CGA.

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

OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to resist physical attacks. FPT_FLS.1 preserves a secure state in occurrence of a failure caused by external effects.

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) covers confidentiality and integrity of the VAD during the identification and authentication of the Signatory 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.

8.3 Dependency Rationale

8.3.1 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 6.4.2 for justification).

Table 8.5 Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FCS_CKM.1	FCS_COP.1/SIGNING, FCS_COP.1/CORRESP, 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[103]
FMT_MSA.1 / Administrator	FDP_ACC.1/Initialisation SFP, FMT_SMR.1, FMT_SMF.1[103]
FMT_MSA.1 / Signatory	FDP_ACC.1/ Signature_Creation SFP, FMT_SMR.1, FMT_SMF.1[103]

[103] See the note in section 5.1.4.6.

Requirement	Dependencies
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[103]
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 (GGA)	
FCS_CKM.2 / CGA	unsupported dependencies, see sub-section 8.3.2 for justification

Requirement	Dependencies
FCS_CKM.3 / CGA	unsupported dependencies, see sub-section 8.3.2 for justification
FDP_UIT.1 / SVD IMPORT	FTP_ITC.1/SVD IMPORT, unsupported dependencies, see sub-section 8.3.2 for justification,
FTP_ITC.1 / SVD IMPORT	None
Functional Requirements for Signature creation application (SCA)	
FCS_COP.1 / SCA HASH	Unsupported dependencies, see sub-section 8.3.2 for justification
FDP_UIT.1 / SCA DTBS	FTP_ITC.1/ SCA DTBS, unsupported dependencies on FDP_ACC.1, see sub-section 8.3.2 for justification
FTP_ITC.1 / SCA DTBS	None
FTP_TRP.1 / SCA	None

8.3.2 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.

Requirement	Unsupported dependencies
FCS_CKM.2/ CGA	The CGA generates qualified electronic certificates 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 the scope of this PP.
FCS_CKM.3/ CGA	The CGA imports SVD via trusted channel implemented by FTP_ITC.1/ SVD import. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside the scope of this PP.
FDP_UIT.1/ SVD Import (CGA)	The access control (FDP_ACC.1) for the CGA is outside the scope of this PP.
FCS_COP.1/ SCA HASH	The hash algorithms implemented by FCS_COP.1/SCA HASH do 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 is outside the scope of this PP.

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

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	SF6 Secure Messaging	SF7 SVD Transfer
FCS_CKM.1			x				
FCS_CKM.4			x				
FCS_COP.1/CORRESP			x				x
FCS_COP.1/SIGNING				x			
FDP_ACC.1/INITIALISATION SFP		x					
FDP_ACC.1/PERSONALISATION SFP	x						
FDP_ACC.1/SIGNATURE-CREATION SFP		x					
FDP_ACC.1/SVD TRANSFER SFP							x
FDP_ACF.1/INITIALISATION SFP		x					
FDP_ACF.1/PERSONALISATION SFP	x						
FDP_ACF.1/SIGNATURE-CREATION SFP		x					
FDP_ACF.1/SVD TRANSFER SFP							x
FDP_ETC.1/SVD Transfer							x
FDP_ITC.1/DTBS		x					
FDP_RIP.1					x		
FDP_SDI.2/Persistent					x		
FDP_SDI.2/DTBS					x		
FDP_UIT.1/SVD TRANSFER						x	x
FDP_UIT.1/TOE DTBS						x	
FIA_AFL.1	x						
FIA_ATD.1	x						
FIA_UAU.1	x						
FIA_UID.1	x						
FMT_MOF.1		x					
FMT_MSA.1/Administrator		x					
FMT_MSA.1/Signatory		x					
FMT_MSA.2			x	x			
FMT_MSA.3		x					
FMT_MTD.1	x	x					
FMT_SMF.1[104]	x	x				x	
FMT_SMR.1	x	x					
FPT_AMT.1					x		
FPT_EMSEC.1	x		x	x			
FPT_FLS.1					x		

[104] See the note in section 5.1.4.6.

TOE Security Functional Requirement / TOESecurity Function	SF1 User Identification and Authentication	SF2 Access Control	SF3 SCD/SVD Pair Generation	SF4 Signature Creation	SF5 Protection	SF6 Secure Messaging	SF7 SVD Transfer
FPT_PHP.1					x		
FPT_PHP.3					x		
FPT_TST.1					x		
FTP_ITC.1/SVD TRANSFER						x	x
FTP_ITC.1/DTBS IMPORT						x	
FTP_TRP.1/TOE						x	

8.5.2 TOE Security Function Sufficiency

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

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

TOE Security Assurance Requirements	TOE Assurance Measures
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 TSFs is already considered in the description of the TSFs in section 6 by using references. The following table summarises the mutual supportiveness between the TSFs.

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 ensuring that the RAD can not be easily guessed by measurement of power consumption or electromagnetic radiation and SF6 ensuring that the VAD and RAD can not be easily eavesdropped during transmission from the terminal.
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 supports this TSF for the correspondence proof.
SF4 Signature Creation	Before this TSF can be used for signature creation, SF1 is responsible for the signatory's 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 TSFs by testing and protecting the TOE.
SF6 Secure Messaging	SF6 supports all TFSs sending or receiving data such as VAD, RAD, DTBS or SVD whose integrity or confidentiality (or both) has to be protected (i.e. SF1, SF4 and SF7).
SF7 SVD Transfer	SF4 supports this TSF for all cases of correspondence proof (Signatory or Administrator creates a signature for the correspondence proof, command Proof Of Correspondence and during key pair generation).

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 the TOE will be issued to users and will, after personalization, 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

According to section 7 this Security Target claims conformance to the Protection Profile – Secure Signature-Creation Device (SSCD-PP) Type 3, [16].

The sections of this document, where threats, objectives and security requirements are defined, clearly state, which of these items are taken from the Protection Profile and which are added in this ST (cf. also sections 7.2 and 7.3). Therefore this is not repeated here. In addition the items added in this Security Target do not contradict the items included in the Protection Profile. The operations done for the SFRs taken from the PP are also clearly indicated.

The assurance level claimed for this target (EAL4+, shown in section 1.3 and 5.2) meets the requirements claimed by the PP (EAL4+).

These considerations show that the Security Target correctly claims conformance to the SSCD-PP.

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] CardOS V4.2B Chipcard Operating System, CAT, DRNG and WIPE Packages & Release Notes, Siemens, Edition 05/2007

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

[4] 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

[5] ISO/IEC 10118-3: 1998 Information technology – Security techniques– Hash functions - Part 3: Dedicated hash functions

[6] RSA Laboratories, PKCS #1 v2.1: RSA Encryption Standard, RSA Laboratories, June 14th, 2002

[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+, CWA 14169:2002 (E), 25.07.2001

[17] Certification report for Infineon Smart Card IC (Security Controller) SLE66CX322P with RSA2048/m148418 from Infineon Technologies AG, certification file BSI-DSZ-CC-0266-2005, BSI, 22.04.2005, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[18] Data Encryption Standard (DES), FIPS PUB 46-3, US NBS, 1977, reaffirmed 1999 October 25, Washington

[19] NIST Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm, US Department of Commerce, October 1999

[20] ANSI X9.19, Financial Institution Retail Message Authentication, 1996

[21] Administrator Guidance CardOS V4.2B_FIPS with Application for Digital Signature, Siemens AG, DS1, Version 1.4, Edition 07/2007

[22] User Guidance CardOS V4.2B_FIPS with Application for Digital Signature, Siemens AG, DS1, Version 1.4, Edition 06/2007

[23] CardOS V4.2B_FIPS ADS Description, Version 1.0, Siemens AG, DS1, 05/2007

[24] 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)

[25] 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)

[26] 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)

[27] 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)

[28] 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 12. April 2007 im Bundesanzeiger Nr. 69, S. 3759, Vom 22. Februar 2007, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

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

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

[31] FIPS PUB 140-2: Security Requirements for Cryptographic Modules, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 25.05.2001. Change Notices 2, 3 and 4: 03.12.2002

[32] CardOS V4.2B Chipcard Operating System, Packages & Release Notes, Siemens, Edition 05/2007

[33] CardOS V4.2B Chipcard Operating System, User's Manual, Siemens, Edition 09/2005

[34] Common Criteria for Information Technology Security Evaluation – Part3: Security assurance requirements, Version 2.1, August 1999, CCIMB-99-033

9.2 Acronyms

CC	Common Criteria
CGA	Certification Generation Application
DS	Digital Signature
DTBS	Data to be signed
EAL	Evaluation Assurance Level
IT	Information Technology
PIN	Personal Identification Number
PIN_T	Transport-PIN
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