SIEMENS

CardOS â V4.4

Security Target
CardOS V4.4 with Application for QES

Edition 04/2010

SIEMENS

Siemens AG
SIS PS CNS SCS
Otto-Hahn-Ring 6

D-81739 Munich
Germany

Disclaimer of Liability

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

Contents

Document History

Version	Release Date	Changed Chapter(s)	Remarks	Author	Sent to Receiver on Date
0.10	14.08.09		First version	Ulrike Ludwig, Andreas Furch, Siemens AG	T-Systems, Dr. Alla Gnedina, Evaluator, on 14.08.09
0.20	20.08.09	7.2 7.3	Additions Addition of 7.3	Ulrike Ludwig Siemens AG	T-Systems, Dr. Alla Gnedina, Evaluator, on 20.08.09
0.30	18.09.09	1.3 3 6.1 7.3 8.3	Addition Added asset Editorial updates Update of 7.3 New glossary	Ulrike Ludwig, Andreas Furch, Siemens AG	T-Systems, Dr. Alla Gnedina, Evaluator, on 18.09.09
0.40	27.11.09	1.3, 1.4, 1.5 (deleted), 7.1.4	Editorial changes, corrections within table 1, removal of internal SHA-1 generation	Andreas Furch, Siemens AG	T-Systems, Dr. Alla Gnedina, Dr. Igor Furgel, Evaluator, on 27.11.09
0.50	29.04.10	1.4, 6.1.1.1, 3.3, 4.2, 4.3	Editorial changes, corrections within table 1, renaming of keygen algorithm, added OSP and OE	Andreas Furch, Siemens AG	Dr. Igor Furgel, Dr. Alla Gnedina, Evaluator, T-Systems, 29.04.2010

1 ST Introduction

1.1 ST Reference

Title: Security Target CardOS V4.4 with Application for QES
Authors: Siemens AG, H SR CRM IPD
CC Version: 3.1, Revision 2
General Status: Draft
Version Number: 0.50 (29.04.10)

The TOE is based on the Infineon chip SLE66CX680PE as ICC platform, which requires a composite evaluation.

This ST provides
- an introduction, in this section,
- the conformance claims in section 2,
- the security problem definition in section 3,
- the security objectives in section 4,
- the extended components definition in section 5,
- the security and assurance requirements in section 6,
- the TOE summary specification (TSS) in section 7, and
- the references in section 8.

1.2 TOE Reference

The TOE “CardOS V4.4 with Application for QES Version 1.00” is based on the Infineon chip SLE66CX680PE (m1534-a14) as ICC platform, which is loaded by the chip manufacturer with the operating system CardOS V4.4. The hardware and the software of the TOE is determined by the components listed within Table 1.
The Trustcenter afterwards personalizes the chipcard with an Application for Qualified Electronic Signatures (QES).

The operating system CardOS V4.4 has the version identifier ‘C80D’.
The TOE may additionally be identified by its factory key values, the historical bytes in the default ATR and the responses to the version dependent GET DATA modes.

The Application for QES can be personalized in two different ways, which are named
‘Centralized model’ and ‘De-centralized model’. Apart from that, different configurations within the models are possible. The variants are determined through the use of the appropriate personalization scripts (cf. Table 1, row 2) or through other personalization processes that guarantee the same result.

1.3 TOE Overview

TOE type

The TOE as defined by this Composite Security Target is a smart card. It is to be used as a Secure Signature Creation Device (SSCD). The smart card is based on an Infineon Chip.

Usage and major security features of the TOE

The TOE allows to generate cryptographically strong Signatures over previously externally calculated hash-values. The TOE generates the signature key pair (SCD/SVD). 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. The restriction on the access to the secret key is done via the well-known PIN authentication mechanism.

Required non-TOE hardware/software/firmware

The smart card on which the TOE bases conforms to ISO 7816 that needs the usual IT environment for such smart cards, i.e. at least a smart card terminal connected to a host equipped with software that is able to communicate with the terminal. As the TOE is conformant to certain laws and regulations concerning qualified electronic signatures, the IT environment may have to be conformant to the same laws and regulations as well if they are applicable for the intended usage.

1.4 TOE Description

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 (SLE66CX680PE from Infineon) used to implement the secure signature-creation device (SSCD) and iii) the pertaining guidance documentation 'User Guidance CardOS V4.4' [19] and 'Administrator Guidance CardOS V4.4' [18]. Therefore the TOE is considered to be a product.

The TOE developer delivers the ROM mask, script-files and pertaining documentation. The Trust Center (certification authority, CA, or CSP) or entities acting under the CA policy initialize and personalize the TOE.

The TOE utilises the evaluation of the underlying platform, which includes the Infineon chip SLE66CX680PE, the IC Dedicated Software and the RSA2048 crypto library V1.5.

The chip SLE66CX680PE is certified for the production site Dresden in Germany (production line indicator '2') (cf [21], Certification Report BSI-DSZ-CC-0437-2008 for SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA 2048 V1.5, and all with specific IC dedicated software from Infineon Technologies AG, 27.Mai 2008, Bundesamt für Sicherheit in der Informationstechnik (BSI)). Other production sites that will be added in the future via Maintenance Reports published by the BSI are also possible.

Table 1: Components of the TOE

No.	Type	Term	Version	Date	Form of delivery
1	Software (Operating System)	CardOS V4.4	C80D	23.06.09	loaded in ROM / EEPROM
2	V4.4 Software Application Digital Signature (Application / Data Structure)	***Centralized Model***: PersAppSigG.CSF	The final versions of these files will be defined at the end of the evaluation and will be listed		Personalization Script Files in **CSF format**, after whose execution the ADS will be loaded
		PersAppSigG_withoutPUK.CSF			
		De-Centralized Model: Pre-PersAppSigG.CSF			
		Post-PersAppSigG.CSF			
		Pre-PersAppSigG_withoutPUK.CSF			
		Post-PersAppSigG_withoutPUK.CSF			
		Mass_Pre-PersAppSigG.CSF			
		Mass_Post-PersAppSigG.CSF			
		Both Models: Defines_1024.csf			

No.	Type	Term	Version	Date	Form of delivery
		Defines_1280.csf Defines_1536.csf Defines_1792.csf Defines_2048.csf	in the certification report		in EEPROM
3	Service Package (mandatory)	Service Package	The final versions of these files will be defined at the end of the evaluation and will be listed in the certification report		Personalization Script Files in CSF format, after whose execution the resp. code will be loaded in EEPROM (included in the (Pre-) Pers-CSF-Scripts above)
4	Software Verify_RC Package (mandatory)	Verify_RC Package			
5	Software SHA-2 Package (optional)	SHA-2 Package			
6	Documentation	CardOS License Package Tool Manual	1.3	09/2005	Paper form or PDF-File
7	Documentation	CardOS V4.2B User's Manual	1.0	09/2005	
8	Documentation	CardOS V4.4 Packages & Release Notes	The final versions of these documents will be defined at the end of the evaluation and listed in the certification report		
9	Admin Documentation	CardOS V4.4 Administrator Guidance			
10	User Documentation	CardOS V4.4 User Guidance			
11	ADS Documentation	CardOS V4.4 ADS_Description			
12	Hardware (Chip)	Infineon SLE66CX680PE	m1534-a14 (Dresden)		Module
	Firmware RMS	RMS	RMS V2.5		Stored in reserved area of User ROM
	Software crypto library	RSA2048 crypto library	Version 1.5		Loaded in ROM
13	Firmware STS	Self Test Software	V55.0B.07		Stored in Test ROM

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

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

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 reference authentication data (RAD).

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

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

Figure 1 shows the ST scope from the structural perspective. The TOE comprises the 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 in a trusted environment.

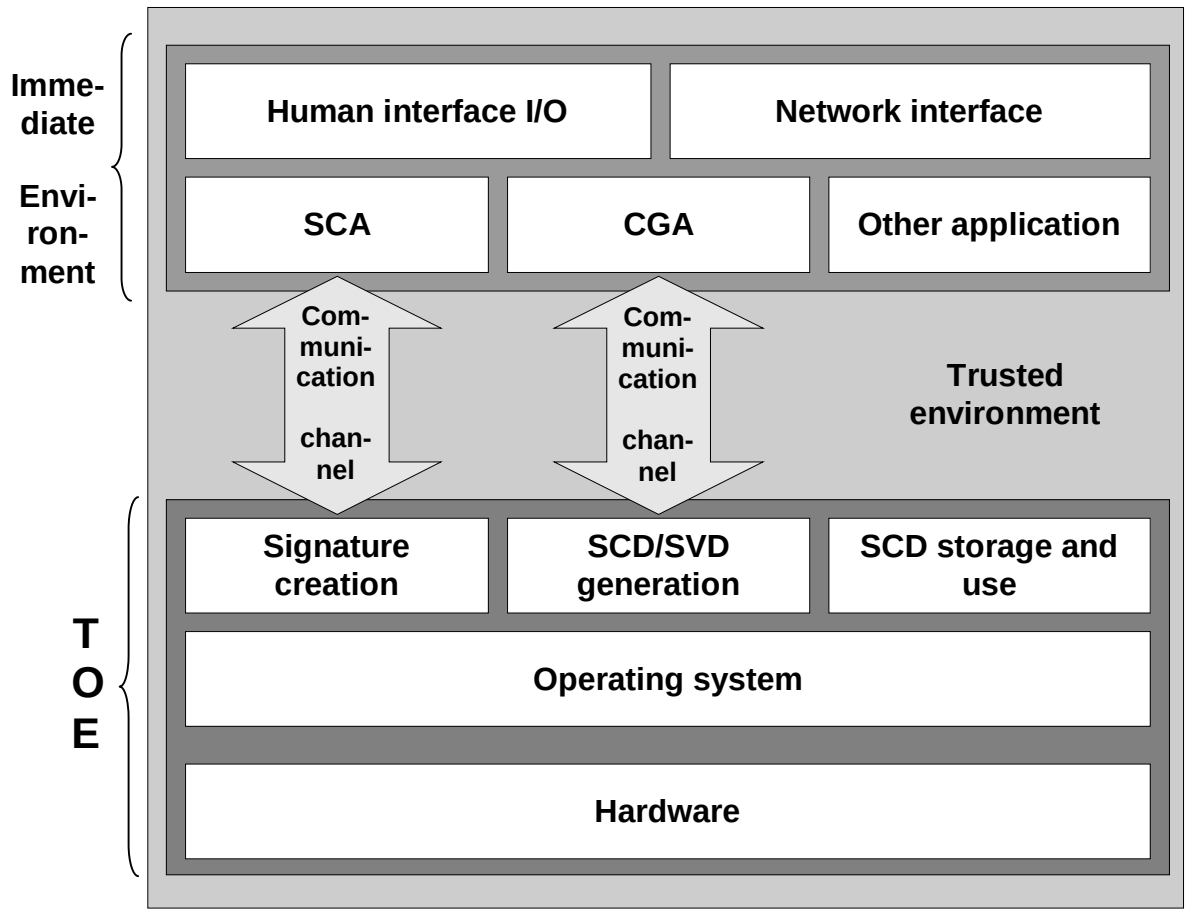


Figure 1: Scope of the SSCD, structural view

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

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

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

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

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

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

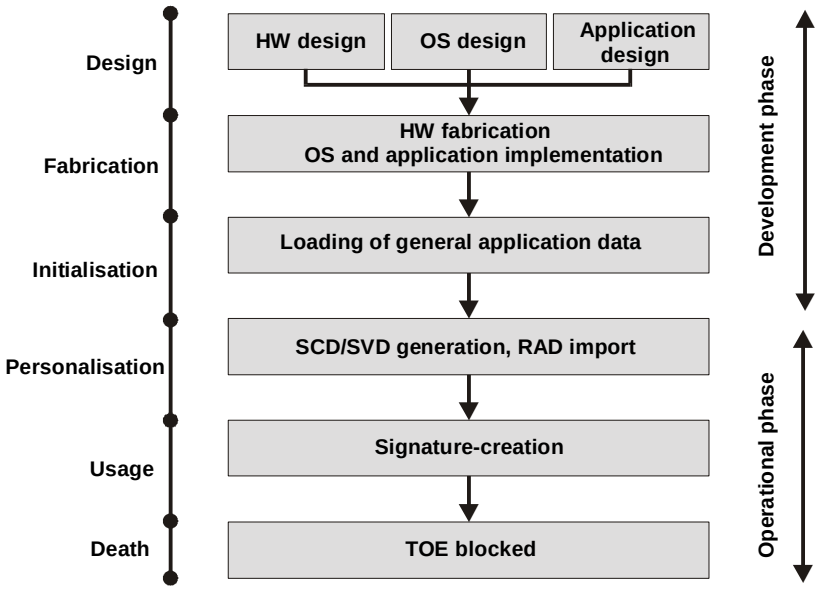


Figure 2: SSCD life cycle

2 Conformance Claims

The TOE is a composite product, as it is based on the Infineon Security Controller SLE66CX680PE, which has been evaluated and certified as being conformant to the Common Criteria version 2.3, CC Part 2 extended, and CC Part 3 conformant (cf. [21]).

As required by AIS36 [24] compatibility between this Composite Security Target and the Platform Security Target [25] of the Infineon chip SLE66CX680PE is claimed. In section 7.2, Usage of Platform TSF by TOE TSF a detailed mapping shows how the Platform TSF are separated into i) relevant Platform TSF (Table 9) being used by the composite ST and ii) irrelevant Platform TSF (Table 10) not being used by the composite ST.

2.1 CC Conformance Claim

This ST claims conformance to the Common Criteria version 3.1 Release 2, cf. [8], [9], and [10].
The ST is CC Part 2 [9] extended, CC Part 3 [10] conformant and the assurance level for this ST is EAL4 augmented.
The short terms for Common Criteria version 3.1 Release 2, Part 1, Part 2 and Part 3 and for the Common Methodology for Information Technology Security Evaluation, version 3.1 used in this document are

- CC-3.1-P1,
- CC-3.1-P2,
- CC-3.1-P3, and
- CEM-3.1 respectively.

For the evaluation the following methodology will be used:

- **Common Methodology for Information Technology** Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007, CCMB-2007-09-004

2.2 PP Claim, Package Claim

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

The assurance level for the TOE is EAL4 augmented. Augmentation results from the selection of:

AVA_VAN.5 Vulnerability Assessment - Advanced Methodical Vulnerability Analysis – Highly resistant

The evaluation is a composite evaluation and uses the results of the chips' CC evaluation provided by [21]. The IC with its primary embedded software is evaluated at level EAL 5 with a minimum strength level for its security functions of SOF-high.

The chip SLE66CX680PE is conformant to the

- **Smartcard IC Platform Protection Profile** (SSVG-PP), Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001, [22]

2.3 Conformance Rationale

2.3.1 PP Claims Rationale

The Security Target does not include a PP claim, see also section 2.2.

2.3.2 Rationale for Assurance Level 4 Augmented

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

AVA_VAN.5 Vulnerability Assessment - Advanced Methodical Vulnerability Analysis – Highly resistant

To allow the evaluator an advanced methodical vulnerability analysis and the required penetration testing the developer has to provide the following items:

- the Security Target,
- the functional specification,
- the TOE design,
- the security architecture description,
- the implementation representation,
- the guidance documentation, and
- the TOE suitable for testing

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_VAN.5 has the following dependencies

- ADV_ARC.1 Security Architecture Description,
- ADV_FSP.2 Security Enforcing Functional Specification,
- ADV_TDS.3 Basic Modular Design,
- ADV_IMP.1 Implementation Representation
- AGD_OPE.1 Operational User Guidance,
- AGD_PRE.1 Preparative Procedures

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

3 Security Problem Definition

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

Assets:

1. SCD: private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).
2. SVD: public key linked to the SCD and used to perform an electronic signature verification.
3. DTBS and DTBS-representation: set of data, or its representation which is intended to be signed.
4. VAD: PIN, PUK (optional) and Transport-PIN code entered by the End User to perform authentication attempts.
5. RAD: Reference PIN, PUK (optional) and Transport-PIN code used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)
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).
8. SCD/SVD parameters. parameters, that ensure the correct generation of a SCD/SVD key pair.

Subjects:

Subjects	Definition
S.User	End user of the TOE which can be identified as S.Admin or S.Signatory
S.Admin	User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions.
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.

Threat agents:

S.OFFCARD	Attacker. A human or a process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker is to access Application sensitive information. The attacker has a **high level attack potential** and **knows no secrets**.

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

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

3.1 Assumptions

A.CGA *Trustworthy certification-generation application*

The CGA protects the authenticity of the Signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.

A.SCA *Trustworthy signature-creation application*

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

3.2 Threats to Security

T.Hack_Phys *Physical attacks through the TOE interfaces*

An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat addresses all the assets.

T.SCD_Divulg *Storing, copying, and releasing of the signature-creation data*

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

T.SCD_Derive *Derive the signature-creation data*

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

T.Sig_Forgery *Forgery of the electronic signature*

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

T.Sig_Repud *Repudiation of signatures*

If an attacker can successfully threaten any of the assets, then the non repudiation of the electronic signature is compromised. This results in the signatory being able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.

T.SVD_Forgery *Forgery of the signature-verification data*

An attacker forges the SVD presented by the TOE to the CGA. This results 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 [1], 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 Annex I of the Directive [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.

P.Env_KeyGen *Environment for key generation*
Generation of the SCD/SVD key pair only takes place during initialisation/personalisation within a trusted environment.

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 modification.

4.1 Security Objectives for the TOE

OT.EMSEC_Design *Provide physical emanations security*

Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.

OT.Lifecycle_Security *Lifecycle security*

The TOE shall detect flaws during the initialisation, personalisation and operational usage.

OT.SCD_Secrecy *Secrecy of the signature-creation data*

The secrecy of the SCD (used for signature generation) is reasonably assured against attacks with a high attack potential.

OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*

The TOE shall ensure the correspondence between the SVD and the SCD in the TOE.

OT.Tamper_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.SCD_Unique *Uniqueness of the signature-creation data*

The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligibly low.

OT.Sigy_SigF *Signature generation function for the legitimate signatory only*

The TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

OT.Sig_Secure *Cryptographic security of the electronic signature*

The TOE generates electronic signatures that can not be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the electronic signatures. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.

4.2 Security Objectives for the Operational Environment

OE.CGA_QCert *Generation of qualified certificates*

The CGA generates qualified certificates which include inter alia
(a) the name of the signatory controlling the TOE,
(b) the SVD matching the SCD implemented in the TOE,
(c) the advanced signature of the CSP.

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

The CGA ensures the integrity and authenticity of the SVD received from the TOE. The CGA ensures the correspondence between the SVD received from the TOE and the SVD in the qualified certificate.

OE.HI_VAD *Protection of the VAD*

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

OE.SCA_Data_Intend *Data intended to be signed*

The SCA
(a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,
(b) sends the DTBS-representation to the TOE and
(c) attaches the signature produced by the TOE to the data or provides it separately.

OE.SCA_Trusted_Env *Trusted environment*

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

OE.Env_KeyGen *Generation of SCD/SVD key pairs*
Generation of the SCD/SVD key pair is only started by the Administrator during initialisation/personalisation within a trusted environment.

4.3 Security Objectives Rationale

4.3.1 Security Objectives Coverage

Table 2: Security Environment to Security Objectives Mapping

Threats - Assumptions - Policies / Security objectives	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.Sigy_SigF	OT.Sig_Secure	OE.CGA_QCert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend	OE.SCA_Trusted_Env	OE.Env_KeyGen
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		
T.Sig_Repud	x	x	x	x	x	x	x	x	x	x	x		x	x	
A.CGA										x	x				
A.SCA													x	x	
P.CSP_QCert				x						x					
P.QSign								x	x	x			x		
P.Sigy_SSCD			x				x	x							
P.Env_KeyGen															x

4.3.2 Security Objectives Sufficiency

4.3.2.1 Policies and Security Objective Sufficiency

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

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

DTBS-representation to the TOE. OT.Sig_Secure and OT.Sigy_SigF address the generation of advanced signatures by the TOE.

P.Sigy_SSCD (TOE as secure signature-creation device) establishes the TOE as secure signature-creation device of the signatory with practically unique SCD. This is addressed by OT.Sigy_SigF ensuring that the SCD is under sole control of the signatory, OT.SCD_Unique ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature and by OT.SCD_Secrecy which preserves the secrecy of the SCD.

P.Env_KeyGen (Environment for key generation) provides that the SCD/SVD key pair is only generated during initialisation/personalisation within a trusted environment. This is obviously assured by OE.Env_KeyGen

4.3.2.2 Threats and Security Objective Sufficiency

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

T.SCD_Divulg (Storing, copying, and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [1] , recital (18). This threat is countered by OT.SCD_Secrecy which assures the secrecy of the SCD used for signature generation.

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

T.DTBS_Forgery (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which then does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The TOE IT environment addresses T.DTBS_Forgery by means of OE.SCA_Data_Intend and OE.SCA_Trusted_Env.

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

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. This threat is in general addressed by OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (Data intended to be signed), OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OE.SVD_Auth_CGA (CGA ensures the integrity and authenticity of the SVD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_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 ensures that the methods used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation are appropriate for the cryptographic methods employed to generate the electronic signature. The combination of OE.CGA_QCert, OT.SCD_SVD_Corresp and OE.SVD_Auth_CGA provides the integrity and authenticity of the SVD that is used by the signature verification process. OT.Sig_Secure, OT.SCD_Secrecy, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

T.Sig_Repud (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGA_QCert (Generation of qualified certificates), OE.SVD_Auth_CGA (CGA ensures the integrity and authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signature-creation data), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security) , OT.Tamper_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 (Data intended to be signed) and OE.SCA_Trusted_Env (Integrity of the DTBS-representation).
OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert and OE.SVD_Auth_CGA ensure the integrity and authenticity of the SVD.
OE.CGA_Qcert, OT.SCD_SVD_Corresp and OE.SVD_Auth_CGA ensure that the SVD in the certificate corresponds to the SCD that is implemented by the SSCD of the signatory.
OT.SCD_Unique provides that the signatory’s SCD can practically occur just once.
OT.Sig_Secure, OT.SCD_Secrecy, OT.Tamper_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 OE.SCA_Trusted_Env ensure that the TOE generates electronic signatures only for DTBS-representations which the signatory has decided to sign as DTBS.

T.SVD_Forgery (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.SCD_SVD_Corresp by ensuring the correspondence between the SVD and SCD stored in the TOE. The export of the SVD is addressed by OE.SVD_Auth_CGA. The trusted environment of the CGA ensures the integrity and authenticity of the SVD sent by the TOE. The CGA furthermore ensures the correspondence between the SVD received by the CGA and the SVD identified in the qualified certificate.

4.3.2.3 Assumptions and Security Objective Sufficiency

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

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

5 Extended Components Definition

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined in section 5.1 below like in the Protection Profile – Secure Signature-Creation Device (SSCD-PP) Type 3 [16], section 6.6.

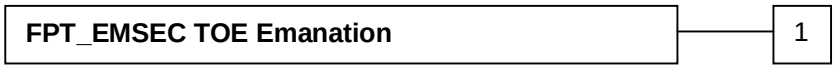
This ST does not define or use other extensions to CC-3.1-P2 [9].

5.1 FPT_EMSEC TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE Emanation has two constituents:

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

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

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.1.1	The TOE shall not emit [assignment: *types of emissions]* in excess of [assignment: specified limits] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMSEC.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

Hierarchical to: No other components.

Dependencies: No other components.

5.2 Rationale for Extensions

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on externally observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations.

6 Security Requirements

This chapter provides the security functional requirements and the security assurance requirements for the TOE.

Security functional requirements components given in section 6.1 “Security Functional Requirements” (except FPT_EMSEC.1 which is explicitly stated) are drawn from Common Criteria part 2 [9]. Some security functional requirements represent extensions to [9]. Operations for assignment, selection and refinement have been made. Operations are identified by an underlined italic font, e.g. *RSA*.
Operations whose meaning may not be implicitly clear are described in more detail in the glossary (see chap. 8.3)

The TOE security assurance requirements given in section 6.2 “Security Assurance Requirements” are drawn from the security assurance components from Common Criteria part 3 [10].

The original text for the elements taken from CC3.1-P2 [9] for each in this ST performed operation is additionally stated in footnotes.

6.1 Security Functional Requirements

6.1.1 Cryptographic support (FCS)

6.1.1.1 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 Key Generator*[1] and specified cryptographic key sizes *1024 up to 2048 bit in 8 bit steps*[2] that meet the following:

Geeignete Algorithmen [4][3].

6.1.1.2 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 The TSF shall perform *digital signature-generation*[4] in accordance with a specified cryptographic algorithm *RSA*[5] and cryptographic key sizes *1024 up to 2048 bit in 8 bit steps*[6] that meet the following:

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

(2) *Geeignete Algorithmen [4]*[7]

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

6.1.2 User data protection (FDP)

6.1.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the *Signature-creation SFP*[8] on *signing of DTBS-representation by Signatory*[9].

6.1.2.2 Security attribute based access control (FDP_ACF.1)

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

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

FDP_ACF.1.1 The TSF shall enforce the *Signature-creation SFP*[10] to objects based on the following: *General attribute and Signature creation attribute*[11].

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

A User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures with the SCD for DTBS sent by the SCA if the security attribute "SCD operational" is set to "yes".[12]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[13].

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

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

(b) *A User with the security attribute "role" set to "Administrator" is not allowed to create electronic signatures with the SCD.*[14]

[8] [assignment: *access control SFP*]
[9] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[10] [assignment: *access control SFP*]
[11] [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*]
[12] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[13] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[14] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

6.1.2.3 Subset residual information protection (FDP_RIP.1)

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from*[15] the following objects: *SCD, VAD, RAD*[16].

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

The following data persistently stored by the TOE have the user data attribute "integrity checked persistent stored data":

1. SCD
2. RAD
3. SVD (if persistently stored by the TOE).

FDP_SDI.2.1/ Persistent The TSF shall monitor user data stored in containers controlled by the TSF for *integrity error*[17] on all objects, based on the following attributes: *integrity checked persistent stored data*[18].

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*[19].

6.1.3 Identification and authentication (FIA)

6.1.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when *3 (Transport PIN) and 3 up to 15 (PIN and PUK)*[20] unsuccessful authentication attempts occur related to *consecutive failed authentication attempts*[21].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*[22], the TSF shall *block RAD*[23].

6.1.3.2 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: *RAD*[24].

Application note: The RAD of Transport PIN, PIN and PUK (optional), besides being TSF data, are security attributes which allow the individual user to initially set the PIN value (with Transport PIN), use the SCD (with PIN) and unblock the PIN (with PUK).

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

6.1.3.3 Timing of authentication (FIA_UAU.1)

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

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

6.1.3.4 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow *no TSF-mediated action*[26] on behalf of the user to be performed before the user is identified.

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

6.1.4 Security management (FMT)

6.1.4.1 Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to *enable*[27] the functions *signature-creation function*[28] to *Signatory*[29].

6.1.4.2 Management of security attributes (FMT_MSA.1)

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

6.1.4.3 Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for *SCD/SVD parameters*[34].

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

6.1.4.4 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the *Signature-creation SFP*[35] to provide *restrictive*[36] default values for security attributes that are used to enforce the SFP.

Refinement: The security attribute of the SCD "SCD operational" is set to "no" after generation of the SCD.

FMT_MSA.3.2 The TSF shall allow the *Administrator*[37] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.5 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to *modify or unblock*[38] the *RAD*[39] to *Signatory*[40].

6.1.4.6 Specification of Management Functions (FMT_SMF.1)

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

(1) *Modifying the SCD operational attribute*

(2) *Creation of RAD*

(3) *Modifying or unblocking of RAD*[41].

.

6.1.4.7 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles

1. *Administrator*
2. *Signatory*[42].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

[35] [assignment: *access control SFP, information flow control SFP*]
[36] [selection: *choose one of: restrictive, permissive,* [assignment: *other property*]]
[37] [assignment: *the authorised identified roles*]
[38] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[39] [assignment: *list of TSF data*]
[40] [assignment: *the authorised identified roles*]
[41] [assignment: *list of security management functions to be provided by the TSF*]
[42] [assignment: *the authorised identified roles*]

6.1.5 Protection of the TSF (FPT)

6.1.5.1 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit *information about IC power consumption*[43] in excess of *unintelligible limits*[44] enabling access to *RAD*[45] and *SCD*[46].

FPT_EMSEC.1.2 The TSF shall ensure *S.User and S.OFFCARD*[47] are unable to use the following interface *physical contacts of the underlying IC hardware*[48] to gain access to *RAD*[49] and *SCD*[50].

Note:
The additional family FPT_EMSEC TOE Emanation is defined in section 5.1.

6.1.5.2 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*[51]

(4) *Out of range failures of temperature, clock and voltage sensors*[52].

6.1.5.3 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.

6.1.5.4 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist *tampering scenarios by intrusion of physical or mechanical means*[53] to the *underlying IC hardware*[54] by responding automatically such that the SFRs are always enforced.

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

6.1.5.5 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* [55]

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

(2) *Signature-creation according to FCS_COP.1*[56]

(3) *VAD verification*

(4) *RAD modification*

(5) *RAD unblocking*

to demonstrate the correct operation of *the TSF*[57].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[58].

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

[55] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*]
[56] [assignment: *conditions under which self test should occur*]
[57] [selection: [assignment: *parts of TSF, the TSF*]]
[58] [selection: [assignment: *parts of TSF, TSF data*]]

6.2 Security Assurance Requirements

Table 3: Assurance Requirements: EAL4+ (the augmentation is done within the Family AVA_VAN, typographically indicated by the bold face setting).

Assurance Class	Assurance Components
ALC	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1
AGD	AGD_PRE.1, AGD_OPE.1
ADV	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_ IMP.1
ATE	ATE_COV.2, ATE_DPT.2, ATE_FUN.1, ATE_IND.2
AVA	**AVA_VAN.5**

These Security Assurance Requirements are taken from Common Criteria for Information Technology Security Evaluation – Part3: Security assurance requirements [10]. No additional operations are performed on these Assurance Requirements.

6.3 Security Requirements Rationale

6.3.1 Security Requirement Coverage

Table 4: Functional Requirement to TOE Security Objective Mapping

TOE Security Functional Requirement / TOE Security objectives	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.Sigy_SigF	OT.Sig_Secure
FCS_CKM.1				x			x		
FCS_COP.1									x
FDP_ACC.1								x	
FDP_ACF.1								x	
FDP_RIP.1			x					x	
FDP_SDI.2/Persistent			x	x				x	x
FIA_AFL.1								x	
FIA_ATD.1								x	
FIA_UAU.1								x	
FIA_UID.1								x	
FMT_MOF.1			x					x	
FMT_MSA.1			x					x	
FMT_MSA.2								x	
FMT_MSA.3			x					x	
FMT_MTD.1								x	
FMT_SMF.1			x					x	
FMT_SMR.1			x					x	
FPT_EMSEC.1	x								
FPT_FLS.1			x			x			
FPT_PHP.1					x				
FPT_PHP.3						x			
FPT_TST.1		x							x

Table 5: Assurance Requirements to Security Objective Mapping

Objectives	Security Assurance Requirements
OT.Lifecycle_Security	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ALC_DEL.1, AGD_PRE.1
OT.SCD_Secrecy	ADV_ARC.1, AGD_PRE.1, AVA_VAN.5
OT.Sigy_SigF	AVA_VAN.5
OT.Sig_Secure	AVA_VAN.5
Security Objectives	ADV_ARC.1, ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, AGD_OPE.1, AGD_PRE.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2

6.3.2 Security Requirements Sufficiency

6.3.2.1 TOE Security Requirements Sufficiency

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

OT.Lifecycle_Security (Lifecycle security) is provided by the security assurance requirements ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ALC_DEL.1, and AGD_PRE.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The functionality of FPT_TST.1 provides failure detection throughout the lifecycle.

OT.SCD_Secrecy (Secrecy of signature-creation data) counters that, with reference to recital (18) of the Directive [1], storage or copying of SCD causes a threat to the legal validity of electronic signatures. OT.SCD_Secrecy is provided by the assurance requirements ADV_ARC, AGD_PRE, and AGD_OPE which ensure that only authorised users can initialise the TOE and create the SCD. The authentication and access management functionality specified by FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1 and FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.
The security functionality specified by FDP_RIP.1 ensures that residual information on SCD is destroyed after the SCD has been used for signature creation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.
The security functionality specified by FDP_SDI.2/Persistent ensures that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD.
FPT_FLS.1 tests the working conditions of the TOE and guarantees a secure state when integrity is violated and thus assures that the specified security functionality is 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 and AVA_VAN.5 by requesting a methodical vulnerability analysis of the TOE which has to prove that the TOE resists attacks with a high attack potential assure that the security functionality is 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 functionality specified by FDP_SDI.2/Persistent ensures that the keys are not modified, so as to retain the correspondence.

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

OT.Sigy_SigF (Signature generation function for the legitimate signatory only) is provided by FIA_UAU.1 and FIA_UID.1 that ensure that no signature generation function can be invoked before the signatory is identified and authenticated.
The security functionality specified by FDP_ACC.1, FDP_ACF.1, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1 ensures that the signature process is restricted to the signatory.
The security functionality specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, and FMT_MSA.3 ensures that the access to the signature generation functions remain under the sole control of the signatory, as well as FMT_MSA.1 provides that the control of corresponding security attributes is under signatory's control.
FDP_SDI.2/Persistent ensures the integrity of stored data.
The security functionality specified by FDP_RIP.1 and FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.
The assurance requirement specified by AVA_VAN.5 which requests that the evaluator performs i) an independent methodical vulnerability analysis and ii) penetration testing, assuming a high attack potential assures that the security functionality is efficient.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1 which ensures the cryptographic robustness of the signature algorithms and by AVA_VAN.5 by requesting that these resist attacks with a high attack potential. The security functionality specified by FPT_TST.1 ensures that the security functions are performing correctly. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE.

OT.Tamper_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 react on (and therefore resist) physical attacks. In case a tampered HW is detected by the underlying hardware the TOE switches into a secure state by FPT_FLS.1.

6.4 Dependency Rationale

6.4.1 Functional and Assurance Requirements Dependencies

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

Table 6: Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FCS_CKM.1	FCS_COP.1, unsupported dependencies, see sub-section 6.4.2 for justification
FCS_COP.1	FCS_CKM.1, unsupported dependencies, see sub-section 6.4.2 for justification
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
FIA_AFL.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.2	FDP_ACC.1, FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1
FMT_SMR.1	FIA_UID.1
FPT_TST.1	
Assurance Requirements	
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1
ADV_FSP.4	ADV_TDS.1
ADV_TDS.3	ADV_FSP.4
ADV_IMP.1	ADV_TDS.3, ALC_TAT.1
AGD_OPE.1	ADV_FSP.1
AGD_PRE.1	
ALC_CMC.4	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1
ALC_CMS.4	
ALC_DEL.1	
ALC_DVS.1	
ALC_LCD.1	
ALC_TAT.1	ADV_IMP.1

Requirement	Dependencies
ATE_COV.2	ADV_FSP.2, ATE_FUN.1
ATE_DPT.2	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	ATE_COV.1
ATE_IND.2	ADV_FSP.2, AGD_PRE.1, AGD_OPE.1, ATE_COV.1, ATE_FUN.1
AVA_VAN.5	ADV_ARC.1, ADV_FSP.2, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1

6.4.2 Justification of Unsupported Dependencies

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

Requirement	Unsupported dependencies
FCS_CKM.1	It is not possible to delete the SCD (FCS_CKM.4) by means of the TSF. But the TOE blocks the SCD after the defined number of consecutive authentication attempts or if the signature application is terminated. When the SCD is blocked, it is not possible to unblock, use or readout the SCD.
FCS_COP.1	FCS_CKM.4 is not supported by the TOE, see argumentation for FCS_CKM.1.

6.5 Security Requirements Grounding in Objectives

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

Table 7: Assurance Requirement to Security Objective Mapping

Requirement	Security Objectives
Security Assurance Requirements	
ADV_ARC.1	EAL 4
ADV_FSP.4	EAL 4
ADV_TDS.3	EAL 4
ADV_IMP.1	EAL 4
AGD_OPE.1	EAL 4
AGD_PRE.1	EAL 4
ALC_CMC.4	EAL 4
ALC_CMS.4	EAL 4
ALC_DEL.1	EAL 4
ALC_DVS.1	EAL 4, OT.Lifecycle_Security
ALC_LCD.1	EAL 4, OT.Lifecycle_Security
ALC_TAT.1	EAL4, OT.Lifecycle_Security
ATE_COV.2	EAL4
ATE_DPT.2	EAL4
ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_VAN.5	EAL 4, OT.Sigy_SigF, OT.SCD_Secrecy, OT.Sig_Secure

7 TOE Summary Specification

7.1 TOE Security Services

This section provides a description of the TOE's Security Services, which show how the TOE meets each SFR of section 6.1.

7.1.1 SS1 User Identification and Authentication

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

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

The Administrator is at first implicitly authenticated within the lifecycle phase ADMINISTRATION or (if required by the personalization model) later on by a successful authentication with an administrator key. The lifecycle ADMINISTRATION starts after changing the original Start_Key with a confidential command sequence received by the TOE software developer and then switching the TOE's life cycle from the MANUFACTURING to the ADMINISTRATION phase which requires the knowledge of the Start_Key and ends by changing into the lifecycle OPERATIONAL.

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

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

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

The TOE will check that the provided VAD is equal to the stored and individual value of the corresponding RAD (FIA_ATD.1). The number of unsuccessful consecutive authentication attempts by the user is limited to a value depending on the RAD length. Thereafter SS1 will block the RAD (FIA_AFL.1).

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

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

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

The successful authentication with the Transport-PIN which is possible only once, also changes the value of the attribute “SCD operational” from “no” to “yes”, see also SS2 Access Control.
It is important that an attacker can not guess the RAD values by measuring or probing physical observables like TOE power consumption or electromagnetic radiation (FPT_EMSEC.1). Further protection functionality is covered by SS5 Protection.

7.1.2 SS2 Access Control

This Security Service is responsible for the realisation of Signature-creation SFP. The security attributes used for these policies are stated in 6.1.2.2. Generally, this access control policy is assigned to user roles. The identification, authentication and association of users to roles is realised by SS1 User Identification and Authentication (FMT_SMR.1).

SS2 controls the access to the signature creation functionality of the TOE. The TOE allows the generation of a signature if and only if (FDP_ACC.1, FDP_ACF.1.1 and FMT_MOF.1):

- the security attribute “SCD operational” is set to “yes”.
- the signature request is sent by an authorised signatory, see also SS1 User Identification and Authentication.

After the generation of the SCD/SVD key pair, the security attribute “SCD operational” is set to “no” (FMT_MSA.3) by the Administrator. The Administrator is able to set other default values. Thereafter only the Signatory is allowed to modify the security attribute “SCD operational” (FMT_MSA.1 and FMT_SMF.1 (1)). The security attribute “SCD operational” is set to “yes” by the TOE after the Signatory has successfully authenticated himself with the Transport-PIN and unblocked the PIN, see also SS1 User Identification and Authentication.

Only the signatory is allowed to modify or unblock the RAD in form of the PIN (FMT_MTD.1 and FMT_SMF.1(3)), see also SS1 User Identification and Authentication.
The Transport-PIN cannot be modified and can be used only once. If the value of the optional PUK is initialized by the Administrator the Transport-PIN can be unblocked, if it has been blocked by too many unsuccessful authentication attempts. If, however, the Transport-PIN is blocked after its successful use, it cannot be unblocked anymore. If the Transport-PIN is initialized by the signatory it can never be unblocked. The optional PUK can always be modified but unblocked never (if initialized by Administrator) or only once (by Transport-PIN).

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

7.1.3 SS3 SCD/SVD Pair Generation

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

The TOE generates RSA signature key pairs with a module length of 1024 up to 2048 bit in 8 bit steps. The generation is done with secure values for SCD/SVD parameters so that the key pairs fulfil the corresponding requirements of [4] for RSA key pairs (FMT_MSA.2 and FCS_CKM.1).For the generation of primes used for the key pair a GCD (Greatest Common Devisor) test and enough rounds of the Rabin Miller Test are performed. The TOE uses the random number generator of the underlying hardware for the generation of the SCD/SVD key pair. The generation is furthermore protected against electromagnetic emanation, SPA and timing attacks (FPT_EMSEC.1), see also SS5 Protection.

7.1.4 SS4 Signature Creation

This Security Service 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 SS1 User Identification and Authentication.
Before mass signatures, which require the entry of two PINs, are generated by the TOE, both Signatorys have to be authenticated successfully, see SS1 User Identification and Authentication.

Technically, SS4 generates RSA signatures for hash values with PKCS#1 padding (block type 1) using the SCD of the Signatory. The signatures generated by this Security Service meet the following standards:

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

[4] Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV, Veröffentlicht am 27.Januar 2009 im Bundesanzeiger Nr. 13, S. 346, Vom 17. November 2008, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

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

The hash value used for the signature creation is calculated over the DTBS in the TOE IT environment and sent to the TOE under the control of the Signature-creation SFP, see SS2 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 certificate of the SLE66CX680PE (Common Criteria level EAL 5+) covers also the RSA 2048 bit functionality for signature creation (see [21]).

7.1.5 SS5 Protection

This Security Service 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 IC platform that underlies the TSF. The following tests are performed during initial start-up (FPT_TST.1):

- The SLE66CX680PE provides 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 [17] chapter 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 integrity of stored TSF executable code is verified. If this check fails the TOE will preserve a secure state (lifecycle DEATH).
- The integrity of stored data (objects and files) is verified before their use.
- 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 random number generator 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 TOE will furthermore run tests during the generation of the SCD/SVD key pair (SS3 SCD/SVD Pair Generation) (FPT_TST.1.1 (1)) and during signature creation (SS4 Signature Creation) (FPT_TST.1.1 (2)). For tests during signature creation the code of the Infineon RSA2048 Library (Crypto Library for SLE 66CX680PE) is used. The correct operation of SS3 is demonstrated by performing the following checks:

- The TOEs lifecycle phase is checked. Only Administrator can perform SCD/SVD pair generation.
- Before command execution the correct functioning of the Random Number Generator (RNG) and of the Active Shield is tested.
- Before a random number from the RNG is used for the generation of the SCD/SVD key pair the correct functioning of the random number generator will be tested according to functionality class P2 with SOF high of AIS31 as described in the Infineon application note SLE66CxxxP and SLE66CxxxPE, Testing the Random Number Generator [23].
- All command parameters are checked for consistency.
- Access rights are checked.
- The ‘generation allowed bit’ is checked (key pair generation allowed only once).

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

- Failure of RNG double check
- Failure of double check of all sensors
- Failure of Active Shield test
- Failure of the extensive RNG test (AIS31) e.g. during key pair generation
- Failure of cryptographic operation, e.g. during signature creation
- Memory failures during TOE execution

The TOE will also run tests before command execution for VAD verification (FPT_TST.1.1 (3)), RAD modification (FPT_TST.1.1 (4)) and RAD unblocking (FPT_TST.1.1 (5)).

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).

SS5 actively destructs temporarily stored SCD, VAD and RAD immediately after their use - as soon as these data are dispensable (FDP_RIP.1).

The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data":

- SCD
- RAD
- SVD

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

The TOE protects itself against interference and logical tampering by the following measures:

- Each application removes its own data from the used memory area at the latest after execution of a command.
- Clearance of sensitive data, as soon as possible (when they are dispensable)
- Removal of channel data, when the channel is closed
- No parallel but only serial execution of commands
- Encapsulation of context data (security relevant status variables, etc.)
- Use of the chips MMU (Memory Management Unit)
- Separation of User ROM and Test ROM, where the chip's self test software is located, and to which entries are not possible (apart from cold or warm reset)

The TOE protects itself against bypass by not allowing any function in the TSF to proceed if a prior security enforcement function was not executed successfully. The TOE always checks that the appropriate user is successfully authenticated (cf. 7.1.1) for a certain action (cf. 7.1.2)

7.2 Usage of Platform TSF by TOE TSF

The **relevant** SFRs (RP_SFR) of the platform being used by the Composite ST are listed in table 8 below.

RP_SFR	Meaning	Used by TOE SFR
FRU_FLT.2	Limited Fault Tolerance	FPT_TST.1
FPT_FLS.1	Failure with Preservation of Secure State	FPT_FLS.1
FPT_PHP.3	Resistance to Physical Attack	FPT_PHP.3
FDP_ITT.1	Basic Internal Transfer Protection	FPT_EMSEC.1
FDP_IFC.1	Subset Information Flow Control	FPT_EMSEC.1
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	FPT_EMSEC.1
FCS_RND.1	Quality Metric for Random Numbers	FCS_CKM.1 (Signature Key Pair generation) FPT_EMSEC.1 (blinding)
FPT_TST.2	Subset TOE Security Testing	FPT_TST.1 FPT_PHP.3 (active shield and sensors)
FCS_COP.1 (3DES)	Cryptographic Support (3DES)	FMT_SMR.1 (authentication of Administrator)
FCS_COP.1 (RSA)	Cryptographic Support (RSA)	FCS_COP.1
FCS_CKM.1	Cryptographic Key Generation	FCS_CKM.1
FDP_SDI.2	Stored Data Integrity Monitoring and Action	FDP_SDI.2/Persistent

Table 8: Relevant Platform SFRs used by Composite ST

The **irrelevant** SFRs (IP_SFR) of the platform not being used by the Composite ST are listed in table 9

IP_SFR	Meaning	Comment
FPT_SEP.1	TSF Domain Separation	only transparent mode used
FDP_SDI.1	Stored Data Integrity Monitoring	Not used by TOE TSF
FMT_LIM.1	Limited Capabilities	Implicitly prevents manipulations in test mode
FMT_LIM.2	Limited Availability	
FAU_SAS.1	Audit Storage	Reading of chip data not used by TOE TSF
FDP_ACC.1	Subset Access Control	Only default setting **transparent mode** is used
FDP_ACF.1	Security Attribute Based Access Control	
MT_MSA.3	Static Attribute Initialisation	
FMT_MSA.1	Management of Security Attributes	
FMT_SMF.1	Specification of Management Functions	

Table 9: Irrelevant Platform SFRs not being used by Composite ST

There is no conflict between the security problem definition, the security objectives and the security requirements of the current Composite Security Target and the Platform Security Target (security target of the controller SLE66CXxxxPE). All related details (operations on SFRs, definition of security objectives, threats etc.) can be found in both the documents.
The Security Objectives for the Platform support the Security Objectives for the TOE.

The Platform Security Requirements for the development of the Smartcard Embedded Software

- **RE.Phase-1** (Design and Implementation of the Smartcard Embedded Software) and
- **RE.Cipher** (Cipher Schemas)

are met.

7.3 Assumptions of Platform for its Operational Environment

Assumptions of the hardware platform related to its operational environment as stated in [23] , chap. 3.2	**Short Description**	**Categorisation**	**Comment**
inherited from the BSI-PP-0002**:**			
A.Plat-Appl	The Smartcard Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents as the hardware data sheet [3], and the hardware application notes, and (ii) findings of the TOE evaluation report [18] relevant for the Smartcard Embedded Software.	automatically fulfilled (CfPA)	Will be automatically fulfilled by the technical design and the implementation
A.Resp-Appl	All security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as defined for the specific application context.	automatically fulfilled (CfPA)	Can be mapped at least to the following security objectives for the Composite-TOE: OT.EMSEC_Design OT.SCD_Secrecy OT.Sigy_SigF OT.Tamper_Resistance
A.Process-Card	Security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).	automatically fulfilled (CfPA)	Will automatically be fulfilled by application of the security assurance requirements of the families ALC_DVS and ALC_DEL
dedicated defined in [25]:			
A.Key-Function	Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced).	automatically fulfilled (CfPA)	Can be mapped at least to the following security objectives for the Composite-TOE: OT.EMSEC_Design OT.SCD_Secrecy

Table 10: Categorisation of the assumptions of Platform for its Operational Environment

8 References

8.1 Bibliography

[1] Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures

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

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

[4] Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV, Veröffentlicht am 27.Januar 2009 im Bundesanzeiger Nr. 13, S. 346, Vom 17. November 2008, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

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

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

[7] FIPS PUB 180-1: Secure Hash Standard, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 17.04.1995

[8] Common Criteria for Information Technology Security Evaluation – Part1: Introduction and general model, Version 3.1, Revision 1, September 2006, CCMB-2006-09-001

[9] Common Criteria for Information Technology Security Evaluation – Part2: Security functional requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-002

[10] Common Criteria for Information Technology Security Evaluation – Part3: Security assurance requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-003

[11] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007, CCMB-2007-09-004

[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 7816-9:1998 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, CWA 14169:2002 (E), 25.07.2001

[17] Data Book SLE66CxxxPE / MicroSlim Security Contoller Family, incl. the errata sheet, Version 07.05, 01.07.2005, Infineon

[18] Administrator Guidance CardOS V4.4 with Application for QES, Siemens AG

[19] User Guidance CardOS V4.4 with Application for QES, Siemens AG

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

[21] Certification Report BSI-DSZ-CC-0437-2008 for SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA 2048 V1.5, and all with specific IC dedicated software from Infineon Technologies AG, 27.Mai 2008, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[22] Smartcard IC Platform Protection Profile (SSVG-PP), Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

[23] Security and Chip Card ICs, SLE66CxxxP and SLE66CxxxPE, Testing the Random Number Generator, Confidential Application Note, 11.2004, Infineon

[24] Anwendungshinweise und Interpretationen zum Schema, AIS36: ETR-lite für zusammengesetzte EVGs, Version 1, 29.07.2002, Bundesamt für Sicherheit in der Informationstechnik

[25] Security Target BSI-DSZ-CC-0437, SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, All Products with RSA 2048 library, Version 1.3, 2007-03-22, Infineon AG

8.2 Acronyms

CC	Common Criteria
CGA	Certification Generation Application
DTBS	Data to be signed
EAL	Evaluation Assurance Level
IT	Information Technology
PIN	Personal Identification Number
PP	Protection Profile
PUK	Personal Unblocking Key
QES	Qualified Electronic Signature
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
SS	Security Service
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

8.3 Glossary

Operation	Meaning
digital signature-generation	Process of signing a hash value sent by SCA and returning the signature as response to SCA
signing of DTBS-representation by Signatory	Only the user authenticated as Signatory may invoke the signing process. The DTBS-representation is a hash value of the data to be signed
prohibit the use of the altered data	All commands using SCD, RAD or SVD check the integrity of the corresponding entities and abort execution if the data have been altered.
inform the Signatory about integrity error	Abortion of command execution because of an integrity error results in an appropriate return code sent to the SCA/CGA.
block RAD	RAD (Transport PIN, PIN, PUK) is made unusable (except for unblocking, if allowed).
Modifying the SCD operational attribute	After generation of SCD/SVD key pair the SCD will not be operational until the signatory has used the Transport PIN to unblock, i.e. reset the retry counter of the initially blocked signature PIN.
Creation of RAD	The entities containing RAD are created in the EEPROM by the administrator. The Transport PIN value is set by the administrator. The values of the signature PIN and optional PUK are set by the signatory.
Modifying or unblocking of RAD	The internally stored values of the signature PIN and optional PUK can always be changed with the appropriate command by the signatory after successful corresponding authentication. If a PUK is present, a blocked signature PIN (with Retry Counter == zero) can be changed and thus unblocked (Retry Counter => max) after successful authentication with PUK.
VAD verification	Comparison of the presented VAD value with the corresponding internally stored RAD value
RAD modification	Overwriting of the internally stored RAD value in EEPROM with new data
RAD unblocking	Setting a PIN’s Retry Counter of zero back to its maximum