Atos

CardOS â DI V4.2C CNS

Security Target
CardOS DI V4.2C CNS with Application for QES

Edition 07/2011

Atos IT Solutions and Services GmbH
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 is reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome.

Subject to change without notice

Contents

Document History

Version	Release Date	Changed Chapter(s)	Remarks	Author	Sent to Receiver on Date
0.10	25.09.09		First version based on evaluated ST "CardOS V4.4 CNS with Application for QES"	Ulrike Ludwig, Andreas Furch, Siemens	Dr. Igor Furgel, Evaluator, T-Systems 25.09.2009
0.20	04.11.09	1.4, 1.5 (deleted), 6.1.1.3, 6.1.2.2, 6.1.5.2, 7.1.4, 8.3	Editorial changes, addition of application note to FPT_EMSEC	Andreas Furch, Siemens	Dr. Igor Furgel, Dr. Alla Gnedina, Evaluator, T-Systems, 04.11.2009
0.30	06.11.09	7.2	Moved FCS_COP.1 (RSA) and FCS_CKM.1 (RSA) from Table 10 to Table 11	Andreas Furch, Siemens	Dr. Igor Furgel, Dr. Alla Gnedina, Evaluator, T-Systems, 06.11.2009
0.40	20.11.09	1.2, 1.4	Removed production site Altis	Andreas Furch, Siemens	Dr. Igor Furgel, Dr. Alla Gnedina, Evaluator, T-Systems, 20.11.2009
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	Dr. Igor Furgel, Dr. Alla Gnedina, Evaluator, T-Systems, 29.04.2010
0.60	22.06.11	1.1, 1.2, 8.1	Maintenance	Andreas Furch, Siemens	Hr. Jan Tietjen, Evaluator, T-Systems, 24.06.2011
0.70	13.07.11	Whole document	Re-branding	Kay Prisille, Atos	Bundesamt für Sicherheit in der Informationstechnik on 2011-07-13

1 ST Introduction

1.1 ST Reference

Title:	Security Target CardOS DI V4.2C CNS with Application for QES
Authors:	Atos IT Solutions and Services GmbH
CC Version:	3.1, Revision 2
General Status:	Draft
Version Number:	0.70, (13.07.11)

The TOE is based on the Infineon Dual Interface chip SLE66CLX800PE 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,
- the references and a glossary in section 8.

1.2 TOE Reference

The TOE “CardOS DI V4.2C CNS with Application for QES Version 1.01” is based on the Infineon chip SLE66CLX800PE (m1581-a14) as ICC platform, which is loaded by the chip manufacturer with the operating system CardOS DI V4.2C. 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 DI V4.2C has the version identifier ‘C80C’.
The TOE may additionally be identified by its factory key values, the historical bytes in the default ATR or the application data field of the ATQB and the responses to the version dependent GET DATA modes.

The Application for QES can be personalized in three different ways, which are named
‘Pre-loaded variant 1’, ‘Pre-loaded variant 2’ and ‘Post-loaded variant’.
These 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 Type 3). The smart card is based on an Infineon Dual Interface Chip.

Usage and major security features of the TOE

The TOE allows to generate cryptographically strong Signatures over previously and externally calculated hash-values. The TOE generates the signature key pair (SCD/SVD) and ensures that the Signature Verification Data (SVD, i.e. public key) is protected from modification and insertion errors during export. 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 TOE is realized as a smart card conforming 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 (SLE66CLX800PE from Infineon) used to implement the secure signature-creation device (SSCD) and iii) the pertaining guidance documentation ’Administrator Guidance CardOS DI V4.2C CNS’ [24], and ‘User Guidance CardOS DI V4.2C CNS’ [33]. Therefore the TOE is considered to be a product.

The TOE developer delivers the ROM mask, script-files and pertaining documentation. The CA (certification authority) 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 SLE66CLX800PE, the IC Dedicated Software and the optional RSA2048 crypto library V1.5, which is not used by the TOE.

The chip is certified for the production site Dresden in Germany (production line indicator ‘2’) (cf [20], Certification report BSI-DSZ-CC-0482-2008 for SLE66CLX800PE / m1581-e13a/a14, SLE66CLX800PEM / m1580-e13a/a14, SLE66CLX800PES / m1582, SLE66CLX800PE / m1599-e13a/a14-e13a/a14, SLE66CLX360PE / m1587-e13a/a14, SLE66CLX360PEM / m1588-e13a/a14, SLE66CLX360PES / m1589-e13a/a14, SLE66CLX180PE / m2080-a14, SLE66CLX180PEM / m2081-a14, SLE66CLX120PE / m2082-a14, SLE66CLX180PEM / m2083-a14,,all optional with RSA 2048 V1.5 and ECC V1.1 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 DI V4.2C	C80C	07.09.09	loaded in ROM / EEPROM
2	V4.2C DI Software Application Digital Signature (Application /	***<u>Pre-loaded variant 1</u>:*** V42C_DI_InitScript_1.csf V42C_DI_InitScript_1_DF_DS_x.csf V42C_DI_CAScript_1.csf V42C_DI_CAScript_1_DF_DS_x.csf V42C_DI_PersScript_1.csf	The final versions of these files will be defined		Personalization Script Files in **CSF format**,

No.	Type	Term	Version	Date	Form of delivery
	Data Structure)	V42C_DI_PersScript_1_DF_DS_x.csf V42C_DI_RAScript_1.csf V42C_DI_RAScript_1_DF_DS_x.csf ***Pre-loaded variant 2:*** V42C_DI_InitScript_2.csf V42C_DI_InitScript_2_DF_DS_x.csf V42C_DI_CAScript_2.csf V42C_DI_CAScript_2_DF_DS_x.csf V42C_DI_CaScript_2_DF_DS_x_cert.csf V42C_DI_PersScript_2.csf V42C_DI_PersScript_2_DF_DS_x.csf V42C_DI_RAScript_2.csf V42C_DI_RAScript_2_DF_DS_x.csf ***Post-loaded variant:*** V42C_DI_InitScript_Post.csf V42C_DI_LRAScript_Post.csf V42C_DI_LRAScript_Post_DF_DS_x.csf ***All variants:*** V42C_DI_Default.csf	at the end of the evaluation and will be listed in the certification report		after whose execution the ADS will be loaded 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 Init_Scripts)
4	Software Command_Set_ Extension Package (mandatory)	CommandSet_Ext_Package			
5	Software CNS Package (mandatory)	CNS Package			
6	Software SISS Package (optional)	SISS Package			
7	Software SSCR Package Technical	SSCR_Tech_Package			Personalization Script Files in CSF format (code only temporarily in EEPROM)
8	Software SSCR Package Organizational	SSCR_Org_Package			
9	Documentation	CardOS License Package Tool Manual	1.3	09/2005	Paper form or PDF-File
10	Documentation	CardOS V4.2B User's Manual	1.0	09/2005	
11	Documentation	CardOS DI V4.2C Packages & Release Notes	The final versions of these documents will be defined at the end of the evaluation and listed in the certification report		
12	Documentation	CardOS DI V4.2C SISS, SSCR Packages & Release Notes			
13	Admin Documentation	CardOS DI V4.2C CNS Administrator Guidance			
14	User Documentation	CardOS DI V4.2C CNS User Guidance			

No.	Type	Term	Version	Date	Form of delivery
15	ADS Documentation	CardOS DI V4.2C CNS ADS_Description			
16	Hardware (Chip)	Infineon SLE66CLX800PE	m1581-a14 (Dresden)		Module
	Firmware RMS	RMS	RMS_E V06		Stored in reserved area of User ROM
	Software crypto library	RSA2048 crypto library	Version 1.4*		Loaded in ROM
17	Firmware STS	Self Test Software	V57.08.07		Stored in Test ROM

*Comment: The OS CardOS DI V4.2C integrates Version 1.4 of the RSA2048 crypto library provided by Infineon, whose functionality is not used by the TOE.

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 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’ [4] 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 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’ [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 verification authentication data (VAD).

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

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.

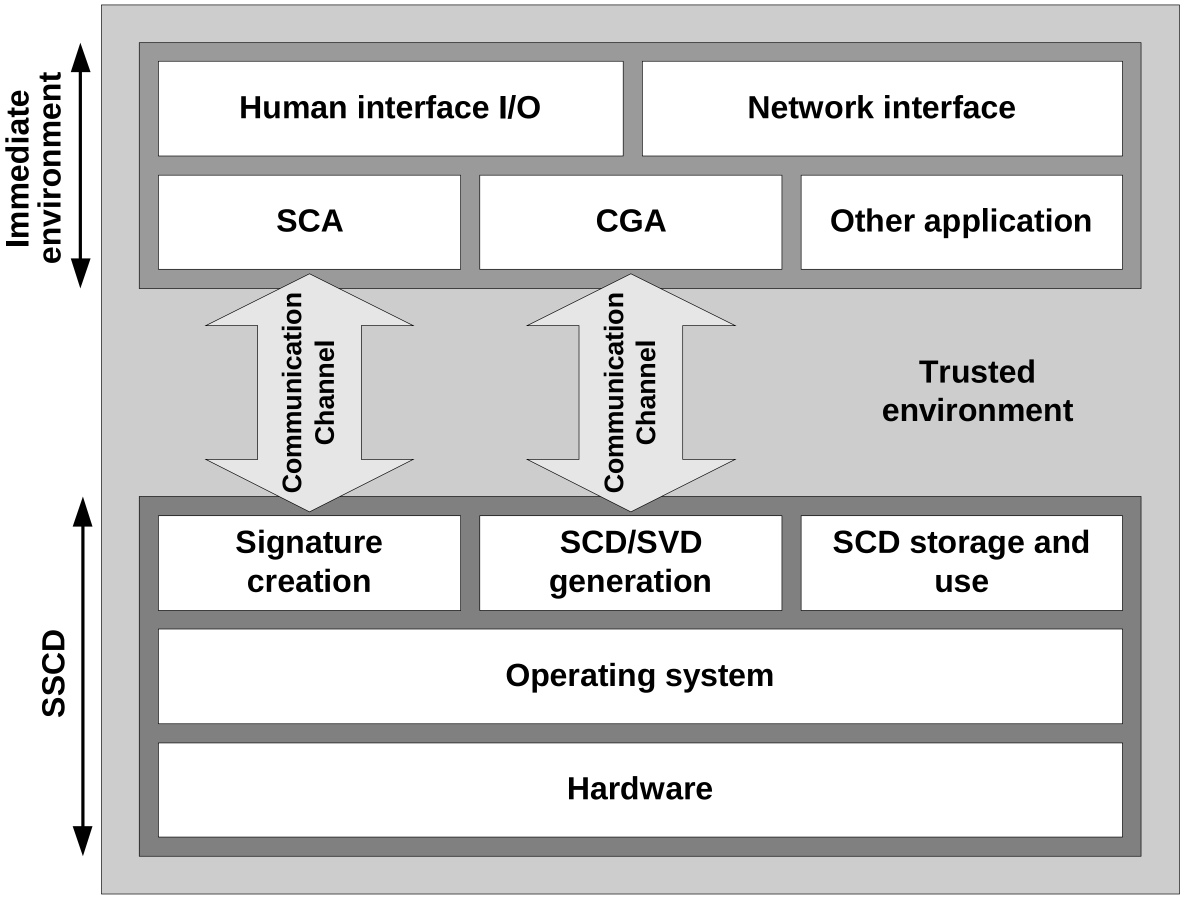

Figure 1: Scope of the SSCD, structural view

There are two physical interfaces of the TOE, a contact interface, which is provided by a connection according to ISO 7816 part 3 [12] and an RF interface (radio frequency power and signal interface) which provides a contactless interface according to ISO/IEC 14443 part 3 [16] and 4 [17]. Only Type B of the contactless protocol is supported. The two interfaces (either one or the other at a time) are 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 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.

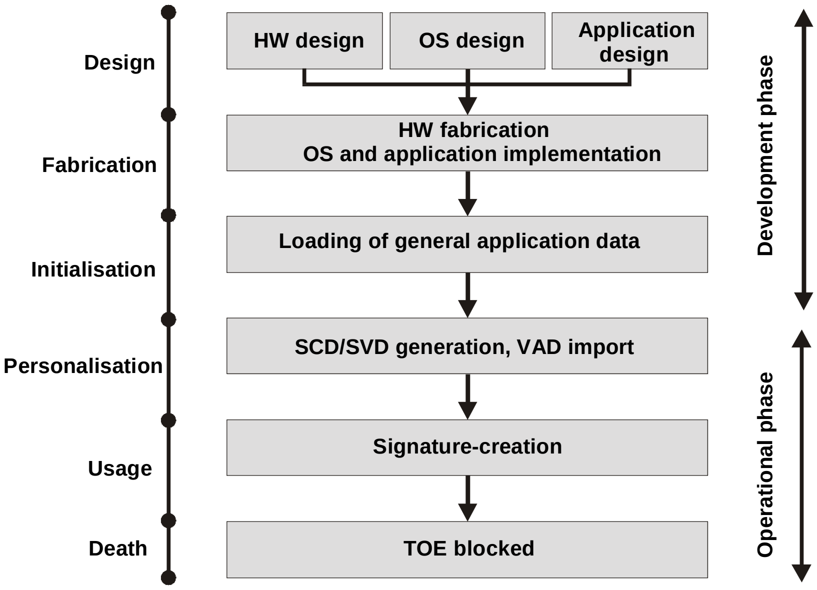

Figure 2: SSCD life cycle

2 Conformance claims

The TOE is a composite product, as it is based on the Infineon Security Controller SLE66CLX800PE, 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. [20]).

As required by AIS36 [31] compatibility between this Composite Security Target and the Platform Security Target [25] of the Infineon chip SLE66CLX800PE 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 10) being used by the composite ST and ii) irrelevant Platform TSF (Table 11) 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

This Security Target claims strict conformance to the following protection profile:

- Protection Profile – Secure Signature-Creation Device (SSCD-PP) Type 3, Version 1.05, CWA 14169:2002 (E), 25.07.2001, [18]

The short term for this protection profile used in this document is SSCD-PP-T3.
The SSCD-PP-T3 has been evaluated and certified as being conformant to the Common Criteria version 2.1 [28], CC Part 2 [29] extended, and CC Part 3 [30] conformant.

The assurance level for the SSCD-PP-T3 and therefore for the TOE is EAL4 augmented.
Augmentation results from the selection of:

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

As the CC versions of this security target and of the SSCD-PP-T3, which it claims strict conformance to, differ in the major versions, 3.1 and 2.1 respectively, the contents of the SSCD-PP-T3 is completely included in this security target. Where changes are necessary they will be commented. For details cf. section 6.1 Security Functional Requirements and section 6.2 Security Assurance Requirements.

The evaluation is a composite evaluation and uses the results of the chip's CC evaluation provided by [20]. 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 SLE66CLX800PE 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, [19]

Refinements concerning SSCD-PP-T3 were made for the following Security Functional Requirements:

- FDP_ACF.1 / Signature Creation SFP (cf. section 6.1.2.2):

  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 [18] is specified more precisely by stating the concrete list of standards:

FCS_CKM.1.1	(cf. section 6.1.1.1)
FCS_COP.1.1 / Corresp	(cf. section 6.1.1.3)
FCS_COP.1.1 / Signing	(cf. section 6.1.1.3)

Due to CC-3.1-P2 [9] the Functional Security Requirement FMT_SMF.1 (cf. 6.1.4.6) has been added as a direct dependency from FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1.

2.3 Conformance Rationale

2.3.1 PP Claims Rationale

According to section 2.2 this Security Target claims strict conformance to the Protection Profile – Secure Signature-Creation Device (SSCD-PP) Type 3, [18].

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 3, 4, and 6). 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 SSCD-PP-T3 are also clearly indicated.

The assurance level claimed for this target (EAL4+, shown in section 2 and 6.2) meets the requirements claimed by the SSCD-PP-T3 (EAL4+).

These considerations show that the Security Target correctly claims conformance to the SSCD-PP-T3.

2.3.2 Rationale for Assurance Level 4 Augmented

The assurance level for this security target is EAL4 augmented. It is exactly the same package claim that holds for the protection profile SSCD-PP-T3. 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 (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).
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 SSCD-PP-T3 [18]	Synonyms used in this evaluation
S.User	User
S.Admin	Administrator
S.Signatory	Signatory
S.OFFCARD	Attacker

[1] The TOE does not support biometric authentication. Therefore the authors changed this asset definition by deleting the term “biometric data”, see also section 3 [18].

[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 [18].

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 [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.

*Comment: This OSP is not part of the SSCD-PP-T3 but has been added by the ST.

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 [18] 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 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 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.

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.

*Comment: This OE is not part of the SSCD-PP-T3 but has been added by the ST.

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.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID x	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	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		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						
P.Env_KeyGen			x														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 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.

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 and supported by the TOE through OT.Init.

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 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.

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.

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.

5 Extended Components Definition

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined in the Protection Profile – Secure Signature-Creation Device (SSCD-PP) Type 3 [18], section 6.6.

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

5.1 Rationale for Extensions

The additional family FPT_EMSEC TOE Emanation was defined in the SSCD-PP-T3 [18]. The developer decided to inherit FPT_EMSEC TOE Emanation from [18]. 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.

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].
Differences between the text of CC-3.1-P 2 [9] and the text of the SSCD-PP-T3 are marked by an asterisk (*) after the new text. All differences are commented directly underneath the respective SFR.
Where operations for assignment, selection and refinement have been made, all these operations are typographically accentuated by underlining these passages (e.g. RSA).
Where any of these operations have changed due to CC3.1-P2 this is commented directly underneath the respective SFR.
Operations that were already carried out within the SSCD-PP-T3 [18] 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*).
Operations whose meaning may not be implicitly clear are described in more detail in the glossary (see chap. 8.3)

The 'Security Requirements for the IT Environment' defined by the SSCD-PP-T3 in section 5.3, are not in the scope of CC-3.1-P 2 [9]. The same holds for the 'Security Requirements for the Non-IT Environment' defined by the SSCD-PP-T3 in section 5.4.

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].
As these SARs differ considerately from the SARs stated in the SSCD-PP-T3, it is shown in Table 5 of section 6.2 how the SARs from the SSCD-PP-T3 are covered by the SARs from CC-3.1-P3 [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*[3] and specified cryptographic key size *1024 bit*[4] that meet the following:

1) *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 [4]*[5].

Refinement:
The already within [18] 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]

6.1.1.2 Cryptographic key destruction (FCS_CKM.4)

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

* Comment (editorial): ‘in case of regeneration of a new SCD’ from the SSCD-PP-T3 has been deleted.

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.

6.1.1.3 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 size *1024 bit*[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 size *1024 bit*[10] that meet the following:

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

(2) *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 [4]*[11]

Refinement:
The already within [18] executed operation ‘List of approved algorithms and parameters’ is replaced with the concrete statement of references.

6.1.2 User data protection (FDP)

6.1.2.1 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].

[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]

FDP_ACC.1.1/ SVD Transfer SFP — The TSF shall enforce the SVD Transfer SFP[12] on export of SVD by User[13].

6.1.2.2 Security attribute based access control (FDP_ACF.1)

The following table lists the subjects and objects controlled by the SFPs of section 6.1.2.1 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 3: 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 the following*: 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*

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].

* Comment: ACF.1.1 (editorial) ‘the following’ has been included in CC-3.1-P2.
ACF.1.4 (editorial) ‘rule’ from the SSCD-PP-T3 has been deleted.

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).

Personalisation SFP

FDP_ACF.1.1/ — The TSF shall enforce the Personalisation SFP[14] to objects based on the

[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 following*: 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* none[18].

* Comment:: ACF.1.1 (editorial) ‘the following’ has been included in CC-3.1-P2.
ACF.1.4 (editorial) ‘rule’ from the SSCD-PP-T3 has been deleted.

Signature-creation SFP

FDP_ACF.1.1/Signature-creation SFP The TSF shall enforce the Signature-creation SFP[14] to objects based on the following*: 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*

(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].

* Comment:: ACF.1.1 (editorial) ‘the following’ has been included in CC-3.1-P2.
ACF.1.4 (editorial) ‘rule’ from the SSCD-PP-T3 has been deleted.

Application note:
The corresponding TSFR of the SSCD-PP-T3 [18], 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		Signatory	
	SCD operational		**SCD operational**	
	“no”	**“yes”**	**“no”**	**“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 4: 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 the following*: 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*: none[18].

* Comment:: ACF.1.1 (editorial) ‘the following’ has been included in CC-3.1-P2.
ACF.1.4 (editorial) ‘rule’ from the SSCD-PP-T3 has been deleted.

6.1.2.3 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 TOE*.

FDP_ETC.1.2/ SVD Transfer — The TSF shall export the user data without the user data’s associated security attributes.

6.1.2.4 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 TOE*.

FDP_ITC.1.2/DTBS — The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE*.

FDP_ITC.1.3/DTBS — The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE*: DTBS-representation shall be sent by an authorised SCA[26].

* Comment (5.1.2.3 and 5.1.2.4) (editorial): ‘TOE’ replaces the former ‘TSC’ from the SSCD-PP-T3.

[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]

[26] [assignment: additional importation control rules]

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.

6.1.2.5 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].

6.1.2.6 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 in containers controlled by the TSF* 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].

* Comment (editorial): ‘in containers controlled by the TSF’ replaces the former ‘within the TSC’.

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 in containers controlled by the TSF* 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].

* Comment (Editorial): ‘in containers controlled by the TSF’ replaces the former ‘within the TSC’.

6.1.2.7 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.

[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.

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 (PIN and PIN_T), resp. 10*[36] *(PUK)* unsuccessful authentication attempts occur related to consecutive failed authentication attempts[37].

Comment**:** The SSCD-PP-T3 offered only the [assignment: number] for unsuccessful authentication attempts. CC-3.1-P2 now offers the selection shown under footnote 36.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been *met*[38], the TSF shall block RAD[39].

Comment**:** Where the text of the SSCD-PP-T3 said ‘met or surpassed’, CC-3.1-P2 now requires the selection of one of the two verbs (shown under footnote 38).

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[40].

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).

6.1.3.3 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.[41]

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

[35] [selection: modification, deletion, insertion, replay]

[36] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

[37] [assignment: list of authentication events]

[38] [selection: met, surpassed]

[39] [assignment: list of actions]

[40] [assignment: list of security attributes]

[41] [assignment: list of TSF mediated actions]

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.

6.1.3.4 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.[42]

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[43] the functions* signature-creation function[44] to Signatory[45].

* Comment: (editorial) ‘functions’ has been newly inserted in CC-3.1-P2

6.1.4.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/ Administrator The TSF shall enforce the Initialisation SFP[46] to restrict the ability to modify[47] the security attributes SCD / SVD management[48] to Administrator[49].

FMT_MSA.1.1/ Signatory The TSF shall enforce the Signature-creation SFP[46] to restrict the ability to modify[47] the security attributes SCD operational[48] to Signatory[49].

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.

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_*[50].

* Comment**:** Where the text of the SSCD-PP-T3 said only ‘security attributes’, CC-3.1-P2 now requires an assignment of security attributes.

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

6.1.4.4 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the Initialisation SFP and Signature-creation SFP[51] to provide restrictive[52] 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.

FMT_MSA.3.2 The TSF shall allow the Administrator[53] 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.

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*[54] the RAD[55] to Signatory[56].

6.1.4.6 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*[57].

Application note:
This TSFR is not taken from [18] but has been introduced due to CC-3.1-P2.

6.1.4.7 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles

1. Administrator and
2. Signatory[58].

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

[51] [assignment: access control SFP(s), information flow control SFP(s)]
[52] [selection: choose one of: restrictive, permissive, [assignment: other property]]
[53] [assignment: the authorised identified roles]
[54] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[55] [assignment: list of TSF data]
[56] [assignment: the authorised identified roles]
[57] [assignment: list of management functions to be provided by the TSF]
[58] [assignment: the authorised identified roles]

6.1.5 Protection of the TSF (FPT)

6.1.5.1 Testing of external entities (FPT_TEE.1)

FPT_TEE.1.1 The TSF shall run a suite of tests *during initial start-up*[59] to check the fulfillment of the *none*[60].

FPT_TEE.1.2 If the test fails the TSF shall *preserve a secure state*[61]

Note:
This element replaces the SFR FPT_AMT.1 from the SSCD-PP-T3.
Application Note:
The assignment “none” within FPT_TEE1.1 comes from the fact that the TOE is the whole smartcard and that no external entities are to be tested. The Security Requirement has nevertheless been taken from the SSCD-PP-T3 in its replaced form (see note above) and using this assignment to reflect the strict conformance to the SSCD-PP-T3. The same equivalently holds for FPR_TEE.1.2.

6.1.5.2 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit *information about IC power consumption*[62] in excess of *unintelligible limits*[63] enabling access to RAD[64] and SCD[65].

FPT_EMSEC.1.2 The TSF shall ensure *S.User and S.OFFCARD*[66] are unable to use the following interface *physical contacts of the underlying IC hardware*[67] to gain access to RAD[68] and SCD[69].

Application Note:
For the platform in question (SLE66CLX800PE) the assignment “physical contacts of the underlying IC hardware” within FPT_EMSEC.1.2 means the contact-based as well as the contactless interface.

Note:
The additional family FPT_EMSEC TOE Emanation is defined in section 6.6.1 of the SSCD-PP-T3.

6.1.5.3 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*

(4) *Out of range failures of temperature, clock and voltage sensors*[70].

[59] [selection: during initial start-up, periodically during normal operation, at the request of an authorised user, assignment [other conditions]]
[60] [assignment: list of properties of the external entities]
[61] [assignment: action(s)]
[62] [assignment: types of emissions]
[63] [assignment: specified limits]
[64] [assignment: list of types of TSF data]
[65] [assignment: list of types of user data]
[66] [assignment: type of users]
[67] [assignment: type of connection]
[68] [assignment: list of types of TSF data]
[69] [assignment: list of types of user data]

6.1.5.4 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.

6.1.5.5 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist *tampering scenarios by intrusion of physical or mechanical means*[71] to the *underlying IC hardware*[72] by responding automatically such that the SFRs are always enforced*.

* Comment (editorial): 'SFRs are always enforced' replaces the former 'TSP is not violated'.

6.1.5.6 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* [73]

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

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

(3) *VAD verification*

(4) *RAD modification*

(5) *RAD unblocking*[74]

to demonstrate the correct operation of *the TSF*[75].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[76].

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

Comment**:** The SSCD-PP-T3 said only 'TSF' (TST.1.1) and 'TSF data' (TST.1.2) while CC-3.1-P2 now offers the selections shown under footnotes 75 and 76.

6.1.6 Trusted path/channels (FTP)

6.1.6.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/
SVD Transfer The TSF shall provide a communication channel between itself and another* 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/ The TSF shall permit *another trusted IT product*[77] to initiate

[70] [assignment: list of types of failures in the TSF]
[71] [assignment: physical tampering scenarios]
[72] [assignment: list of TSF devices/elements]
[73] [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions]
[74] [assignment: conditions under which self test should occur]
[75] [selection: [assignment: parts of TSF, the TSF]]
[76] [selection: [assignment: parts of TSF, TSF data]]

SVD Transfer — 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[78].

***** Comment (editorial, FTP_ITC.1.1 and 1.2): ‘another’ replaces the former text ‘a/the remote’.

FTP_ITC.1.1/DTBS import — The TSF shall provide a communication channel between itself and another* 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**[77] 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[78].

***** Comment (editorial): ‘another’ replaces the former text ‘a remote’.

6.1.6.2 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[79] 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*[80].

FTP_TRP.1.2/TOE — The TSF shall permit *local users*[81] 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,*

(2) *modification of the RAD and*

(3) *unblocking the RAD*[82].

.

Comment: CC-3.1-P2 now offers the selections shown under the footnotes 80 and 81.

[77] [selection: the TSF, another trusted IT product]
[78] [assignment: list of functions for which a trusted channel is required]
[79] [selection: remote, local]
[80] [selection: modification, disclosure [assignment: other types of integrity or confidentiality violation]]
[81] [selection: the TSF, local users, remote users]
[82] [selection: initial user authentication, [assignment: other services for which trusted path is required]]

6.2 Security Assurance Requirements

In this chapter a mapping of the **EAL4** Security Assurance Requirements from the SSCD-PP-T3 [18] (Table 5.1 in section 5.2) and those of **CC-3.1-P3** [10] is provided.

Table 5 shows how the **Security Assurance Requirements from** the **SSCD-PP-T3 are covered by those of CC-3.1-P3** [10], (the augmentation is now done within the Family **AVA_VAN**, typographically indicated by the **bold face setting**).

The **CC-3.1-P3** lists the EAL4 Security Assurance Requirements within section 8.6 of [10].

SSCD-PP-T3		**Comments regarding coverage of the SSCD-PP-T3 components**	**CC-3.1-P3**	
Assurance			**Assurance**	
Class	**Component**		**Component**	**Class**
ACM	ACM_AUT.1	contents have been combined and are covered by	ALC_CMC.4	ALC
	ACM_CAP.4			
	ACM_SCP.2	content completely covered by	ALC_CMS.4	
ADO	ADO_DEL.2	content now covered by two components	ALC_DEL.1	ALC
			AGD_PRE.1	AGD
	ADO_IGS.1	content now covered by two components	ADV_ARC.1.	ADV
			AGD_PRE.1	AGD
ADV	ADV_FSP.2	content completely covered by	ADV_FSP.4	ADV
	ADV_HLD.2	contents have been combined and are covered by	ADV_TDS.3	
	ADV_LLD.1			
	ADV_RCR.1			
	ADV_IMP.1	completely covered by	ADV_ IMP.1	
	ADV_SPM.1	for EAL4 not required anymore	-	
AGD	AGD_ADM.1	contents have been combined and are covered by	AGD_OPE.1	AGD
	AGD_USR.1			
ALC	ALC_DVS.1	content completely covered by	ALC_DVS.1	ALC
	ALC_LCD.1		ALC_LCD.1	
	ALC_TAT.1		ALC_TAT.1	
ATE	ATE_COV.2	content completely covered by	ATE_COV.2	ATE
	ATE_DPT.1		ATE_DPT.2	
	ATE_FUN.1		ATE_FUN.1	
	ATE_IND.2		ATE_IND.2	
AVA	**AVA_MSU.3**	contents have been combined and are covered by	**AVA_VAN.5**	**AVA**
	AVA_SOF.1			
	AVA_VLA.4			

Table 5: SARs from SSCD-PP-T3 versus SARs from CC-3.1-P3

6.3 Security Requirements Rationale

6.3.1 Security Requirement Coverage

Table 6: 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						
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[83]			x	x							x	
FMT_SMR.1				x							x	
FPT_TEE.1		x		x								x
FPT_EMSEC.1	x											

[83] See the note in section 6.1.4.6.

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
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	

Table 7: 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.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, ALC_DEL.1, and AGD_PRE.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functionality of FPT_TST.1

and FPT_TEE.1 provides 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 [1], storage or copying of SCD causes a threat to the legal validity of electronic signatures. OT.SCD_Secrecy is provided by the security functionality 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 functionality 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 ensures 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 and FCS_CKM.4 ensures 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 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_TEE.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 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, 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 functionality 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 functionality 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 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/SIGNATORY provides that the control of corresponding security attributes is under signatory's control.
The security functionality specified by FDP_SDI.2 and FTP_TRP.1/TOE ensures the integrity of stored data both during communication and while stored.

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/SIGNING 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_TEE.1 and FPT_TST.1 ensures that the TOE's 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.

6.4 Dependency Rationale

6.4.1 Functional and Assurance Requirements Dependencies

The functional and assurance requirements dependencies for the TOE are completely fulfilled.

Table 8: Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FCS_CKM.1	FCS_COP.1/SIGNING, FCS_COP.1/CORRESP, FCS_CKM.4
FCS_CKM.4	FCS_CKM.1
FCS_COP.1 / CORRESP	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4
FCS_COP.1 / SIGNING	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4
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[84]
FMT_MSA.1 / Administrator	FDP_ACC.1/Initialisation SFP, FMT_SMR.1, FMT_SMF.1[84]
FMT_MSA.1 / Signatory	FDP_ACC.1/ Signature_Creation SFP, FMT_SMR.1, FMT_SMF.1[84]
FMT_MSA.2	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[84]

[84] See the note in section 6.1.4.6.

Requirement	Dependencies
FMT_SMR.1	FIA_UID.1
FPT_FLS.1	
FPT_PHP.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
ATE_COV.2	ADV_FSP.2, ATE_FUN.1
ATE_DPT.2	ADV_ARC.1, ADV_TDS.2, 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

6.5 Security Requirements Grounding in Objectives

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

Table 9: 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).

The Administrator is at first implicitly identified and authenticated after the card has changed its lifecycle from MANUFACTURING to ADMINISTRATION and (if required by the personalization model) later on by a successful authentication with an administrator key 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. The Transport-PIN is used to secure the TOE delivery process.

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 used only once for the activation of the dedicated file containing the SCD/SVD key pair.

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 ability to initially create the RAD (PIN, PUK and Transport-PIN) is restricted to the Administrator (FDP_ACC.1 / Personalisation SFP, FDP_ACF.1 / Personalisation SFP and FMT_SMF.1 (3)).

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 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) (cf. also 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:

- 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),
- 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 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 (4)), see also SS1 User Identification and Authentication.
The PUK can be modified but not unblocked. 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 SS1 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.

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. 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 Divisor) 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.

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 SS7 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).

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.

Technically, SS4 generates RSA signatures for SHA-1 [7], RIPEMD160 [5] or SHA-2 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:

[4] 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

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

[34] FIPS PUB 180-2 + Change Notice to include SHA-224: Secure Hash Standard, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2002, August 1

The Security Service SS4 supports RSA key length of 1024 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 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 (contact-based as well as RF-interface) of the underlying hardware.

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 (FPT_TEE.1). The following tests are performed during initial start-up (FPT_TST.1):

- The SLE66CLX800PE 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 [3] 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), during signature creation (SS4 Signature Creation), the verification of VAD, the unblocking and changing of 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 Random Number Generator (RNG), of the sensors and of the Active Shield is tested.
- All command parameters are checked for consistency.
- Prerequisites for command execution are checked (see also SS2).
- Before a random number from the RNG is used for the generation of the SCD/SVD key pair or for random padding used by Secure Messaging 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 [32].

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 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 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).

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) and/or enforces secure messaging (cf. 7.1.6).

7.1.6 SS6 Secure Messaging

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

Secure messaging (SS6) 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).

7.1.7 SS7 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 SS6 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 a key size of 1024 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.
  - Still during personalization the authenticated “Administrator” prepares a certificate request for the CGA that is signed with the SCD without prior PIN entry. The “Administrator” in this case acts on behalf of the “Signatory”, who must have given his consent for this special use of the SCD. The signature allows the CGA to verify the authenticity of the SVD.
- 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.

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 10 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) FTP_ITC.1/SVD Transfer FTP_ITC.1/DTBS Import FTP_TRP.1/TOE (SM with random padding for communication with SCA) 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 Operation	FMT_SMR.1 (authentication of Administrator) FDP_UIT.1/SVD Transfer FDP_UIT.1/TOE DTBS FTP_ITC.1/SVD Transfer FTP_ITC.1/DTBS import FTP_TRP.1/TOE (Secure Messaging)
FDP_SDI.2	Stored Data Integrity Monitoring and Action	FDP_SDI.2/Persistent

Table 10: 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 11 below.

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	
FCS_COP.1 (ECDSA)	Cryptographic Operation	Not used by TOE TSF
FCS_CKM.1 (EC)	Cryptographic Key Generation	
FCS_COP.1 (ECDH)	Cryptographic Operation	
FCS_COP.1 (RSA)	Cryptographic Operation	
FCS_CKM.1 (RSA)	Cryptographic Key Generation	

Table 11: 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 [25] , 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 [20] 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 12: 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] Italian Signature Law: Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999; Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

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

[4] 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

[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 180-1: 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] ISO/IEC 14443-3: 2001 Identification cards – Contactless Integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision, International Standard

[17] ISO/IEC 14443-4: 2001 Identification cards – Contactless Integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol, International Standard

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

[19] 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

[20] Certification report BSI-DSZ-CC-0482-2008 for SLE66CLX800PE / m1581-e13a/a14, SLE66CLX800PEM / m1580-e13a/a14, SLE66CLX800PES / m1582, SLE66CLX800PE / m1599-e13a/a14-e13a/a14, SLE66CLX360PE / m1587-e13a/a14, SLE66CLX360PEM / m1588-e13a/a14, SLE66CLX360PES / m1589-e13a/a14, SLE66CLX180PE / m2080-a14, SLE66CLX180PEM / m2081-a14, SLE66CLX120PE / m2082-a14, SLE66CLX180PEM / m2083-a14,,all optional with RSA 2048 V1.5 and ECC V1.1 and all with specific IC dedicated software from Infineon Technologies AG, 27.Mai.2008, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

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

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

[24] Administrator Guidance CardOS DI V4.2C CNS with Application for QES, Atos

[25] Security Target for SLE66CLX800PE / m1581-e13a/a14, SLE66CLX800PEM / m1580-e13a/a14, SLE66CLX800PES / m1582, SLE66CLX800PE / m1599-e13a/a14-e13a/a14, SLE66CLX360PE / m1587-e13a/a14, SLE66CLX360PEM / m1588-e13a/a14, SLE66CLX360PES / m1589-e13a/a14, SLE66CLX180PE / m2080-a14, SLE66CLX180PEM / m2081-a14, SLE66CLX120PE / m2082-a14, SLE66CLX180PEM / m2083-a14, all optional with libraries RSA 2048 V1.5 and ECC V1.1, Version 1.2, 2008-01-09 Infineon Technologies AG

[26] ADS Description CardOS DI V4.2C CNS with Application for QES, Atos

[27] Errata & delta Sheet - SLE66CxxxPE / MicroSlim Security Contoller Family, Controllers - Products and Bondouts, Release 11.07, Infineon

[28] Common Criteria for Information Technology Security Evaluation – Part1: Introduction and general model, Version 2.1, August 1999, CCIMB-99-031

[29] Common Criteria for Information Technology Security Evaluation – Part2: Security functional requirements, Version 2.1, August 1999, CCIMB-99-032

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

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

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

[33] User Guidance CardOS DI V4.2C CNS with Application for QES, Atos

[34] FIPS PUB 180-2 + Change Notice to include SHA-224: Secure Hash Standard, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2002, August 1

[35] 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

8.2 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
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
SFR	Security Functional Requirement
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 Functionality
TSFI	TSF Interface
VAD	Verification Authentication Data

8.3 Glossary

Operation	**Meaning**
SCD / SVD correspondence verification	Verification that the SCD and the SVD correspond cryptographically, i.e. it is assured that the SVD can be used to verify signatures created by the SCD.
Digital signature-generation	Process of signing a hash value sent by SCA and returning the signature as response to SCA.
Generation of SCD/SVD pair by User	Process, done by the Administrator, of sending an external command with the aim to generate an SCD/SVD cryptographic key pair together with the processing of the command.
Creation of RAD by Administrator	Process, done by the Administrator, of sending an external command with the aim to create RAD together with the processing of the command.
Sending of DTBS representation by SCA	Process of sending a hash value that represents the DTBS by the 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.
Export of SVD by User	Process of sending a command to read the SVD and of responding with the proper data.
Create the RAD	Process of sending an external command with the aim to create RAD together with the processing of the command.
DTBS-representation shall be sent	Possibility to check the source sending a hash value that represents the DTBS.
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/SVD management attribute	Setting the ability or non-ability to generate an SCD/SVD key pair.
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.
Changing 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
RF interface	Radio frequency interface, synonymous to contactless interface