JCOP_3_SECID _P40 SSCD

ChipDoc-Lite Applet in SSCD Configuration on JCOP3_SECID_P40

v1.2 — 18 Sep 2017 **Security Target Lite**

DDocument information

Info	Content
Keywords	Common Criteria, ASE, Security Target Lite
	JCOP_3_SECID_P40, ChipDoc-Lite, SSCD

Revision history

Rev	Date	Description
1.0	20170531	Release Version
1.1	20170717	Correct typo in CPLC Data
1.2	20170918	Add specified UGM references

Contact information

For more information, please visit: http://www.nxp.com

1. Introduction

1.1 ST Identification

Table 1. Security Target Identification

ST Title	**NXP JCOP_3_SECID_P40 ChipDoc-Lite in SSCD Configuration on NXP P40C072VE Microcontroller**
Authors	NXP Semiconductors
Status	Release
ST Reference	ST-JCOP_3_SECID_P40 SSCD-02
Version	1.2
Date	18 Sep 2017
Common Criteria	CC version 3.1 [1] Part 1: CCMB 2012-09-001 revision 4 [2] Part 2: CCMB 2012-09-002 revision 4 [3] Part 3: CCMB 2012-09-003 revision 4
PP Claim	[4] Protection profiles for Secure Signature Creation Device — Part 2: Device with key generation Version: 2.0.1, EAL 4+ Identification: BSI-CC-PP-0059-2009-MA-01
	[5] Protection profiles for Secure Signature Creation Device — Part 3: Device with key import Version: 1.0.2, EAL 4+ Identification: BSI-CC-PP-0075

1.2 TOE Identification

Table 2. TOE Identification

Title	**NXP JCOP_3_SECID_P40 ChipDoc-Lite in SSCD Configuration on NXP P40C072VE Microcontroller**
TOE Reference	NXP JCOP_3_SECID_P40_CDL-SSCD ROM Details Release Date: 0x5331 Release Level: 0x0001 ROM Code reference: JCOP_3_P40C072_SID_001 EEPROM O/S Patch: Patch 0x01 Applet Details ROM Integrated Applet: ChipDocLite version 1.0.10 Applet EEPROM patch: Patch 0x01 Configuration Details Applet Configuration: SSCD
Platform Composition	P40C072VE NXP Revision: E Certificate: NSCIB-CC17-65655 Interfaces: Contact Firmware Library NXP Version: 2.0 Certificate: NSCIB-CC-15-65156

1.3 Composite TOE

JCOP 3 SID (Operating System) Platform is embedded on NXP P40C072VE IC.

Both platform and CI are developed by NXP.

The composition analysis conducted in this section will use the words Platform to designate the contact only interface NXP P40C072VE IC [6, 7], Application to designate the software component (Operating System) JCOP 3 SID, and Composite Product to designate the TOE.

According to the Composite product documentation [14], the different roles considered in the composition activities are associated as follows:

Platform Developer	NXP
Platform Evaluator	BrightSight
Platform Certification Body	TÜVRheinland
Platform certificate	NSCIB-CC17-65655
Application Developer	NXP
Composite Product Integrator	NXP
Composite Product Evaluator	Brightsight
Composite Product Certification Body	TÜVRheinland
Composite Product evaluation Sponsor	NXP

See composition requirements coverage:

[R1] Platform was evaluated to CC EAL 5+ according to BSI-PP-0035 and Composite Product ST relies on this claim.

[R2] Platform Security Target is available.

[R3] Evaluated versions of the Platform and Application are exposed

[R4] Integration evidences are provided as part of the process.

[R5] Integration is guided by delivery procedures enforced by NXP.

[R6] Integration process involves all configuration parameters provided by NXP Athena SCS department.

[R7] Application development process incorporates the Platform User Guide as technical input.

[R8] EAL 5+ certification of the Platform provides:

- List of applicable Technical Guides, Application Notes and Errata Sheets
- Certified Platform ETR
- Platform Certification Report

[R9] TOE Test Plan describes validation of the Application on Platform dedicated emulator.

[R10] TOE Test Plan describes validation of the Application on the Platform.

[R11] Platform certification includes testing evaluation.

[R12] Platform samples are delivered by NXP to TOE's evaluator for testing purpose.

[R13] Composite Product samples are delivered by NXP to TOE's evaluator for penetration testing purpose.

[R14] Platform open samples are delivered by NXP to TOE's evaluator for testing purpose.

[R15] EAL 5+ certification of the Platform provides Certified Platform ETR-Lite and Certification Report.

Integration of the composite product by the IC manufacturer is guided by delivery procedures enforced by NXP.

1.4 TOE Overview

The TOE implements a Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC [12] as a smart card which allows the generation and importation of signature creation data (SCD) and the creation of qualified electronic signatures. The TOE protects the SCD and ensures that only an authorized Signatory can use it.

The TOE meets all the following requirements as defined in the European Directive (article 2.2):

(a) it is uniquely linked to the signatory
(b) it is capable of identifying the signatory
(c) it is created using means that the signatory can maintain under his sole control
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The TOE type is compliant with both of the claimed PPs, which are not considered to be mutually exclusive:

BSI-CC-PP-0059-2009-MA-01	Secure Signature Creation Device with Key Generation
BSI-CC-PP-0075	Secure Signature Creation Device: Device with Key Import

The TOE is compliant with the representation provided in both PPS.

The conformance to the PPs is strict.

The TOE Secure Signature-Creation Device representing the SCD/SVD import, generation, SCD Storage and signature-creation components.
The TOE is a personalized component, meaning that it can only be used for signature-creation by one specific user – the signatory – only.

N.B. : Although the notion of SSCD types is no longer supported in the published EN's, the previous set of standards defining Secure Signature Creation device used 'Type 2' to define an SSCD that can import the SCD/SVD keys and 'Type 3' to define an SSCD which could generate it's own SCD/SVD key-pairs. This terminology is still used within industry.

2. Target of Evaluation

The TOE for this security target, specified in European standards prEN 14169-2 and prEN 14169-3 for Secure Signature Creation Devices with Key Generation and Key Import respectively is a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD). The SSCD protects the SCD during its whole life cycle as to be used in a signature-creation process solely by its signatory.

> NOTE: In this clause the term **TOE** is used as reference to the target of evaluation for the protection profiles (PP0059 [4] and PP0075 [5]) specified in the European standard prEN 14169. The term **SSCD** is used to refer to a product that incorporates the TOE.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the digital signature.

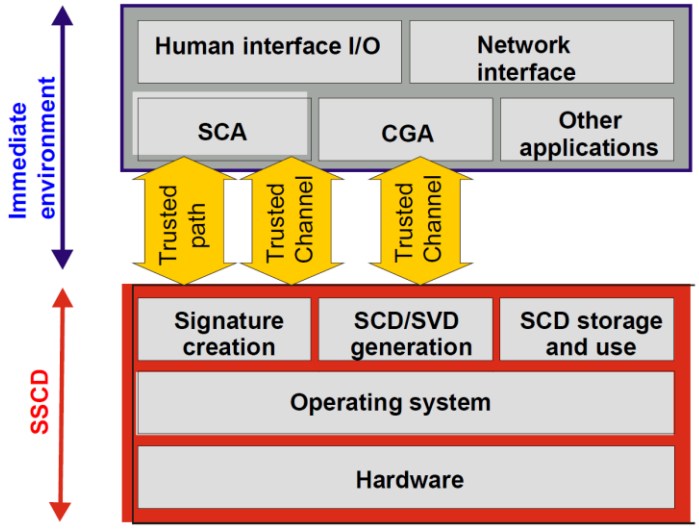

Fig 1. SSCD Scope, Structural View

Fig 1 shows the TOE scope from a structural perspective. The SSCD, i.e. 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 shall communicate with the TOE over a trusted channel, a trusted path for the human interface provided by the SCA, respectively.

The TOE described in this ST is a smart card operating system implemented on a smart card IC which is certified CC EAL 5+. The TOE includes embeddable software in the NVM of the IC and a file system including the digital signature application stored in EEPROM. Parts of the operating systems may be stored in EEPROM.

2.1 Secure Signature Creation Device (SSCD)

An SSCD provides the following functions:

- to generate or import signature-creation data (SCD) and the correspondent signature-verification data (SVD),
- to export the SVD for certification if this has been created by the device and optionally receive and
- store certificate info,
- to initialize user authentication data (RAD),
- to switch the SSCD from a non-operational state to an operational state, and
- if in an operational state, to create digital signatures for data with the following steps:

  (a) select an SCD if multiple are present in the SSCD,
  (b) receive data to be signed or a unique representation thereof (DTBS/R)
  (c) authenticate the signatory and determine its intent to sign,
  (d) apply an appropriate cryptographic signature-creation function using the selected SCD to the DTBS/R.

An SSCD shall only be switched to an operational state if it is properly prepared for the signatory's use and sole control by

— generating at least one SCD/SVD pair, and
— personalising for the signatory by storing in the TOE:
  (a) the signatory’s reference authentication data (RAD)
  (b) optionally, certificate info for at least one SCD in the TOE.

Upon receiving an SSCD the signatory shall verify that any SCD it contains is in a non-operational state.

The SSCD provides management functions for key generation or import initiated by the user as specified in 2.1.1.2.

2.1.1 Additional Functions

2.1.1.1 User Authentication

The SSCD provides functions to enable the user to

(1) Unblock the RAD,
(2) Change the value of the RAD,
(3) Add or modify user information to be included in signatory identification data in a SVD certificate.

2.1.1.2 User Management of Signing Key

The SSCD provides functions to enable the user to

(1) Install an SCD, generated outside the device in a trusted environment and communicated over a secure communication link 2.1.1.3(2)
(2) Generate an SCD,
(3) Disabling an SCD it holds, e.g. by erasing it from memory,
(4) Create, extend or modify certificate info stored in the device, and
(5) Create SVD for an SCD stored and export it for certification by a certificate generating application protected by trusted communication (2.1.1.3 (1)).

2.1.1.3 Secure Communication

The SSCD provides functions to establish a trusted, cryptographically protected communication with

(1) A certificate-generation application,
(2) An SVD-generating application, and
(3) A signature-creation application.

The supported functions include functions for management of the cryptographic keys, parameters and configuration used to establish the trusted communication.

2.2 SSCD Product Lifecycle

The life cycle of a generic SSCD product is given here, in Fig 2, to introduce the role of the SSCD Provisioning service.

The SSCD Life-cycle distinguishes stages for development, production, preparation and operational use. Development and production of the SSCD together constitute the development phase of the TOE. The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class. The development phase ends with the delivery of the TOE to an SSCD-provisioning service provider. The functional integrity of the TOE shall be protected in delivering it to an SSCD-provisioning service provider.

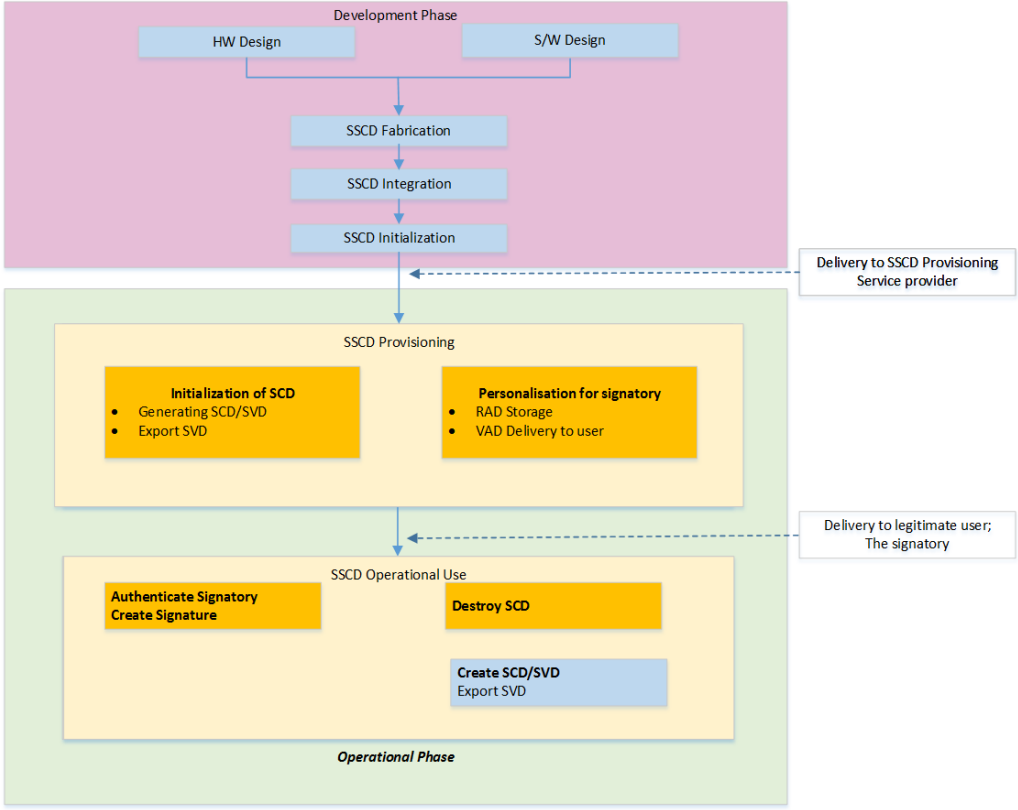

Fig 2. SSCD Product Life-Cycle

2.2.1 Development Phase

2.2.1.1 S/W and H/W Design

The TOE is developed in this phase. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

H/W Design	– NXP
S/W Design	– NXP Development departments – Livingston, Scotland

2.2.1.2 SSCD Fabrication

H/W Fabrication	– NXP
S/W implementation	– NXP Development departments – Livingston, Scotland
IC Manufacturing	– NXP

The software parts of the TOE which are developed by NXP are transferred in a secure way for masking in ROM. In addition to the TOE, the mask contains confidential data, knowledge of which is required in order to initialize and personalize the chip.

2.2.1.3 SSCD Integration

IC Manufacturing	– NXP
IC Packaging	– NXP
Card Manufacturing	– NXP

This phase corresponds to the integration of the hardware and firmware components into the final product body. The TOE is protected during transfer between various parties.

IC Packaging and Card Manufacturing are not part of the scope of this TOE.

2.2.1.4 SSCD Initialization

Initialization	– NXP

The TOE and the confidential information required to complete this phase are transferred securely between the NXP sites. Initialization is done within NXP facilities used for the Common Criteria certified ICs production, under the governance of NXP.

The initialization phase consists of the application configuration and could include patching (in EEPROM) if required. During this phase, the SSCD File System is initiated and the General Application Data are loaded (EEPROM). Once the SSCD file System is initiated, patching commands are no longer available.

The product becomes operational and is delivered to the SSCD Provisioning Service after this initialization phase. The card is protected by a Transport Key during the transfer between NXP Manufacturing and the SSCD Provisioning Service site.

2.2.2 Operational Phase

This ST addresses the functions used in the operational phases but developed during development phase.

Usage – Where upon the card is delivered from the Customer (the Card Issuer) to the End User and the End User may use it for signature-creation including all supporting functionality (e.g., SCD storage and SCD use) but only following a correct verification of the initial PIN-Activate PIN which allows the End User to make sure that he is the first user to ever use this SCA for electronic signature.

The product is considered in use phase.

2.2.2.1 SSCD Provisioning

An SSCD-provisioning service provider having accepted it from a manufacturer prepares the TOE for use and delivers it to its legitimate user. The preparation phase ends when the legitimate user of the TOE, having received it from an SSCD provisioning service enables an SCD it holds for use in signing.

During preparation of the TOE, an SSCD-provisioning service provider performs the following tasks:

- Obtain information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user of the TOE;
- Generate a PIN and/or obtain a biometric sample of the legitimate user, store this data as RAD in the TOE and prepare information about the VAD for delivery to the legitimate user;
- Generate a certificate for at least one SCD either by:
  (a) The TOE generating an SCD/SVD pair and obtaining a certificate for the SVD exported from the TOE, or
  (b) Initializing security functions in the TOE for protected export of the SVD and obtaining a certificate for the SVD after receiving it from the TOE;
- Optionally, present certificate info to the SSCD;
- Deliver the TOE and the accompanying VAD info to the legitimate user.

The SVD certification task (third list item above) of an SSCD-provisioning service provider as specified in this PP may support a centralised, pre-issuing key generation process, with at least one key generated and certified, before delivery to the legitimate user. Alternatively, or additionally, that task may support key generation by the signatory after delivery and outside the secure preparation environment. A TOE may support both key generation processes, for example with a first key generated centrally and additional keys generated by the signatory in the operational use stage.

Data required for inclusion in the SVD certificate at least includes (**The Directive:Annex** II):

- The SVD;
- The name of the signatory either:
  (a) A legal name, or
  (b) A pseudonym together with an indication of this fact.

The data included in the certificate may have been stored in the SSCD during personalization.

Before initiating the actual certificate signature the certificate-generating application verifies the SVD received from the TOE by asserting:

- the sender as genuine SSCD
- the integrity of the SVD to be certified as sent by the originating SSCD,
- that the originating SSCD has been personalized for the legitimate user,
- correspondence between SCD and SVD, and

- that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

The proof of correspondence between an SCD stored in the TOE and an SVD may be implicit in the security mechanisms applied by the CGA. Optionally, the TOE may support a function to provide an explicit proof of correspondence between an SCD it stores and an SVD realized by self-certification. Such a function may be performed implicitly in the SVD export function and may be invoked in the preparation environment without explicit consent of the signatory[i]. Security requirements to protect the SVD export function and the certification data if the SVD is generated by the signatory and then exported from the SSCD to the CGA are specified in part 4 of this series of European standards

Prior to generating the certificate the certification service provider shall assert the identity of the signatory as the legitimate user of the TOE.

After preparation the intended, legitimate user should be informed of the signatory's verification authentication data (VAD) required for use of the TOE in signing. If the VAD is a password or PIN, providing this information to the legitimate user shall protect the confidentiality of the corresponding RAD.

2.2.2.2 SSCD Operational Use

In the operational-use stage the signatory can use the TOE to create advanced electronic signatures.
The signatory can render an SCD in the TOE permanently unusable. Rendering the last SCD in the TOE permanently unusable may end the life of the TOE as SSCD.

> NOTE: An SSCD that supports key generation in the operational-use stage does not end its life when it no longer has a usable SCD.

The TOE may support functions to generate signing keys in the operational stage (6.2.2.3(2)). For an additional key the signatory may be allowed to choose the kind of certificate (qualified, or not) to obtain for the SVD of the new key. The signatory may also be allowed to choose some of the data to be incorporated in the certificate, for instance to use a pseudonym instead of the legal name4. If the conditions to obtain a qualified certificate are met the new key can also be used to create advanced electronic signatures. The optional TOE functions for additional key generation and certification may require additional security functions in the TOE and an interaction with the SSCD-Provisioning service provider in an environment that is secure or using trusted communication.

2.2.3 Application Note: Scope of SSCD PP application

This ST refers to qualified certificates as electronic attestation of the SVD corresponding to the signatory's SCD that is implemented by the TOE.

While the main application scenario of a SSCD will assume a qualified certificate to be used in combination with a SSCD, there still is a large benefit in the security when such SSCD is applied in other areas and such application is encouraged. The SSCD may as well be applied to environments where the certificates expressed as 'qualified certificates' in the SSCD do not fulfil the requirements laid down in Annex I and Annex II of the Directive [12].

When an instance of a SSCD is used with a qualified certificate, such use is from the technical point of view eligible for an electronic signature as referred to in Directive [12],

article 5, paragraph 1. This Directive does not prevent TOE itself from being regarded as a SSCD, even when used together with a non-qualified certificate.

2.3 TOE Form Factor & Physical Interfaces

Typically the TOE is provided as an ISO-7816 module or card.

The TOE is linked to a card reader/writer via its HW and physical interfaces.

- The contact type interface of the TOE smartcard is ISO/IEC 7816 compliant.
- Engineering packages may be combined with NXP carrier boards to provide ISO-7816 compliant interface.

There are no other external interfaces of the TOE except the ones described above.

The card reader/writer is connected to a computer such as a personal computer and allows application programs (APs) to use the TOE.

2.4 TOE Guidance

The TOE guidance comprises the following documentation:

Table 3. TOE Guidance

Applicable Guidance Documents

Title	Version
um369010_JCOP 3 SecID P40 User Guidance and Administrator Manual_1.0	V1.0; 06 Jun 2016
um376712_ChipDoc Lite 1.0 Applet User Manual_1.2	V1.2; 04 Nov 2016
Hestia_SSCD_CertifiedConfiguration_v0_2_20170405	V0.2; 05 Apr 2017

3. Conformance Claims

3.1 CC Conformance claims

The ST claims compliance with the following references:

- Common Criteria Version 3.1 Part 1 [1] revision 4
- Common Criteria Version 3.1 Part 2 [2] revision 4 extended
- Common Criteria Version 3.1 Part 3 [3] revision 4 conformant

Extensions are based on the Protection Profiles (PP [4] and PP [5]) presented in the next section:

- FPT_EMS.1 'TOE emanation'

The assurance level for this ST is EAL 4 augmented with:

- AVA_VAN.5
- ALC_DVS.2

3.2 PP Claim

This ST claims strict compliance to the following SOGIS Protection Profiles:

[4]	Protection Profile — Secure Signature-Creation Device Type 2
Document ID	prEN 14169-2:2012 (E)
Version	2.0.1
Date	2012-01-23
Sponsor	CEN/ISSS
Certification Body	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Registration	BSI-CC-PP-0059-2009-MA-01

[5]	Protection Profile — Secure Signature-Creation Device Type 3
Document ID	prEN 14169-3:2012 (E)
Version	1.0.2
Date	2012-07-24
Sponsor	CEN/ISSS
Certification Body	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Registration	BSI-CC-PP-0075

4. Security Problem Definition

4.1 Assets

SCD

Private key used to perform a digital signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.

SVD

Public key linked to the SCD and used to perform digital signature verification. The integrity of the SVD when it is exported must be maintained.

DTBS and DTBS/R

Set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the digital signature must be maintained.

Signature-creation function

Code of the SSCD dedicated to the generation of digital signature of DTBS using the SCD (The integrity of the function must be maintained so that it can participate to the legal validity of electronic signatures)

4.2 Subjects

This Security Target considers the following users and subjects representing users:

Table 4. Users & Subjects

Users	Subjects	Definition
User	**S.User**	End user of the TOE which can be identified as S.Admin or S.Signatory. The subject S.User may act as S.Admin in the role *Administrator* or as S.Signatory in the role *Signatory*.
Administrator	**S.Admin**	User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. The subject S.Admin is acting in the role *Administrator* for this user after successful authentication as *Administrator*
Signatory	**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. The subject S.Signatory is acting in the role *Signatory* for this user after successful authentication as *Signatory*.

4.3 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used:

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 electronic signature of the CSP.

A.SCA	*Trustworthy signature-creation application*

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of data the signatory wishes to sign in a form appropriate for signing by the TOE.

A.CSP	*Secure SCD/SVD management by CSP*

The CSP uses only a trustworthy SCD/SVD generation device and ensures that this device can be used by authorised user only. The CSP ensures that the SCD generated practically occurs only once, that generated SCD and SVD actually correspond to each other and that SCD cannot be derived from the SVD. The CSP ensures the confidentiality of the SCD during generation and export to the TOE, does not use the SCD for creation of any signature and irreversibly deletes the SCD in the operational environment after export to the TOE.

4.4 Threats

4.4.1 Threat Agents

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

4.4.2 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 obtain 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.SVD_Forgery	*Forgery of the signature-verification data*

An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

T.DTBS_Forgery	*Forgery of the DTBS/R*

An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R 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.

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.

4.5 Organizational Security Policy

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

P.CSP_QCert	*Qualified certificate*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (The Directive: 2:9, Annex I) for the SVD generated by the SSCD. The certificates contain at least 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 as SSCD 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 an advanced electronic, which is a qualified electronic signature if it is based on a valid qualified certificate. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the digital signature created with a SCD implemented in the SSCD that the signatory maintains under his sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

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.Sig_Non-Repud	*Non-repudiation of signatures*

The lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

5. Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

5.1 Security Objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

OT.EMSEC_Design	*Provide physical emanations security*

The TOE shall be designed and built 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 initialization, personalisation and operational usage. The TOE shall provide functionality to securely destroy the SCD on demand of the signatory.

Application note 1: The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD import. The signatory shall be able to destroy the SCD stored in the SSCD, e.g. after the (qualified) certificate for the corresponding SVD has been expired.

OT.SCD/SVD_Auth_Gen *Authorized SCD/SVD generation*

The TOE shall provide security features to ensure that authorised users only may invoke the generation of the SCD and the SVD.

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.

Application note 2: The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD import, signature creation operation, storage and secure destruction.

OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD.

OT.Tamper_ID *Tamper detection*

The TOE shall provide system features that detect physical tampering of a system component, and use those features to limit security breaches.

OT.Tamper_Resistance *Tamper resistance*

The TOE shall prevent or resist physical tampering with specified system devices and components.

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

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

OT.DTBS_Integrity_TOE *Verification of the DTBS/R integrity*

The TOE must not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation.

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

The TOE shall provide 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 shall create electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the electronic signatures or any other data exportable from the TOE. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.SCD_Auth_Imp *Authorized SCD import*

The TOE shall provide security features to ensure that authorized users only may invoke the import of the SCD.

5.2 Security Objectives for the Operational Environment

Security objectives for the operational environment which are independent from the fact whether SCD are imported from the operational environment or generated by the TOE itself are OE.SVD_Auth, OE.CGA_QCert, OE.SSCD_Prov_Service, OE.HID_VAD, OE.DTBS_Intend, OE.DTBS_Protect and OE.Signatory. The remaining four security objectives OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique and OE.SCD_SVD_Corresp only apply if the TOE supports key import, which this TOE does.

OE.SVD_Auth	*Authenticity of the SVD*

The operational environment shall ensure the authenticity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

OE.CGA_QCert	*Generation of qualified certificates*

The CGA generates a qualified certificate that includes, inter alias

(a) the name of the signatory controlling the TOE,
(b) the SVD matching the SCD stored in the TOE and controlled by the signatory,
(c) the advanced signature of the CSP.

The CGA confirms with the generated certificate that the SCD corresponding to the SVD is stored in a SSCD.

OE.SSCD_Prov_Service *Authentic SSCD provided by SSCD Provisioning Service*

The SSCD-provisioning service shall initialise and personalise for the signatory an authentic copy of theTOE and deliver this copy as SSCD to the signatory.

OE.HID_VAD	*Protection of the VAD*

If an external device provides the human interface for user authentication, this device shall ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface. In particular, if the TOE requires a trusted channel for import of the VAD, the HID shall support usage of this trusted channel.

OE.DTBS_Intend	*SCA sends data intended to be signed*

The signatory shall use a trustworthy SCA that

(a) generates the DTBS/R 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/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,

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

Application note 3: The SCA should be able to support advanced electronic signatures. Currently, there exist three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CadES [22], XadES [23] and PadES [24]. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.

OE.DTBS_Protect	*SCA protects the data intended to be signed*

The operational environment shall ensure that the DTBS/R cannot be altered in transit between the SCA and the TOE. In particular, if the TOE requires a trusted channel for import of the DTBS/R, the SCA shall support usage of this trusted channel.

OE.Signatory	*Security obligation of the Signatory*

The Signatory checks that the SCD stored in the SSCD received from SSCD provisioning service is in non-operational state. The Signatory keeps his or her VAD confidential.

OE.SCD/SVD_Auth_Gen	*Authorized SCD/SVD generation*

The CSP shall provide security features to ensure that authorised users only may invoke the generation of the SCD and the SVD.

OE.SCD_Secrecy	*SCD Secrecy*

The CSP shall protect the confidentiality of the SCD during generation and export to the TOE. The CSP shall not use the SCD for creation of any signature and shall irreversibly delete the SCD in the operational environment after export to the TOE.

OE.SCD_Unique	*Uniqueness of the signature-creation data*

The CSP shall ensure the cryptographic quality of the SCD/SVD pair, which is generated in the environment, for the qualified or advanced electronic signature. The SCD used for

signature creation shall practically occur only once, i.e. the probability of equal SCDs shall be negligible, and the SCD shall not be reconstructable from the SVD.

OE.SCD_SVD_Corresp	*Correspondence between SVD and SCD*

The CSP shall ensure the correspondence between the SVD and the SCD generated by the CSP. This includes the correspondence between the SVD send to the CGA and the SCD exported to the TOE of the signatory identified in the SVD certificate.

5.3 Security Objectives Rationale

All the security objectives described in the ST are traced back to items described in the TOE security environment and any items in the TOE security environment are covered by those security objectives appropriately.

5.3.1 Security Objectives Coverage

The following table indicates that all security objectives of the TOE are traced back to threats and/or organizational security policies and that all security objectives of the environment are traced back to threats, organizational security policies and/or assumptions.

Threats Assumptions Policies / Security objectives	OT.EMSEC_Design	OT.lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.SCD_Auth_Imp	OE.CGA_Qcert	OE.SVD_Auth	OE.HID_VAD	OE.SCD/SVD_Auth_Gen	OE.SSCD_Prov_Service	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.SCD_SVD_Corresp	OE.SCD_Secrecy	OE.SCD_Unique
T.Hack_Phys	x			x		x	x																
T.SCD_Divulg				x								x				x						x	
T.SCD_Derive			x								x												x
T.SVD_Forgery					x									x							x		
T.DTBS_Forgery									x									x	x				
T.SigF_Misuse		x							x	x					x			x	x	x			
T.Sig_Forgery								x			x		x										x
A.CGA													x	x									
A.SCA																		x					
A.SCP																x					x	x	x
P.CSP_Qcert		x			x							x	x			x					x		
P.Qsign										x	x		x					x					
P.Sigy_SSCD	x	x	x	x			x	x	x	x	x	x				x	x					x	x
P.Sig_Non-Repud	x	x		x	x	x	x	x	x	x	x		x	x			x	x	x	x	x	x	x

Table 1 – Security Environment to Security Objectives Mapping

5.3.2 Security Objectives Sufficiency

5.3.2.1 Policies and Security Objective Sufficiency

P.CSP_QCert (CSP generates qualified certificates) establishes the CSP generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD under sole control of this signatory. **P.CSP_QCert** is addressed by:

- the TOE security objective **OT.Lifecycle_Security**, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- the TOE security objective **OT.SCD_SVD_Corresp**, which requires the TOE to ensure the correspondence between the SVD and the SCD during their generation, and
- the security objective for the operational environment **OE.CGA_QCert** for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory
- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation,

personalisation and operational usage,

- OE.SCD/SVD_Auth_Gen, which ensures that the SCD/SVD generation can be invoked by authorized users only,
- OT.SCD_Auth_Imp which ensures that authorised users only may invoke the import of the SCD,
- OE.SCD_SVD_Corresp, which requires the CSP to ensure the correspondence between the SVD and the SCD during their generation, and
- OE.CGA_QCert for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature generation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE generates digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. The OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

P.Sigy_SSCD (*TOE as secure signature-creation device*) requires the TOE to meet **Annex** III. This is ensured as follows:

- **OT.SCD_Unique** meets the paragraph 1(a) of **Annex** III, by the requirements that the SCD used for signature generation can practically occur only once;
- **OT.SCD_Unique**, **OT.SCD_Secrecy** and **OT.Sig_Secure** meet the requirement in paragraph 1(a) of **Annex** III by the requirements to ensure secrecy of the SCD. **OT.EMSEC_Design** and **OT.Tamper_Resistance** address specific objectives to ensure secrecy of the SCD against specific attacks;
- **OT.SCD_Secrecy** and **OT.Sig_Secure** ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE;
- **OT.Sigy_SigF** ensure that the TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others;
- **OT.DTBS_Integrity_TOE**: the TOE must not alter the DTBS/R.

The usage of SCD under sole control of the signatory is ensured by :

- **OT.Lifecycle_Security** requiring the TOE to detect flaws during the initialisation, personalisation and operational usage,
- **OT.SCD/SVD_Gen**, which limits invoke the generation of the SCD and the SVD to authorised users only,

- **OT.Sigy_SigF**, which requires the TOE to provide the signature generation function for the legitimate signatory only and to protect the SCD against the use of others.
- **OT.SCD_Auth_Imp,** which limits SCD import to authorised users only,
- **OE.SCD_Secrecy**, which ensures the confidentiality of the SCD during generation and export to the TOE, and deletes the SCD after export to the TOE. The CSP does not use the SCD for signature creation.

OE.SSCD_Prov_Service ensures that the signatory obtains a TOE sample as an authentic, initialised and personalised SSCD from an SSCD provisioning service.

P.Sig_Non-Repud (*Non-repudiation of signatures***)** deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensure the aspects of signatory's sole control over and responsibility for the digital signatures generated with the TOE. **OE.SSCD_Prov_Service** ensures that the signatory uses an authentic TOE, initialised and personalised for the signatory. **OE.CGA_QCert** ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. **OE.SVD_Auth** and **OE.CGA_QCert** require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. **OT.SCD_SVD_Corresp** ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. **OT.SCD_Unique** provides that the signatory's SCD can practically occur just once.

OE.SCD/SVD_Auth_Gen, **OE.SCD_Secrecy** and **OE.SCD_Unique** ensure the security of the SCD in the CSP environment. **OE.SCD_Secrecy** ensures the confidentiality of the SCD during generation, during and after export to the TOE. The CSP does not use the SCD for creation of any signature and deletes the SCD irreversibly after export to the TOE. **OE.SCD_Unique** provides that the signatory's SCD can practically occur just once. **OE.SCD_SVD_Corresp** ensures that the SVD in the certificate of the signatory corresponds to the SCD that is implemented in the copy of the TOE of the signatory.

OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD of the signatory. **OE.SVD_Auth** and **OE.CGA_QCert** require the environment to ensure the authenticity of the SVD as being exported by the TOE under sole control of the signatory. **OE.CGA_QCert** ensures that the certificate allows to identify the signatory and thus to link the SVD of the signatory. **OE.SVD_Auth** and **OE.CGA_QCert** require the environment to ensure the authenticity of the SVD as being exported by the TOE under sole control of the signatory.

OE.Signatory ensures that the Signatory checks that the SCD, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the Signatory becomes into sole control over the SSCD). **OT.Sigy_SigF** provides that only the signatory may use the TOE for signature creation. As prerequisite **OE.Signatory** ensures that the Signatory keeps his or her SVAD confidential. **OE.DTBS_Intend**, **OE.DTBS_Protect** and **OT.DTBS_Integrity_TOE** ensure that the TOE generates digital signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by **OT.Sig_Secure** ensure that only this SCD may generate a valid digital signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE **OT.Lifecycle_Security** (*Lifecycle security*), **OT.SCD_Secrecy** (*Secrecy of the signature-creation data*), **OT.EMSEC_Design** (*Provide physical emanations security*), **OT.Tamper_ID** (*Tamper detection*) and **OT.Tamper_Resistance** (*Tamper resistance*) protect the SCD against any compromise.

5.3.2.2 Threats and Security Objective Sufficiency

T.SCD_Divulg (*Storing, copying, and releasing of the signature-creation data***)** addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in recital (18) of **The European Directive**. This threat is countered by **OE.SCD_Secrecy**, which assures the secrecy of the SCD in the CSP environment, and **OT.SCD_Secrecy**, which assures the secrecy of the SCD during use by the TOE for signature creation.

Furthermore, generation and/or import of SCD known by an attacker is countered by **OE.SCD/SVD_Auth_Gen**, which ensures that only authorized SCD generation in the environment is possible, and **OT.SCD_Auth_Imp**, which ensures that only authorised SCD import is possible.

T.SCD_Derive (*Derive the signature-creation data***)** deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. **OT.SCD/SVD_Gen** counters this threat by implementing cryptographic secure generation (as well as **OE.SCD_Unique**)of the SCD/SVD-pair. **OT.Sig_Secure** ensures cryptographic secure digital signatures.

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. OT.EMSEC_Design** counters physical attacks through the TOE interfaces and observation of TOE emanations. **OT.Tamper_ID** and **OT.Tamper_Resistance** counter the threat **T.Hack_Phys** by detecting and by resisting tampering attacks.

T.SVD_Forgery (*Forgery of the signature-verification data***)** deals with the forgery of the SVD exported by the TOE to the CGA to generation a certificate. T.SVD_Forgery is addressed by **OE.SCD_SVD_Corresp** or **OT.SCD_SVD_Corresp** (depending if SCD/SVD generation occurs in the SSCD Type 1 or in the TOE), which ensure correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and **OE.SVD_Auth** that ensures the integrity of the SVD exported by the TOE to the CGA. **T.SVD_Forgery** is also addressed by **OE.SVD_Auth,** which ensures the authenticity of the SVD given to the CGA of the CSP.

T.SigF_Misuse (*Misuse of the signature-creation function of the TOE*) addresses the threat of misuse of the TOE signature-creation function to create SDO by others than the signatory to create a digital signature on data for which the signatory has not expressed the intent to sign,. **OT.Lifecycle_Security** (*Lifecycle security*) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. **OT.Sigy_SigF** (*Signature creation function for the legitimate signatory only*) ensures that the TOE provides the signature-generation function for the legitimate signatory only. **OE.DTBS_Intend** (*Data intended to be signed*) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and **OE.DTBS_Protect** counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. **OT.DTBS_Integrity_TOE** (*DTBS/R integrity inside the TOE*) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, **OE.HID_VAD** (*Protection of the VAD*) provides confidentiality and integrity of the VAD as needed by the authentication method employed. **OE.Signatory** ensures that the Signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the Signatory becomes control

over the SSCD. **OE.Signatory** ensures also that the Signatory keeps his or her VAD confidential.

T.DTBS_Forgery (*Forgery of the DTBS/R***)** addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of **OE.DTBS_Intend**, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of **OE.DTBS_Protect**, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of **OT.DTBS_Integrity_TOE** by ensuring the integrity of the DTBS/R inside the TOE.

T.Sig_Forgery (*Forgery of the digital signature***)** deals with non-detectable forgery of the digital signature. **OT.Sig_Secure**, **OT.SCD_Unique** and **OE.CGA_Qcert** address this threat in general. The **OT.Sig_Secure** (*Cryptographic security of the digital signature*) ensures by means of robust cryptographic techniques that the signed data and the digital signature are securely linked together. **OT.SCD_Unique** ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. **OE.CGA_Qcert** prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision on a forged signature. **OE.SCD_Unique** ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

5.3.2.3 Assumptions and Security Objective Sufficiency

A.SCA (*Trustworthy signature-creation application***)** establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by **OE.DTBS_Intend** *(Data intended to be signed*) which ensures that the SCA generates the DTBS/R for 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** (*Authenticity of the SVD*), which ensures the protection of the integrity and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

A.CSP (Secure SCD/SVD management by CSP) establishes several security aspects concerning handling of SCD and SVD by the CSP. That the SCD/SVD generation device can only be used by authorized users is addressed by **OE.SCD/SVD_Auth_Gen** (Authorized SCD/SVD Generation), that the generated SCD is unique and cannot be derived by the SVD is addressed by **OE.SCD_Unique** (Uniqueness of the signature creation data), that SCD and SVD correspond to each other is addressed by **OE.SCD_SVD_Corresp** (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are

deleted in the environment once exported to the TOE is addressed by **OE.SCD_Secrecy** (SCD Secrecy).

5.3.3 Security Objectives Coverage

Table 5. Security Environment to Security Objectives Mapping

Threats Assumptions Policies / Security objectives	OT.EMSEC_Design	OT.lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.SCD_Auth_Imp	OE.CGA_Qcert	OE.SVD_Auth	OE.HID_VAD	OE.SCD/SVD_Auth_Gen	OE.SSCD_Prov_Service	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.SCD_SVD_Corresp	OE.SCD_Secrecy	OE.SCD_Unique
T.Hack_Phys	x			x		x	x																
T.SCD_Divulg				x								x				x						x	
T.SCD_Derive			x								x												x
T.SVD_Forgery					x									x							x		
T.DTBS_Forgery									x									x	x				
T.SigF_Misuse		x							x	x					x			x	x	x			
T.Sig_Forgery								x			x		x										x
A.CGA													x	x									
A.SCA																		x					
A.CSP																x					x	x	x
P.CSP_Qcert		x			x							x	x			x					x		
P.Qsign										x	x		x					x					
P.Sigy_SSCD	x	x	x	x			x	x	x	x	x	x				x	x					x	x
P.Sig_Non-Repud	x	x		x	x	x	x	x	x	x	x		x	x			x	x	x	x	x	x	x

5.3.4 Security Objectives Sufficiency

5.3.4.1 Policies and Security Objective Sufficiency

P.CSP_QCert (CSP generates qualified certificates) establishes the CSP generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD under sole control of this signatory. **P.CSP_QCert** is addressed by

- **OT.Lifecycle_Security**, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- **OE.SCD/SVD_Auth_Gen**, which ensures that the SCD/SVD generation can be invoked by authorized users only,
- **OT.SCD_Auth_Imp** which ensures that authorised users only may invoke the import of the SCD,
- **OE.SCD_SVD_Corresp**, which requires the CSP to ensure the correspondence between the SVD and the SCD during their generation, and
- **OE.CGA_QCert** for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature generation function for the legitimate signatory only and to protect the SCD against the

use of others. OT.Sig_Secure ensures that the TOE generates digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. The OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

P.Sigy_SSCD (*TOE as secure signature-creation device*) requires the TOE to meet **Annex** III. This is ensured as follows:

- **OT.SCD_Unique** meets the paragraph 1(a) of **Annex** III, by the requirements that the SCD used for signature generation can practically occur only once;
- **OT.SCD_Unique**, **OT.SCD_Secrecy** and **OT.Sig_Secure** meet the requirement in paragraph 1(a) of **Annex** III by the requirements to ensure secrecy of the SCD. **OT.EMSEC_Design** and **OT.Tamper_Resistance** address specific objectives to ensure secrecy of the SCD against specific attacks;
- **OT.SCD_Secrecy** and **OT.Sig_Secure** meet the requirement in paragraph 1(b) of **Annex** III by the requirements to ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE;
- **OT.Sigy_SigF** meets the requirement in paragraph 1(c) of **Annex** III by the requirements to ensure that the TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others;
- **OT.DTBS_Integrity_TOE** meets the requirements in paragraph 2 of **Annex** III as the TOE must not alter the DTBS/R.

Paragraph 2 of **Annex** III, requires that an SSCD does not prevent the data to be signed from being presented to the signatory prior to the signature process is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the signatory and send it to the SSCD for signing.

The usage of SCD under sole control of the signatory is ensured by

- **OT.Lifecycle_Security** requiring the TOE to detect flaws during the initialisation, personalisation and operational usage,
- **OT.SCD/SVD_Gen**, which limits invoke the generation of the SCD and the SVD to authorised users only,
- **OT.Sigy_SigF**, which requires the TOE to provide the signature generation function for the legitimate signatory only and to protect the SCD against the use of others.

OE.SSCD_Prov_Service ensures that the signatory obtains a TOE sample as an authentic, initialised and personalised SSCD from an SSCD provisioning service.

P.Sig_Non-Repud (*Non-repudiation of signatures***)** deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensure the aspects of signatory's sole control over and responsibility for the digital signatures generated with the TOE. **OE.SSCD_Prov_Service** ensures that the signatory uses an authentic TOE, initialised and personalised for the signator*y*. **OE.CGA_QCert** ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. **OE.SVD_Auth** and **OE.CGA_QCert** require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. **OT.SCD_SVD_Corresp** ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. **OT.SCD_Unique** provides that the signatory's SCD can practically occur just once.

OE.SCD/SVD_Auth_Gen, **OE.SCD_Secrecy** and **OE.SCD_Unique** ensure the security of the SCD in the CSP environment. **OE.SCD_Secrecy** ensures the confidentiality of the SCD during generation, during and after export to the TOE. The CSP does not use the SCD for creation of any signature and deletes the SCD irreversibly after export to the TOE. **OE.SCD_Unique** provides that the signatory's SCD can practically occur just once. **OE.SCD_SVD_Corresp** ensures that the SVD in the certificate of the signatory corresponds to the SCD that is implemented in the copy of the TOE of the signatory. **OE.CGA_QCert** ensures that the certificate allows to identify the signatory and thus to link the SVD of the signatory. **OE.SVD_Auth** and **OE.CGA_QCert** require the environment to ensure the authenticity of the SVD as being exported by the TOE under sole control of the signatory. **OE.CGA_QCert** ensures that the certificate allows to identify the signatory and thus to link the SVD of the signatory. **OE.SVD_Auth** and **OE.CGA_QCert** require the environment to ensure the authenticity of the SVD as being exported by the TOE under sole control of the signatory.

OE.Signatory ensures that the Signatory checks that the SCD, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the Signatory takes sole control over the SSCD). **OT.Sigy_SigF** provides that only the signatory may use the TOE for signature creation. As prerequisite **OE.Signatory** ensures that the Signatory keeps his or her VAD confidential. **OE.DTBS_Intend**, **OE.DTBS_Protect** and **OT.DTBS_Integrity_TOE** ensure that the TOE generates digital signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by **OT.Sig_Secure** ensure that only this SCD may generate a valid digital signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE **OT.Lifecycle_Security** (*Lifecycle security*), **OT.SCD_Secrecy** (*Secrecy of the signature-creation data*), **OT.EMSEC_Design** (*Provide physical emanations security*), **OT.Tamper_ID** (*Tamper detection*) and **OT.Tamper_Resistance** (*Tamper resistance*) protect the SCD against any compromise.

5.3.4.2 Threats and Security Objective Sufficiency

T.SCD_Divulg (*Storing, copying, and releasing of the signature-creation data***)** addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in recital (18) of **The European Directive**. This threat is countered by

- **OE.SCD_Secrecy**, which assures the secrecy of the SCD in the CSP environment, and
- **OT.SCD_Secrecy**, which assures the secrecy of the SCD during use by the TOE for signature creation.

Furthermore, generation and/or import of SCD known by an attacker is countered by **OE.SCD/SVD_Auth_Gen**, which ensures that only authorized SCD generation in the environment is possible, and **OT.SCD_Auth_Imp**, which ensures that only authorised SCD import is possible.

T.SCD_Derive (*Derive the signature-creation data***)** deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. **OT.SCD/SVD_Gen** counters this threat by implementing cryptographic secure generation (as well as **OE.SCD_Unique**)of the SCD/SVD-pair. **OT.Sig_Secure** ensures cryptographic secure digital signatures.

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. OT.EMSEC_Design** counters physical attacks through the TOE interfaces and observation of TOE emanations. **OT.Tamper_ID** and **OT.Tamper_Resistance** counter the threat **T.Hack_Phys** by detecting and by resisting tampering attacks.

T.SVD_Forgery (*Forgery of the signature-verification data***)** deals with the forgery of the SVD exported by the TOE to the CGA to generation a certificate. T.SVD_Forgery is addressed by **OE.SCD_SVD_Corresp** or **OT.SCD_SVD_Corresp** (depending if SCD/SVD generation occurs in the SSCD Type 1 or in the TOE), which ensure correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and **OE.SVD_Auth** that ensures the integrity of the SVD exported by the TOE to the CGA. **T.SVD_Forgery** is also addressed by **OE.SVD_Auth,** which ensures the authenticity of the SVD given to the CGA of the CSP.

T.SigF_Misuse (*Misuse of the signature-creation function of the TOE*) addresses the threat of misuse of the TOE signature-creation function to create SDO by others than the signatory to create a digital signature on data for which the signatory has not expressed the intent to sign,. **OT.Lifecycle_Security** (*Lifecycle security*) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. **OT.Sigy_SigF** (*Signature creation function for the legitimate signatory only*) ensures that the TOE provides the signature-generation function for the legitimate signatory only. **OE.DTBS_Intend** (*Data intended to be signed*) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and **OE.DTBS_Protect** counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. **OT.DTBS_Integrity_TOE** (*DTBS/R integrity inside the TOE*) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, **OE.HID_VAD** (*Protection of the VAD*) provides confidentiality and integrity of the VAD as needed by the authentication method employed. **OE.Signatory** ensures that the Signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the Signatory has control over the SSCD. **OE.Signatory** ensures also that the Signatory keeps his or her VAD confidential.

T.DTBS_Forgery (*Forgery of the DTBS/R***)** addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of **OE.DTBS_Intend**, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of **OE.DTBS_Protect**, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of **OT.DTBS_Integrity_TOE** by ensuring the integrity of the DTBS/R inside the TOE.

T.Sig_Forgery (*Forgery of the digital signature***)** deals with non-detectable forgery of the digital signature. **OT.Sig_Secure**, **OT.SCD_Unique** and **OE.CGA_Qcert** address this threat in general. The **OT.Sig_Secure** (*Cryptographic security of the digital signature*) ensures by means of robust cryptographic techniques that the signed data and the digital signature are securely linked together. **OT.SCD_Unique** ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in

another certificate by chance. **OE.CGA_Qcert** prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision on a forged signature. **OE.SCD_Unique** ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

5.3.4.3 Assumptions and Security Objective Sufficiency

A.SCA (*Trustworthy signature-creation application***)** establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by **OE.DTBS_Intend** *(Data intended to be signed*) which ensures that the SCA generates the DTBS/R for 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** (*Authenticity of the SVD*), which ensures the protection of the integrity and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

A.CSP (Secure SCD/SVD management by CSP) establishes several security aspects concerning handling of SCD and SVD by the CSP. That the SCD/SVD generation device can only be used by authorized users is addressed by **OE.SCD/SVD_Auth_Gen** (Authorized SCD/SVD Generation), that the generated SCD is unique and cannot be derived by the SVD is addressed by **OE.SCD_Unique** (Uniqueness of the signature creation data), that SCD and SVD correspond to each other is addressed by **OE.SCD_SVD_Corresp** (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are deleted in the environment once exported to the TOE is addressed by **OE.SCD_Secrecy** (SCD Secrecy).

6. Extended Components Definition

This ST contains the following extended component defined as extension to CC part 2 in the claimed PPs [4] & [5]:

- SFR FPT_EMS.1 'TOE emanation' (denoted as FPT_EMSEC in PP[4])

6.1 TOE Emanation (FPT_EMS.1)

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

FPT_EMS TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMS TOE emanation	1

FPT_EMS.1 TOE Emanation has two constituents:

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions identified that shall be auditable if FAU_GEN Security audit data generation is included in a PP or ST using FPT_EMS.1.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 **The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].**

FPT_EMS.1.2 **The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to**

gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

7. Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE.
Security functional requirements components given in section 7.1, except FPT_EMS.1 which is explicitly stated, are drawn from Common Criteria part 2 v3.1.

Some security functional requirements represent extensions to [2]. Operations for assignment, selection and refinement have been made and are designated by an underline, in addition, where operations that were uncompleted in the PPs (performed in this ST) are also identified by *italic underlined* type.

The TOE security assurance requirements statement given in section is drawn from the security assurance components from Common Criteria part 3 [3].

7.1 TOE Security Functional Requirements

7.1.1 Cryptographic support (FCS)

7.1.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1	The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm *RSA* and specified cryptographic key sizes *between 1024 bit and 2048 bit* that meet the following: : *PKCS#1 v1.5 as per Algorithms and parameters for algorithms [13]*.

7.1.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1	The TSF shall destroy cryptographic in accordance with a specified cryptographic key destruction method: *overwriting old key with new key* that meets the following: *none*.

7.1.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1	The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *1024 bit, 1536 bit and 2048 bit* that meet the following: *RSA CRT with hashing SHA-1 or SHA-256 and with padding PKCS#1 v1.5 as per Algorithms and parameters for algorithms [13]*.
FCS_COP.1.1/ ENC	The TSF shall perform *data encryption/decryption for Administrator and Signatory authentication and Secure Messaging* in accordance with a specified cryptographic algorithm *TDES CBC* and cryptographic key sizes *16 bytes* that meet the following: *FIPS PUB 46-3 Data Encryption Standard (DES) [20]*.
FCS_COP.1.1/ MAC	The TSF shall perform *Message Authentication Code for Secure Messaging* in accordance with a specified cryptographic

algorithm *TDES MAC* and cryptographic key sizes *16 bytes* that meet the following: *FIPS PUB 46-3 Data Encryption Standard (DES) [20]*.

7.1.2 User Data Protection (FDP)

The security attributes for the user, TOE components and related status are defined in Table 6

Table 6. Security Attributes for Access control

Subject / Object	Attribute	Status
General Attribute		
S.User	Role	Administrator, Signatory
Initialisation Attribute		
S.User	SCD / SVD management	Authorized, Not Authorized
SCD	Secure SCD import allowed	No, Yes
SCD	SCD Identifier	Arbitrary Value (2 bytes)
Signature-Creation Attribute Group		
SCD	SCD operational	No, Yes
DTBS, DTBS/R	sent by an authorized SCA	No, Yes

The verification of the Security attributes for Access control is covered by SF.Access Control.

7.1.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1/ SVD_Transfer	The TSF shall enforce the SVD Transfer SFP on **(1) subjects: S.User,** **(2) objects: SVD** (3) operations: export

Application note:

FDP_ACC.1/SVD Transfer SFP is only required to protect the exportation of the SVD as the SVD is never imported from an SSCD type 1 into the TOE.

FDP_ACC.1.1/ SCD_Import	The TSF shall enforce the SCD Import SFP on (1). subjects: S.User, (2) objects: DTBS/R, SCD, (3) operations: import of SCD
FDP_ACC.1.1/ SCD/SVD_Generation	**The TSF shall enforce the SCD/SVD_Generation SFP on** **(1) subjects: S.User,**

	(2) objects: SCD, SVD, **(3) operations: generation of SCD/SVD pair**
FDP_ACC.1.1/ Signature-creation	The TSF shall enforce the Signature-creation SFP on (1) subjects: S.User, (2) objects: DTBS/R, SCD, (3) operations: signature creation.

7.1.2.2 Security attribute based access control (FDP_ACF.1)

SVD Generation SFP

FDP_ACF.1.1/ SCD/SVD_Generation	The TSF shall enforce the SCD/SVD_Generation SFP to objects based on the following: S.User is associated with the security attribute “SCD / SVD Management “.
FDP_ACF.1.2/ SCD/SVD_Generation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute “SCD / SVD Management” set to “authorised” is allowed to generate SCD/SVD pair.
FDP_ACF.1.3/ SCD/SVD_Generation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ SCD/SVD_Generation	The TSF shall explicitly deny access of subjects to objects based on the rule: S.User with the security attribute “SCD / SVD management” set to “not authorised” is not allowed to generate SCD/SVD pair.

SVD Transfer SFP

FDP_ACF.1.1/ SVD_Transfer	The TSF shall enforce the SVD Transfer SFP to objects based on the following: 1) the S.User is associated with the security attribute Role, 2) the SVD.
FDP_ACF.1.2/ SVD_Transfer	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute “role” set to “Administrator” or to “Signatory” is allowed to export SVD.
FDP_ACF.1.3/ SVD_Transfer	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ SVD_Transfer	The TSF shall explicitly deny access of subjects to objects based on the rule: none.

SCD Import SFP

FDP_ACF.1.1/ SCD_Import	The TSF shall enforce the SCD Import SFP to objects based on the following: the S.User is associated with the security attribute “SCD/SVD Management.”
FDP_ACF.1.2/ SCD_Import	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute “SCD/SVD Management” set to “authorised” is allowed to import SCD.
FDP_ACF.1.3/ SCD_Import	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ SCD_Import	The TSF shall explicitly deny access of subjects to objects based on the rule: S.User with the security attribute “SCD/SVD management” set to “not authorised” is not allowed to import SCD.

Signature-creation SFP

FDP_ACF.1.1/ Signature-Creation	The TSF shall enforce the Signature-creation SFP to objects based on the following: (1) the S.User is associated with the security attribute “Role” and (2) the SCD with the security attribute “SCD Operational”
FDP_ACF.1.2/ Signature-Creation	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 digital signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “yes”
FDP_ACF.1.3/ Signature-Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/ Signature-Creation	The TSF shall explicitly deny access of subjects to objects based on the rules: S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “no”.

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

FDP_ITC.1.1/ SCD	The TSF shall enforce the SCD Import SFP when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2/ SCD	The TSF shall ignore any security attributes associated with the **SCD** when imported from outside the TOE.
FDP_ITC.1.3/ SCD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: SCD shall be sent by an authorized SCD/SVD generation application from outside of the TOE.

7.1.2.4 Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1.1/ SCD	The TSF shall enforce the SCD Import SFP to be able to receive SCD in a manner protected from unauthorised disclosure.

7.1.2.5 Subset residual information protection (FDP_RIP.1)

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

7.1.2.6 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" (integrity redundancy code):

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 on all objects, based on the following attributes: *integrity checked persistent data*.
FDP_SDI.2.2/ Persistent	Upon detection of a data integrity error, the TSF shall 1. prohibit the use of the altered data, 2. inform the Signatory about integrity error.

The DTBS/R 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 on all objects, based on the following attributes: *integrity checked stored data*.
FDP_SDI.2.2/ DTBS	Upon detection of a data integrity error, the TSF shall 1. prohibit the use of the altered data

2. inform the Signatory about integrity error.

7.1.3 Identification and Authentication (FIA)

7.1.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1	The TSF shall detect when *5 consecutive* unsuccessful authentication attempts occur related to: *RAD authentication and PUK authentication.*
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall block RAD.

7.1.3.2 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow

1. Self test according to FPT_TST.1
2. Identification of the user by means of TSF required by FIA_UID.1.
3. Establishing a trusted path between the TOE and a SSCD of Type 1 by means of TSF required by FTP_ITC.1/SCD.

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

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

Application note:

The user mentioned in component FIA_UAU.1.1 is the local user using the trusted path provided between the SGA in the TOE environment and the TOE.

7.1.3.3 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow

1. Self test according to FPT_TST.1
2. Establishing a trusted channel between the TOE and a SSCD of Type 1 by means of TSF required by FTP_ITC.1/SCD.

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.

7.1.4 Security Management

7.1.4.1 Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1/ Sign	The TSF shall restrict the ability to enable the functions signature-creation function to Signatory.

7.1.4.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/ Admin	The TSF shall enforce the SCD Import SFP and SCD/SVD generation SFP to restrict the ability to modify the security attributes SCD/SVD management and Secure SCD import allowed to

Administrator.

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

7.1.4.3 Secure security attributes (FMT_MSA.2)

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

7.1.4.4 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 — The TSF shall enforce the SCD Import SFP, SCD/SVD_Generation SFP, SVD_Transfer SFP and Signature-creation SFPs to provide restrictive default values for security attributes that are used to enforce the SFP.

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

7.1.4.5 Static attribute value inheritance (FMT_MSA.4)

FMT_MSA.4.1 — The TSF shall use the following rules to set the value of security attributes:

i. If Administrator successfully generates an SCD/SVD pair without Signatory being authenticated the security attribute “SCD operational” of the SCD shall be set to “no” as a single operation.
ii. If Signatory successfully generates an SCD/SVD pair the security attribute “SCD operational” of the SCD shall be set to “yes” as a single operation.
iii. If Administrator imports SCD while Signatory is not currently authenticated, the security attribute “SCD operational” of the SCD shall be set to “no” after import of the SCD as a single operation
iv. If Administrator imports SCD while Signatory is currently authenticated, the security attribute “SCD operational” of the SCD shall be set to “yes” after import of the SCD as a single operation.

7.1.4.6 Management of TSF data (FMT_MTD.1)

FMT_MTD.1/Admin — The TSF shall restrict the ability to create the RAD to Administrator.

Application note:

The RAD can be unblocked by the Signatory after presentation of the PUK by the Signatory.

FMT_MTD.1/Signatory — The TSF shall restrict the ability to modify *or unblock* the RAD

to Signatory.

7.1.4.7 Security Management (FMT_SMF.1)

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

i. Creation and Modification of the RAD
ii. Enabling the signature creation function,
iii. Modification of the security attribute SCD/SVD management, SCD
iv. operational,
v. Change the default value of the security attribute SCD Identifier, Access Condition Management

7.1.4.8 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles Administrator and Signatory.

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

7.1.5 Protection of the TSF (FPT)

7.1.5.1 TOE Emanation (FPT_EMS.1)

FPT_EMS.1.1 The TOE shall not emit *information of IC Power consumption* in excess of *State of the Art values* enabling access to RAD and SCD.

FPT_EMS.1.2 The TSF shall ensure *any user* is unable to use the following interface *physical chip contacts and contactless I/O* to gain access to RAD and SCD.

Application note:

The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.
Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

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

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

i. *failure from self-test under FPT_TST*
ii. *IC Environmental sensors detection (Temperature out of range, Supply Voltage of chip),*
iii. *IC Internal error detection sensors failure (Parity, RNG*

operation)

7.1.5.3 Passive detection of physical attack (FPT_PHP.1)

FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

7.1.5.4 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1	The TSF shall resist *Environment attacks (clock frequency and voltage tampering) and Intrusive attacks (penetration of the module protective layers)* to the *IC Hardware* by responding automatically such that the SFRs are always enforced.

7.1.5.5 TSF testing (FPT_TST.1)

FPT_TST.1.1	The TSF shall run a suite of self-tests *during initial start-up or before running a secure operation* to demonstrate the correct operation of the TSF. Application-note: Crypto Self-tests are performed by the Operating System during start-up.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of *TSF (stored executable code).*

7.1.6 Trusted Path/Channels (FTP)

7.1.6.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SCD	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/ SCD	The TSF shall permit *another trusted IT product* to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCD	The TSF shall initiate communication via the trusted channel for *i.* *Data exchange integrity according to FDP_UCT.1/SCD,* *ii.* *SCD Import*

Refinement:

The mentioned remote trusted IT products are: an authorized SCD/SVD generation application for SCD import, the CGA for the SVD export, and the SCA for DTBS Import.

Application note 19: The component FPT_ITC.1 requires the TSF to support a trusted channel established to another trusted IT product generating the SCD/SVD pair for import the SCD as described by FDP_UCT.1/SCD. The ST writer shall perform the missing operations in the element FTP_ITC.1.3/SCD. If the TSF does not enforce the use of trusted channel for other functions the operation in the element FTP_ITC.1.3/SCD is “none”.

7.2 TOE Security Assurance Requirements

TOE Security Assurance Requirements as stated in the claimed protection profiles BSI-CC-PP0059-2009-MA-01– Protection profiles for Secure Signature Creation Device — Part 2: Device with key generation [4] (section 9.2) and BSI-CC-PP0075-2012– Protection profiles for Secure Signature Creation Device — Part 3: Device with key import [5] (section 10.3)

ALC_DVS is augmented from 1 to 2, and AVA_VAN is augmented from 3 to 5, compared to the CC V3.1 package for EAL4.

7.2.1 SARs Measures

Table 7. Assurance Requirements: EAL4 augmented

Assurance Class	Component	Description
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Lifecycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem of Tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	**Sufficiency of security measures**
	ALC_LCD.1	Developer defined lifecycle model
	ALC_TAT.1	Well defined development tools
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Test	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: security enforcing modules
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	**AVA_VAN.5**	**Advanced methodical vulnerability analysis**

7.2.2 SARs Rationale

The EAL4+ was chosen to permit the developer to gain maximum assurance from positive security engineering based on good commercial development practices. EAL4 is the level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

Augmentation results from the selection of:

1. **ALC_DVS.2** Life-cycle support- Sufficiency of security measures
   The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing especially for the secure handling of the MRTD's material.
   The component ALC_DVS.2 has no dependencies.

2. **AVA_VAN.5** Vulnerability Assessment - Advanced methodical vulnerability analysis
   The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the TOE security objectives.

   The component AVA_VAN.5 has the following dependencies:
   a. ADV_ARC.1 Security architecture description
   b. ADV_FSP.4 Complete functional specification
   c. ADV_TDS.3 Basic modular design
   d. ADV_IMP.1 Implementation representation
   e. AGD_OPE.1 Operational user guidance
   f. AGD_PRE.1 Preparative procedures
   g. ATE_DPT.1 Testing: basic design

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

7.3 Security Requirements Rationale

7.3.1 Security Requirement Coverage

The following table indicates the association of the security requirements and the security objectives of the TOE. Some requirements correspond to the security objectives of the TOE in combination with other objectives.

TOE SFRs / TOE Security objectives	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Auth_Imp
FCS_CKM.1	X		X	X	X							
FCS_CKM.4	X				X							
FCS_COP.1	X					X						
FCS_COP.1/ENC	X											
FCS_COP.1/MAC	X											
FDP_ACC.1/ SCD/SVD_Generation	X	X										

TOE SFRs / TOE Security objectives	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Auth_Imp
FDP_ACC.1/ SVD_Transfer	X											
FDP_ACC.1/SCD_Import	X											X
FDP_ACC.1/Signature_Creation	X						X					
FDP_ACF.1/ SCD/SVD_Generation	X	X										
FDP_ACF.1/ SVD_Transfer	X											
FDP_ACF.1/SCD_Import	X	X										
FDP_ACF.1/Signature_Creation	X						X					
FDP_ITC.1/SCD	X											
FDP_UCT.1/SCD	X				X							
FDP_RIP.1					X		X					
FDP_SDI.2/Persistent				X	X	X						
FDP_SDI.2/DTBS							X	X				
FIA_AFL.1							X					
FIA_UAU.1		X					X					X
FIA_UID.1		X					X					X
FMT_MOF.1	X						X					
FMT_MSA.1/Admin	X	X										
FMT_MSA.1/Signatory	X						X					
FMT_MSA.2	X	X					X					
FMT_MSA.3	X	X					X					
FMT_MSA.4	X	X					X					
FMT_MTD.1/Admin	X						X					
FMT_MTD.1/Signatory	X						X					
FMT_SMR.1	X						X					
FMT_SMF.1	X						X					
FPT_EMS.1					X				X			
FPT_FLS.1					X							
FPT_PHP.1										X		
FPT_PHP.3					X						X	
FPT_TST.1	X				X	X						
FTP_ITC.1/SCD	X				X							

Table 2 – Functional Requirement to TOE Security Objective Mapping

7.3.2 Security Requirements Sufficiency

OT.Lifecycle_Security (Lifecycle security) is provided by the SFR as follows. The SCD import is controlled by TSF according to FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import and FDP_ITC.1/SCD. The confidentiality of the SCD is protected during import according to FDP_UCT.1/SCD in the trusted channel FTP_ITC.1/SCD.

For SCD/SVD generation FCS_CKM.1, SCD usage FCS_COP.1 and SCD destruction FCS_CKM.4 ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation SFP and FDP_ACF.1/SCD/SVD_Generation SFP. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer SFP and FDP_ACF.1/SVD_Transfer SFP.
The secure SCD usage is ensured cryptographically according to FCS_COP.1. The SCD usage is controlled by access control FDP_ACC.1/Signature_Creation_FSP, FDP_ACF.1/Signature_Creation_FSP which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory. The FMT_SMF.1 and FMT_SMR.1 defines security management rules and functions. The test functions FPT_TST.1 provides failure detection throughout the lifecycle. The SFR FCS_CKM.4 ensures a secure SCD destruction. Confidentiality is preserved with FCS_COP.1/ENC and integrity with FCS_COP.1/MAC.

OT.SCD_Auth_Imp (Authorized SCD import) is provided by the security functions specified by the following SFR. FIA_UID.1 and FIA_UAU.1 ensure that the user is identified and authenticated before SCD can be imported. FDP_ACC.1/SCD_Import and **OT.SCD/SVD_Gen** (*SCD/SVD generation*) addresses that generation of a SCD/SVD pair requires proper user authentication. 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 SFRFDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute initialisation. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute “SCD operational” of the SCD.

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

OT.SCD_SVD_Corresp (*Correspondence between SVD and SCD*) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT_SMF.1 and by FMT_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

OT.SCD_Secrecy (Secrecy of signature creation data) is provided by the security functions specified by the following SFR. FDP_UCT.1/SCD and FTP_ITC.1/SCD ensures the confidentiality for SCD import. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.
FCS_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).
The SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1, which ensure the cryptographic robustness of the signature algorithms. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensures self-tests ensuring correct signature creation.

OT.Sigy_SigF (Signature creation function for the legitimate signatory only) is provided by SFR for identification authentication and access control.
The FIA_UAU.1 and FIA_UID.1 that ensure that no signature creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. The SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS.
FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature-creation process).”
FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.
The security functions specified by FDP_ACC.1/Signature_Creation and FDP_ACF.1/Signature_Creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. FMT_MOF.1 ensures that only the signatory can enable/disable the signature creation function. The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory.
Furthermore, the security functionality specified by FDP_RIP.1 will ensure that no attacker can get hold of the SCD (to create signatures outside the TOE) once SCD have been deleted by the legitimate signatory.

OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensures that the DTBS/R is not altered by the TOE. The verification that the DTBS/R has not been altered by the TOE is provided by integrity functions specified by FDP_SDI.2/DTBS.

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

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

OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to resist physical attacks.

8. TOE Summary Specification

8.1 SF.Access Control

This function checks that for each operation initiated by a user, the security attributes for user authorization (FMT_SMR.1) and data communication required are satisfied.

8.2 SF.Administration

This TSF manages the identification and authentication enforcing role separation (FMT_SMR.1) between the Signatory and the Administrator and Access to the Management Functions FMT_SMF.1

8.3 SF.Signatory Authentication

This TSF manages the identification and authentication of the Signatory and enforces role separation (FMT_SMR.1) between the Signatory and the Administrator.

8.4 SF.Signature Creation

This TSF is responsible for signing DTBS data using the SCD by the Signatory, following successful authentication of the Signatory.

The SF generates digital signatures using RSA 1024 to 2048 bit (FMT_MSA.2, FCS_COP.1) and SHA-1, SHA-256 hashing calculated by the host. The signature is calculated based on PKCS#1 version 1.5 [14].

8.5 SF.Secure Messaging

This function is responsible for confidentiality and data authentication. Confidentiality is ensured through the encryption of communication data by symmetric cryptography by the use 3DES operations (FCS_COP.1/ENC). Data authentication and integrity is achieved by calculating of a cryptographic checksum (MAC) (FCS_COP.1/MAC).

8.6 SF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation and operations on data such as encrypt and sign.

This TSF enforces protection of Key material during cryptographic functions processing and Key Generation, against state-of-the-art attacks, including IC power consumption analysis (FPT_EMS.1)

8.7 SF.Protection

This Security Function is responsible for protection of the TSF data, user data, and TSF functionality. The SF.Protection function is composed of is composed of software implementations of test and security functions including self-tests, secure deallocation, card content loading and installation and patching services.

9. Conventions & Terminology

9.1 Legislative References

This European standard reflects the requirement of a European directive in the technical terms of a protection profile. The following terms are used in the text to reference the directive:

9.1.1 The Directive

Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on "*a Community framework for electronic signatures*" [12],

9.1.2 Annex

One of the annexes, Annex I, Annex II or Annex III of **The Directive**

9.2 Symbols & Abbreviated Terms

Table 8. Symbols & Abbreviations

Term	Definition
Administrator	User who performs TOE initialization, TOE personalization, or other TOE administrative functions
ADF	Application Dedicated File
aka	Also Known As
CC	Common Criteria
CGA	Certification generation application (CGA) means a collection of application elements which requests the SVD from the SSCD for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair by the SSCD, if the requested SVD has not been generated by the SSCD yet. The CGA verifies the authenticity of the SVD by means of the SSCD proof of correspondence between SCD and SVD and checking the sender and integrity of the received SVD.
CSP	Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (defined in the Directive, article 2.11).
CVM	Cardholder Verification Method
DI	Dual Interface
Directive	The Directive; DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures
DTBS	Data to be signed (DTBS) means the complete electronic data to be signed (including both user message and signature attributes)
DTBS/R	Data to be signed representation (DTBS/R) means the representation data sent by the SCA to the TOE for signing and is

Term	Definition
	- a hash-value of the DTBS or - an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or - the DTBS The SCA indicates to the TOE the case of DTBS/R, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.
EEPROM	Electrically Erasable Programmable Non Volatile Memory
MAC	Message Authentication Code
MF	Master File (aka Root File)
Retail MAC	Commonly used DES based MAC, aka ISO 9797-1 mode 3 with DES
NVM	Non Volatile Memory
PUK	PIN Unlock Key
ROM	Read Only Memory
OS	Operating System
Qualified Certificate	Means a certificate which meets the requirements laid down in Annex I of the Directive and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive. (defined in the Directive, article 2.10)
RAD	Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.
RNG	Random Number Generator
HRNG	Hardware Random Number Generator
DRBG	Deterministic Random Bit Generator
SCA	Signature-creation application (SCA) means the application used to create an electronic signature, excluding the SSCD. i.e., the SCA is a collection of application elements. - to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision, - to send a DTBS/R to the TOE, if the signatory indicates by specific non mis-interpretable input or action the intend to sign, - to attach the qualified electronic signature generated by the TOE to the data or provides the qualified electronic signature as separate data.
SCD	Signature-creation data (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. (defined in the Directive, article 2.4)

Term	Definition
SDO	Signed data object (SDO) means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.
Signatory	Signatory means a person who holds a SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. (defined in the Directive, article 2.3)
SSCD	Secure signature-creation device (SSCD) means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive. (SSCD is defined in the Directive, article 2.5 and 2.6)
SSCD-Provisioning Service	Service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD
SVD	Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (defined in the Directive, article 2.7)
VAD	Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics.

10. References

Certification References	
[1]	Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-001 - Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012.
[2]	Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-002 -Part 2: Security functional requirements, Version 3.1, Revision 4, September 2012.
[3]	Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-003 -Part 3: Security assurance requirements, Version 3.1, Revision 4, September 2012.
[4]	BSI-CC-PP0059-2009-MA-01– Protection profiles for Secure Signature Creation Device — Part 2: Device with key generation – Version: 2.01, 01/2012 (prEN 14169-2:2012)
[5]	BSI-CC-PP0075-2012– Protection profiles for Secure Signature Creation Device — Part 3: Device with key import - Version: 1.0.2, 07/2012 (prEN 14169-3:2012)
[6]	BSI-PP-0035-2007 – Security IC Platform Protection Profile – version 1.0 – EAL4+
[7]	CCDB-2007-09-001 – Composite product evaluation for Smart Cards and similar devices – Version: 1.0, revision 1, September 2007
IC Platform References	
[8]	ds2629xx_SmartMX2 P40 family P40C008-012-024-040-072 Secure Smart Card Controller
[9]	NSCIB-15-65655-CR – NXP Secure Smart Card Controller P40C008/012/024/040/072 VD/VE – NXP Semiconductors Germany GmbH. V1.
[10]	
[11]	NXP Secure Smart Card Controller P40C008/012/024/040/072 VD/VE Security Target Lite – Rev 1.3
Standards References	
[12]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures
[13]	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.
[14]	PKCS#1: RSA Cryptography Standard, Version 1.5

[15]	ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002
[16]	ISO/IEC 9796-2: Information technology — Security techniques — Signature Schemes giving message recovery — Part 2: Integer factorization based mechanisms, 2002
[17]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[18]	Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006.
[19]	FIPS PUB 180-2, FIPS Publication – Secure hash standard (+ Change Notice to include SHA-224), 2002, NIST
[20]	FIPS PUB 46-3, FIPS Publication – Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. Department of Commerce/NIST
[21]	IEEE 1363-2000 – IEEE Standard Specification for Public-Key Cryptography
[22]	ETSI Technical Specification 101 733, CMS Advanced Electronic Signatures (CAdES), v2.2.1, 2013-04
[23]	ETSI Technical Specification 101 903, XML Advanced Electronic Signatures (XAdES), v1.4.2, 2010-12
[24]	ETSI Technical Specification 102 778: PDF Advanced Electronic Signatures (PAdES), v1.1.2, 2009-12
Additional References	
[25]	CCDB-2012-04-004 - Security Architecture requirements (ADV_ARC) for smart cards and similar devices - Appendix 1
[26]	NSCIB-CC-15-65156 – Security Target-Lite Firmware Libraries V2.0 on P40C008/012/024/040/072 VD/VE
[27]	FIPS PUB 180-3: Secure Hash Standard, Federal Information Processing Standards Publication, October 2008, US Department of Commerce/National Institute of Standards and Technology

11. Legal information

11.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

11.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

11.3 Licenses

Purchase of NXP <xxx> components
<License statement text>

11.4 Patents

Notice is herewith given that the subject device uses one or more of the following patents and that each of these patents may have corresponding patents in other jurisdictions.

<Patent ID> — owned by <Company name>

11.5 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

<Name> — is a trademark of NXP Semiconductors N.V.

12. List of figures

Fig 1. SSCD Scope, Structural View 7
Fig 2. SSCD Product Life-Cycle 9

13. List of tables

Table 1. Security Target Identification....3
Table 2. TOE Identification 4
Table 3. TOE Guidance 14
Table 4. Users & Subjects 16
Table 5. Security Environment to Security Objectives Mapping 29
Table 6. Security Attributes for Access control 36
Table 7. Assurance Requirements: EAL4 augmented ..45
Table 8. Symbols & Abbreviations 51

14. Contents

1. Introduction 3
1.1 ST Identification 3
1.2 TOE Identification 4
1.3 Composite TOE 4
1.4 TOE Overview 6
2. Target of Evaluation 7
2.1 Secure Signature Creation Device (SSCD) 8
2.1.1 Additional Functions 8
2.1.1.1 User Authentication 8
2.1.1.2 User Management of Signing Key 8
2.1.1.3 Secure Communication 8
2.2 SSCD Product Lifecycle 9
2.2.1 Development Phase 10
2.2.1.1 S/W and H/W Design 10
2.2.1.2 SSCD Fabrication 10
2.2.1.3 SSCD Integration 10
2.2.1.4 SSCD Initialization 10
2.2.2 Operational Phase 10
2.2.2.1 SSCD Provisioning 11
2.2.2.2 SSCD Operational Use 12
2.2.3 Application Note: Scope of SSCD PP application 12
2.3 TOE Form Factor & Physical Interfaces 13
2.4 TOE Guidance 14
3. Conformance Claims 15
3.1 CC Conformance claims 15
3.2 PP Claim 15
4. Security Problem Definition 16
4.1 Assets 16
4.2 Subjects 16
4.3 Assumptions 16
4.4 Threats 17
4.4.1 Threat Agents 17
4.4.2 Threats to Security 17
4.5 Organizational Security Policy 19
5. Security Objectives 19
5.1 Security Objectives for the TOE 19
5.2 Security Objectives for the Operational Environment 21
5.3 Security Objectives Rationale 23
5.3.1 Security Objectives Coverage 23
5.3.2 Security Objectives Sufficiency 23
5.3.2.1 Policies and Security Objective Sufficiency 23
5.3.2.2 Threats and Security Objective Sufficiency 26
5.3.2.3 Assumptions and Security Objective Sufficiency 27
5.3.3 Security Objectives Coverage 29
5.3.4 Security Objectives Sufficiency 29
5.3.4.1 Policies and Security Objective Sufficiency 29
5.3.4.2 Threats and Security Objective Sufficiency 31
5.3.4.3 Assumptions and Security Objective Sufficiency 33
6. Extended Components Definition 34
6.1 TOE Emanation (FPT_EMS.1) 34
7. Security Requirements 35
7.1 TOE Security Functional Requirements 35
7.1.1 Cryptographic support (FCS) 35
7.1.1.1 Cryptographic key generation (FCS_CKM.1) 35
7.1.1.2 Cryptographic key destruction (FCS_CKM.4) 35
7.1.1.3 Cryptographic operation (FCS_COP.1) 35
7.1.2 User Data Protection (FDP) 36
7.1.2.1 Subset access control (FDP_ACC.1) 36
7.1.2.2 Security attribute based access control (FDP_ACF.1) 37
7.1.2.3 Import of user data without security attributes (FDP_ITC.1) 39
7.1.2.4 Basic data exchange confidentiality (FDP_UCT.1) 39
7.1.2.5 Subset residual information protection (FDP_RIP.1) 39
7.1.2.6 Stored data integrity monitoring and action (FDP_SDI.2) 39
7.1.3 Identification and Authentication (FIA) 40

Date of release: 18 Sep 2017

Document identifier: ST-JCOP_3_SECID_P40 SSCD-02

7.1.3.1 Authentication failure handling (FIA_AFL.1) 40
7.1.3.2 Timing of authentication (FIA_UAU.1) 40
7.1.3.3 Timing of identification (FIA_UID.1) 40
7.1.4 Security Management 40
7.1.4.1 Management of security functions behaviour (FMT_MOF.1) 40
7.1.4.2 Management of security attributes (FMT_MSA.1) 40
7.1.4.3 Secure security attributes (FMT_MSA.2) 41
7.1.4.4 Static attribute initialisation (FMT_MSA.3) 41
7.1.4.5 Static attribute value inheritance (FMT_MSA.4) 41
7.1.4.6 Management of TSF data (FMT_MTD.1) 41
7.1.4.7 Security Management (FMT_SMF.1) 42
7.1.4.8 Security roles (FMT_SMR.1) 42
7.1.5 Protection of the TSF (FPT) 42
7.1.5.1 TOE Emanation (FPT_EMS.1) 42
7.1.5.2 Failure with preservation of secure state (FPT_FLS.1) 42
7.1.5.3 Passive detection of physical attack (FPT_PHP.1) 43
7.1.5.4 Resistance to physical attack (FPT_PHP.3) 43
7.1.5.5 TSF testing (FPT_TST.1) 43
7.1.6 Trusted Path/Channels (FTP) 44
7.1.6.1 Inter-TSF trusted channel (FTP_ITC.1) 44
7.2 TOE Security Assurance Requirements 44
7.2.1 SARs Measures 45
7.2.2 SARs Rationale 45
7.3 Security Requirements Rationale 46
7.3.1 Security Requirement Coverage 46
7.3.2 Security Requirements Sufficiency 47
8. TOE Summary Specification 50
8.1 SF.Access Control 50
8.2 SF.Administration 50
8.3 SF.Signatory Authentication 50
8.4 SF.Signature Creation 50
8.5 SF.Secure Messaging 50
8.6 SF.Crypto 50
8.7 SF.Protection 50
9. Conventions & Terminology 51
9.1 Legislative References 51
9.1.1 The Directive 51
9.1.2 Annex 51
9.2 Symbols & Abbreviated Terms 51
10. References 54
11. Legal information 56
11.1 Definitions 56
11.2 Disclaimers 56
11.3 Licenses 56
11.4 Patents 56
11.5 Trademarks 56
12. List of figures 57
13. List of tables 58
14. Contents 59

[i] Self-certification of the SVD is effectively computing a digital signature with the corresponding SCD. A signing operation requires explicit sole signatory control, however this specific case, if supported, provides an exception to this rule as,before being delivered to the signatory, such control is evidently impossible.

Date of release: 18 Sep 2017

Document identifier: ST-JCOP_3_SECID_P40 SSCD-02