ChipDoc v2 on JCOP 3 P60 in SSCD configuration

Security Target Lite

Rev. 1.1 — 01 April 2020
Final

Evaluation documentation
PUBLIC

Document information

Info	Content
Keywords	Common Criteria, Security Target Lite, ChipDoc v2 on JCOP 3 P60. SSCD
Abstract	Security Target Lite of ChipDoc v2 application on JCOP 3 P60 in SSCD configuration, which is developed and provided by NXP Semiconductors, Business Unit Identification according to the Common Criteria for Information Technology Security Evaluation Version 3.1 at Evaluation Assurance Level 5 augmented.

Revision history

Rev	Date	Description
1.0	2020-03-27	Initial Version of this Security Target Lite
1.1	2020-04-01	Update of Reference to Guidance Document

Contact information

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

For sales office addresses, please send an email to: salesaddresses@nxp.com

1. ST Introduction (ASE_INT)

1.1 ST Reference and TOE Reference

Table 1. ST Reference and TOE Reference

Title	ChipDoc v2 on JCOP 3 P60 in SSCD configuration Security Target Lite
Version	Revision 1.1
Date	2020-04-01
Product Type	Java Card Applet
TOE Name	ChipDoc v2 on JCOP 3 P60 in SSCD configuration Version v7b4_2
CC Version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 4, September 2012 (Part 1 [1], Part 2 [2] and Part 3 [3])

1.2 TOE Overview

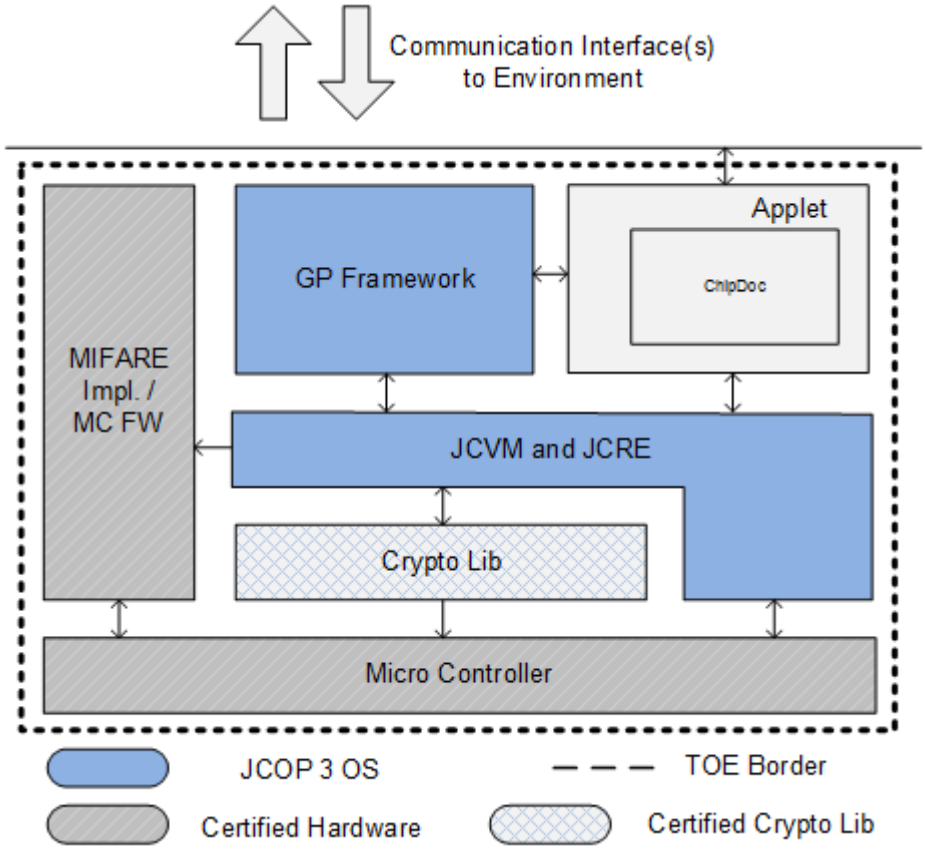


Fig 1. Components of the TOE

The TOE consists of an applet which is executed by a software stack that is stored on a Micro Controller. For a complete picture of the TOE see Fig 1, and for details with regards to the different components see section 1.3.1. The TOE is delivered in closed configuration, meaning that all other interfaces apart from the SSCD ones are locked and do not act as communication interfaces towards the environment.

The Protection Profiles [4] and [5] claimed by this Security Target assume a well-defined process signature-creation to take place. Note that [26], stating Part 1 of Protection Profiles for secure signature creation devices and being referenced by [4] and [5] has been superseded by [27]. The latter states that the functionality referred to as “Type 2” (specifying devices with key import) in the remainder of this ST, can be found in [5], while the functionality referred to as “Type 3” (specifying devices with key generation) in the remainder of this ST, can be found in [4]. The present chapter defines two possible SSCD implementations, referred to as ‘SSCD types’. SSCD Type 2 and Type 3, both parts of the TOE.

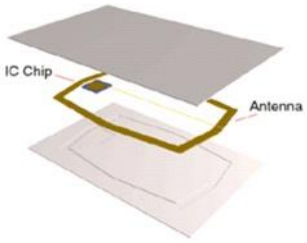
If the SSCD holds the SVD and exports the SVD to a CGA for certification, a trusted channel is to be provided. The CGA initiates SCD/SVD generation (“Init.”) and the SSCD exports the SVD for generation of the corresponding certificate (“SVD into cert.”).

The signatory must be authenticated to create signatures that he sends his authentication data (e.g., a PIN) to the SSCD Type 2 or Type 3 (e.g., a smart card). The data to be signed (DTBS) representation (i.e., the DTBS itself, a hash value of the DTBS, or a pre-hashed value of the DTBS) shall be transferred by the SCA to the SSCD only over a trusted channel. The same shall apply to the signed data object (SDO) returned from a SSCD to the SCA.

The TOE implements a trusted channel with regards to commands and responses that are exchanged between the TOE and any external device. Various data and processes such as DTBSs, signatures, public keys, identification and authentication data, SVD Transfer or other user data are embedded in command and response frames. Thus the TOE is capable of providing a secure communication channel between legitimate end points both of the TOE and the external device.

SSCD Type 2 and 3 components are personalized components: they can be used for signature creation by one specific user – the signatory - only.

The TOE is available in a variety of form factors where digital application software is masked in ROM:



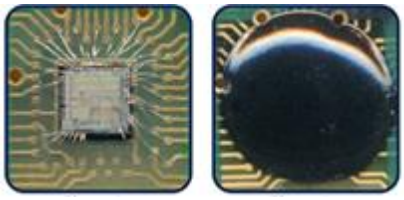
(antenna embedded in plastic)

Contactless interface cards and modules

(antenna embedded in plastic)

(contactless interface absent or disabled)

Dual interface cards and modules | Contact only cards and modules



SOIC8 package | QFN44 package | Chip on Board (PCB)

Fig 2. TOE Form Factor

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.
- The contactless type interface of the TOE smartcard is ISO/IEC 14443 compliant.
- The interfaces of the TOE SOIC-8 are ISO 9141 compliant.
- The interfaces of the TOE QNF-44 are JEDEC compliant.

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

The antenna and the packaging are both out of the scope of this TOE.

The TOE smartcard form factors may be applied to a contact type card reader/writer or to a contactless card reader/writer when the contactless interface of the smartcard is available. The card reader/writer is connected to a computer such as a personal computer and allows application programs (APs) to use the TOE.

1.3 TOE Description

1.3.1 TOE Components and Composite Certification

The certification of this TOE is a composite certification. This means that for the certification of this TOE other certifications of components which are part of this TOE are re-used. In the following sections more detailed descriptions of the components of Fig 1 are provided. In the description it is also made clear whether a component is covered by a previous certification or whether it is covered in the certification of this TOE.

1.3.1.1 Micro Controller

The Micro Controller is a secure smart card controller from NXP from the SmartMX2 family. The Micro Controller contains a co-processor for symmetric cipher, supporting DES operations and AES, as well as well as an accelerator for asymmetric algorithms. It contains volatile (RAM) and non-volatile (ROM and EEPROM) memory. The Micro Controller has been certified in a previous certification and the results are re-used for this certification.

The exact reference to the previous certification is given in the following table:

Table 2. Reference to certified Micro Controller

Name	NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software
Certification ID	BSI-DSZ-CC-1059
Reference	[21]

1.3.1.2 IC Dedicated Software

- **Micro Controller Firmware**: The Micro Controller Firmware is used for testing of the Micro Controller at production, for booting of the Micro Controller after power-up or after reset, for configuration of communication devices and for writing data to non-volatile memory. The MC FW has been certified in a previous certification. It has been certified together with the Micro Controller and the same references ([21]) as given for the Micro Controller also apply for the Micro Controller Firmware.
- **MIFARE Implementation:** The NXP Secure Smart Card Controller P6022y VB hardware of this TOE can be configured as follows:
  - P6022P VB: without MIFARE,
  - P6022M VB: including MIFARE Plus MF1PLUSx0,
  - P6022D VB: including MIFARE DESFire EV1,
  - P6022J VB: including both, MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1.

  The MIFARE Implementation has been certified in a previous certification. It has been certified together with the Micro Controller and the same references ([21]) as given for the Micro Controller also apply for the MIFARE Implementation. Only the P6022J VB configuration can be considered as certified hardware configuration for the TOE in the scope of this Security Target.

- **Crypto Library:** The Crypto Lib is certified in a previous certification and the results are re-used for this certification. The exact reference to the certification is given in the following table:

Table 3. Reference to certified Crypto Library

Name	Crypto Library V3.1.x on P6022y VB
Certification ID	NSCIB-CC-67206-CR4
Reference	[22]

- **JCOP3 OSB:** The Operating System consists of JCVM, JCRE, JCAPI and GP framework. It is implemented according to the Java Card Specification and GlobalPlatform and has been certified in the course of a previous certification, where the results are re-used for this certification. The exact reference to the certification is given in the following table:

Table 4. Reference to certified Operating System

Name	JCOP 3 P60
Certification ID	NSCIB-CC-98209-CR4
Reference	[24]

1.3.1.3 IC Embedded Software

- **ChipDoc v2[1] Applet:** The applet implements a Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC [11] 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

1.3.2 TOE lifecycle

The TOE lifecycle is shown in Fig 3.

The integration phase is added to the PP generic lifecycle as this particular TOE requires that card production phase is refined.

1. [1] Please note that in the remainder of the document, *ChipDoc v2* is referred to as *ChipDoc* for the sake of simplicity

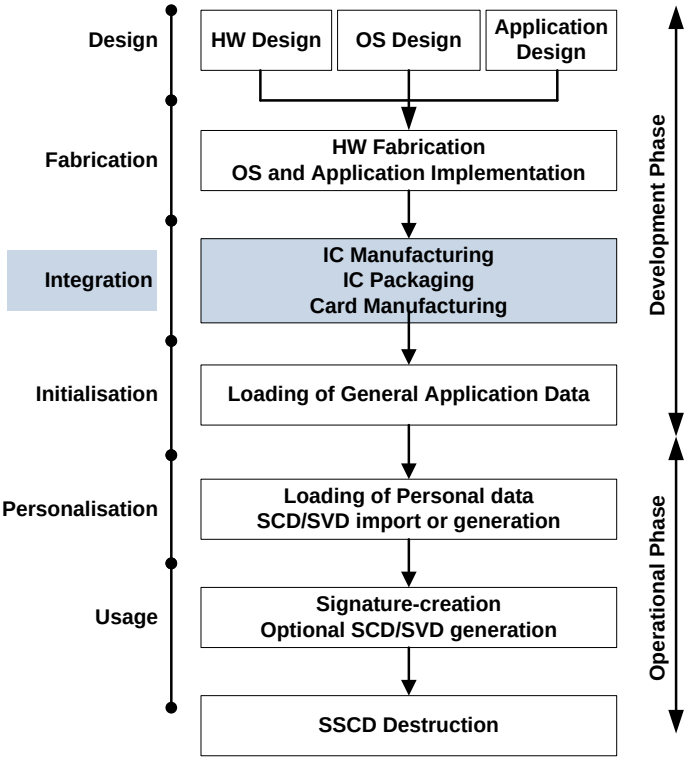


Fig 3. TOE lifecycle

1.3.2.1 Design Phase

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.

1.3.2.2 Fabrication Phase

The Operating System and applicative parts of the TOE are sent in a secure way for masking into ROM. In addition to the TOE, the mask contains confidential data, knowledge of which is required in order to initialize and personalize the chip. Java Card applets are included in the mask and the corresponding converted files (.cap or.jca) are also provided.

1.3.2.3 Integration Phase

This phase corresponds to the integration of the hardware and firmware components into the final product body. In the case of this TOE it will be a smart card, but it could also be a USB token. The TOE is protected during transfer between various parties with a diversified (per card) Transport Key.

1.3.2.4 Initialization Phase

The initialization phase consists in OS configuration, applet instantiation and/or applet and OS patching activities (in EEPROM)[2]. The TOE is protected during transfer by the confidential information which resides in the card during mask production (transport key). Creation of the application implies applet instantiation and the creation of MF and ChipDoc ADF[3]. It is not the case of this TOE, but additional applets could be loaded in the TOE at this point. Card Content Loading and Installing mechanism is terminated in this phase (the platform is closed). The product becomes operational and is delivered after this initialization phase.

1.3.2.5 Personalization Phase

After unlocking the product with the transport key, NXP or 3rd Party Personalization facility which includes the loading of Personal Application Data and optional generation of the SCD/SVD pair if loading does not include importing an SCD/SVD pair. The product is considered in use phase.

1.3.2.6 Operational Phase

This ST addresses the functions used in the operational phases but developed during development phase. 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). The product is considered in use phase.

1.3.2.7 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 [11].

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 [11], 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.

1.3.3 TOE Limits

The TOE is a secure signature-creation device (combination of SSCD type 2 and type 3) according to Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [11].The destruction of the SCD is mandatory before the TOE generate a new pair SCD/SVD or loads a new pair SCD/SVD.

[2] The application of platform patches is only allowed on a CC certified site. If the TOE issuer is able to provide such a facility NXP will supply all patching materials, otherwise the task is undertaken by NXP trust provisioning service, prior to dispatch from NXP.

[3] Besides the certified file system, one or more additional file systems might be present on the TOE.

A SSCD is a configured device used to implement the signature-creation data (SCD).

The TOE described in this ST is a product 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. NVM (Non Volatile Memory) corresponds to ROM memory for the NXP P6022y VB IC [21] [6].

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

1. to import signature creation data (SCD) and, optionally, the correspondent signature verification data (SVD),
2. to export the SVD for certification,
3. to generate the SCD and the correspondent signature-verification data (SVD)
4. to create qualified Electronic Signatures
    a. after allowing for the Data To Be Signed (DTBS) to be displayed correctly by the appropriate environment
    b. using appropriate hash functions that are, according to [5], agreed as suitable for qualified electronic signatures
    c. after appropriate authentication of the signatory by the TOE
    d. using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed as suitable according to [5].

The TOE is able to generate SCD/SVD key pair (Type 3), to export the SVD (Type 3) and import SCD (Type 2). Thus the TOE itself implements Type 2 and Type 3, where both SSCD Type 2 and Type 3 are parts of the TOE, co-existing besides each other, not being subject to configuration to the user.

The TOE implements all IT security functionality which are necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control. The TOE provides a trusted channel for user authentication by its own, where in addition IT measures are implemented to support a trusted path to a trusted human interface device.

This TOE does not implement, in addition to the functions of the SSCD, the signature-creation application (SCA). The SCA presents the data to be signed (DTBS) to the signatory and prepares the DTBS-representation the signatory wishes to sign for performing the cryptographic function of the signature. The SCA is considered as part of the environment of the TOE.

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

1. importation of the SCD or generation of SCD/SVD pair
2. personalization for the signatory by means of the signatory’s verification authentication data (VAD)

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP). The TOE will destroy the SCD if the SCD is no longer used for signature generation.

The TOE does not provide a Human Interface (HI) for user authentication itself, but IT measures implement a trusted human interface device connected via a trusted channel with the TOE. The human interface device is used for the input of VAD for authentication by knowledge. The TOE holds RAD to check the provided VAD. The human interface implies appropriate hardware. The second approach allows to reduce the TOE hardware to a minimum e. g. a smart card.

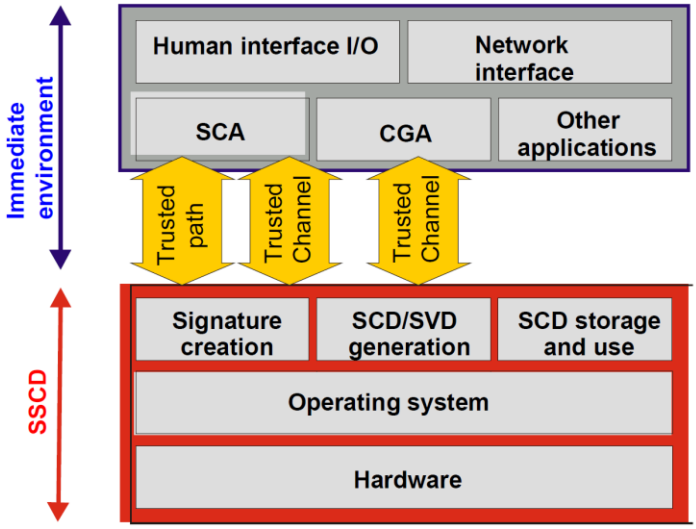


Fig 4. Scope of the SSCD, structural view

Fig 4 shows the PP scope from the 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.

1.3.4 TOE Identification

1.3.4.1 TOE Delivery

The delivery comprises the following items:

Table 5. Delivery Items

Type	Name	Version	Form of delivery
JCOP 3 P60 Platform including ChipDoc v2 application	NXP Secure Smart Card Controller P6022y VB ROM Code (Platform ID) Patch Code (Patch ID)		Micro Controller including on-chip software: Firmware, Crypto Library and JCOP 3 Operating System
Document	ChipDoc SSCD, Preparation and Operation Manual [25]	1.9	Electronic document

1.3.4.2 Identification of the TOE

The TOE can be identified by

- Identifying the JCOP 3 P60 platform: the IDENTIFY command shall be sent to the TOE to verify the correct values of the Platform ID and the Patch ID as stated in section “2.3 Product identification” of the User Manual for this TOE [25]
- Identifying the SSCD application: The ChipDoc v2 application can be verified according the instructions in section “2.2 Applet identification” in [25]

1.3.4.3 Evaluated Package Types

A number of package types are supported for this TOE. All package types, which are covered by the certification of the used platform (see [24]), are also allowed to be used in combination with each product of this TOE.

The package types do not influence the security functionality of the TOE. They only define which pads are connected in the package and for what purpose and in which environment the chip can be used. Note that the security of the TOE is not dependent on which pad is connected or not - the connections just define how the product can be used. If the TOE is delivered as wafer the customer can choose the connection on his own.

2. Conformance Claims (ASE_CCL)

2.1 CC Conformance Claim

This Security Target claims to be conformant to version 3.1 of Common Criteria for Information Technology Security Evaluation according to

- "Common Criteria for Information Technology Security Evaluation, Part 1, Version 3.1, Revision 4, September 2012" [1]
- "Common Criteria for Information Technology Security Evaluation, Part 2, Version 3.1, Revision 4, September 2012" [2]
- "Common Criteria for Information Technology Security Evaluation, Part 3, Version 3.1, Revision 4, September 2012" [3]

The following methodology will be used for the evaluation:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4" [23]

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in section 6.

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

- FPT_EMSEC.1 ‘TOE emanation’

2.2 Package Claim

This Security Target claims conformance to the assurance package EAL5 augmented. The augmentations to EAL5 are AVA_VAN.5 “Advanced methodical vulnerability analysis” and ALC_DVS.2 “Sufficiency of security measures”.

2.3 PP Claim

This ST claims strict compliance to the following Protection Profiles:

[4]	**Protection Profile for Secure Signature-Creation Device - Part 2**
Version	2.0.1.
Date	01/2012
Identification	prEN 14169-2:2012
Approved by	AFNOR
Registration	BSI-CC-PP-0059-2009-MA-01

[5]	**Protection Profile for Secure Signature-Creation Device - Part 3**
Version	1.0.2
Date	07/2012
Identification	prEN 14169-3:2012
Approved by	AFNOR
Registration	BSI-PP-0075

3. Security Problem Definition (ASE_SPD)

3.1 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-representation

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 quality of the function must be maintained so that it can participate to the legal validity of electronic signatures).

3.2 Subjects

This Security Target considers the following subjects:

Subjects	Definition
User	End user of the TOE who can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.
Admin	User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.
Signatory	User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

3.3 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 signature of the CSP.

A.SCA	*Trustworthy signature-creation application*

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

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.

3.4 Threats

3.4.1 Threat agents

Attacker	Human or process acting on their behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the electronic signature. The attacker has got a high attack potential and knows no secret.

3.4.2 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 release the SCD during generation, storage and use for signature-creation in the TOE.

T.SCD_Derive	*Derive the signature-creation data*

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

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

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

T.DTBS_Forgery	*Forgery of the DTBS-representation*

An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intended to sign.

T.SigF_Misuse	*Misuse of the signature-creation function of the TOE*

An attacker misuses the signature-creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

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.

3.5 Organizational Security Policies

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 the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alias the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.

P.QSign	*Qualified electronic signatures*

The signatory uses a signature-creation system to sign data with 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 maintain 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.

4. Security Objectives (ASE_OBJ)

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

4.1 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*

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

OT.Lifecycle_Security	*Lifecycle security*

The TOE shall detect flaws during the personalisation and operational usage. The TOE shall provide functionality to securely destroy the SCD.

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

The TOE provides security features to ensure that authorised users only 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.

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 a digital signature creation with the SCD.

OT.Tamper_ID	*Tamper detection*

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

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

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

OT.DTBS_Integrity_TOE	*Verification of the DTBS-representation integrity*

The TOE must not alter the DTBS/R This objective does not conflict with a signature-creation process where the TOE applies a cryptographic hash function on the DTBS/R to prepare for signature creation algorithm.

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

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

OT.Sig_Secure	*Cryptographic security of the electronic signature*

The TOE generates digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the digital signatures or any other data exported from the TOE. The digital 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 authorised users only may invoke the import of the SCD.

4.2 SOs for the Environment

Since ChipDoc SSCD is both SSCD type 2 and SSCD type 3 means that the TOE environment consists of a CGA, an SCA and a specific development environment.

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.SVD_Auth	*Authenticity of the SVD*

The operational environment ensures the authenticity of the SVD exported by the TOE to the CGA. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

OE.HID_VAD	*Protection of the VAD*

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

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

The SSCD Provisioning Service handles authentic devices that implement the TOE to be prepared for the legitimate user as signatory, personalises and delivers the *TOE* as SSCD to the signatory.

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

The Signatory uses trustworthy SCA that

- 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,
- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
- attaches the signature produced by the TOE to the data or provides it separately.

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_Corresp	*Correspondence between SVD and SCD*

The SCD/SVD generation device shall ensure the correspondence between the SVD and the SCD, and shall verify the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.

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

4.3 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.

4.3.1 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.

Table 6. 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.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

4.3.2 Security Objectives Sufficiency

4.3.2.1 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 the Annex II of **the directive [11]**. This is ensured as follows

- OT.SCD_Unique meets the paragraph 1(a) of the directive [11], Annex III, by the requirements that the SCD used for signature creation can practically occur only once.
- OT.SCD_Unique, OT.SCD_Secrecy and OE.SCD_Secrecy meet the paragraph 1(a) of **the directive** [11], Annex III, by the requirements to ensure the secrecy of the SCD. OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of SCD against specific attacks.
- OT.SCD_Secrecy and OT.Sig_Secure meet the paragraph 1(b) of **the directive** [11], 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 and OE.SCD_Secrecy meet the paragraph 1(c) of **the directive** [11], Annex III, by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others.
- - OT.DTBS_Integrity_TOE meets the requirements the paragraph 2 of **the directive** [11], Annex III,

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, personalization and operational usage
- OE.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only,
- 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.
- OT.Sigy_SigF, which requires the TOE to provide the signature creation 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 an authentic copy of the TOE, initialised and personalised as SSCD from the 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.

4.3.2.2 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 outside 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.

4.3.2.3 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. Extended Components Definition (ASE_ECD)

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

- SFR FPT_EMSEC.1 ‘TOE emanation’

5.1 TOE emanation (FPT_EMSEC.1)

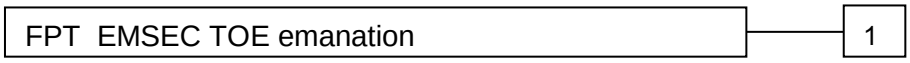
The additional family FPT_EMSEC (FPT_EMS in the PP) (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable 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_EMSEC 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_EMSEC TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMSEC.1 TOE Emanation has two constituents:

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

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

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_EMSEC.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6. Security Requirements (ASE_REQ)

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

Security functional requirements components given in section 6.1, except FPT_EMSEC.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 6.2 is drawn from the security assurance components from Common Criteria part 3 [3].

6.1 TOE Security Functional Requirements

6.1.1 Cryptographic support (FCS)

6.1.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate 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 v2.1 [28]*.

6.1.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys *in case of re-importation and regeneration of a new SCD* in accordance with a specified cryptographic key destruction method *overwriting old key with new key or random data* that meets the following: *none*.

Application note:

The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.

Re-importation is not supported by the TOE.

6.1.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1 *Cryptographic operation*

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

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 2048bit* that meet the following: *RSA CRT with hashing SHA-1 or SHA-256 and with padding PKCS#1 v2.1: EME-OAEP, EMSA-PSS [7]*
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 AES* and cryptographic key sizes *128, 192 and 256 bits* that meet the following: *FIPS PUB 46-3 Data Encryption Standard (DES) [18] and FIPS PUB 197[31]*
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 AES* and cryptographic key sizes *128, 192 and 256 bits* that meet the following: *ISO/IEC 9797-1: 2011 Information technology -- Security techniques – Message Authentication Codes (MACs) [20].*

6.1.2 User data protection (FDP)

6.1.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1/SVD_Transfer *Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

FDP_ACC.1/SCD_Import *Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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/SCD/SVD_Generation *Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.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/Signature_Creation *Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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.

6.1.2.2 Security attribute based access control (FDP_ACF.1)

The security attributes for the user, TOE components and related status are:

User, subject or object the attribute is associated with	Attribute	Status
General attribute		
User	Role	Administrator, Signatory
Initialization attribute		
User	SCD / SVD management	Authorized, not authorized
SCD	Secure SCD import allowed	No, yes
Signature-creation attribute group		
SCD	SCD operational	No, yes
DTBS, DTBS-representation	sent by an authorized SCA	No, yes

SVD Generation

FDP_ACF.1/SCD/SVD_Generation *Security attribute based access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1/ SCD/SVD_Generation	The TSF shall enforce the SCD/SVD_Generation_SFP to objects based on the following: the user 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

FDP_ACF.1/SVD_Transfer *Security attribute based access control*

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

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: *R.Admin and R.Sigy* are 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 following additional rules: none.

SCD Import

FDP_ACF.1/SCD_Import *Security attribute based access control*

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

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

FDP_ACF.1/Signature creation *Security attribute based access control*

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

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-representation 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”.

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

FDP_ITC.1/SCD Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

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 ~~user data~~ **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 authorised SSCD from outside the TOE.*

6.1.2.4 Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1/SCD Basic data exchange confidentiality

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1/ SCD	The TSF shall enforce the SCD Import SFP to be able to receive ~~user data~~ **SCD** in a manner protected from unauthorised disclosure.

6.1.2.5 Subset residual information protection (FDP_RIP.1)

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

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

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

1. SCD
2. *RAD*
3. *SVD (if persistent stored by TOE)*

FDP_SDI.2/Persistent *Stored data integrity monitoring and action*

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
Dependencies:	No dependencies.
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 S.Sigy about integrity error.

The DTBS-representation temporarily stored by TOE has the user data attribute "integrity checked stored data":

FDP_SDI.2/DTBS *Stored data integrity monitoring and action*

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

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 DTBS.

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 S.Sigy about integrity error.

6.1.3 Identification and authentication (FIA)

6.1.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when *10* unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD.

6.1.3.2 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 SCD/SVD generation component 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.

6.1.3.3 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 SCD/SVD generation component 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.

6.1.4 Security management (FMT)

6.1.4.1 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.

6.1.4.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1/Admin Management of security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1/ Admin	The TSF shall enforce the SCD/SVD_Generation_SFP and SCD Import SFP to restrict the ability to modify *and none* the security attributes SCD/SVD management to R.Admin.

FMT_MSA.1/Signatory *Management of security attributes*

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
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 R.Sigy.

6.1.4.3 Secure security attributes (FMT_MSA.2)

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

6.1.4.4 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_SFP 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.

6.1.4.5 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:

If S.Admin 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.

If S.Sigy successfully generates an SCD/SVD pair the security attribute “SCD operational of the SCD” shall be set to “yes” as a single operation.

If S.Admin imports SCD while S. 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

If S.Admin imports SCD while S. 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.

6.1.4.6 Management of TSF data (FMT_MTD.1)

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

Application note:

The RAD can be unblocked by the Signatory after presentation of the PUK by the Signatory. in case of a PIN. In case of a DES Key, the RAD cannot be unlocked.

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

6.1.4.7 Specifications of Management Functions (FMT_SMF.1)

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: (1) Creation and modification of RAD, (2) Enabling the signature creation function, (3) Modification of the security attribute SCD/SVD management, SCD operational, (4) *Change the default value of the security attribute SCD Identifier,* (5) *Access Condition Management to files (according to [25]).*

6.1.4.8 Security roles (FMT_SMR.1)

FMT_SMR.1.1	The TSF shall maintain the roles R.Admin and R.Sigy.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1	The TOE shall not emit *information of IC Power consumption* in excess of *non-useful information* enabling access to RAD and SCD.

FPT_EMSEC.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.

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

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

(1) self-test according to FPT_TST fails,
(2) *IC sensors failure detection (RNG failure, EEPROM failure, out of range temperature, clock and voltage of chip).*

6.1.5.3 Passive detection of physical attack (FPT_PHP.1)

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

6.1.5.4 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist *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.

6.1.5.5 TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up or before running a secure operation* to demonstrate the correct operation of the TSF.

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

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

6.1.6 Trusted k/channels (FTP)

6.1.6.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SCD	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/ SCD	The TSF shall permit *the remote trusted IT product* to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCD	The TSF or the trusted IT shall initiate communication via the trusted channel for Data exchange integrity according to FDP_UCT.1/SCD, *SCD Import, transfer of SVD,*

Refinement:

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

6.2 TOE Security Assurance Requirements

TOE Security Assurance Requirements as stated in section 9.2 and 10.3 of the claimed PPs [4] [5], respectively.

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 EAL5.

6.2.1 SARs Measures

The assurance measures that satisfy the TOE security assurance requirements are the following:

Table 7. Assurance Requirements: EAL5 augmented

Assurance Class	Component	Description
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete Semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semi-formal 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.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	**Sufficiency of security measures**
	ALC_LCD.1	Developer defined lifecycle model
	ALC_TAT.2	Compliance with implementation standards
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.3	Testing: modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	**AVA_VAN.5**	**Advanced methodical vulnerability analysis**

6.2.2 SARs Rationale

The EAL5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, although rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL5 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL5 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:

ALC_DVS.2 Life-cycle support- Sufficiency of security measures

The selection of the component ALC_DVS.2 provides a higher assurance with regards to the security measures providing the necessary level of protection to maintain the confidentiality and integrity of the TOE.

The component ALC_DVS.2 has no dependencies.

AVA_VAN.5 Vulnerability Assessment - Advanced methodical vulnerability analysis

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

The component AVA_VAN.5 has the following dependencies:

ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_TDS.3	Basic modular design
ADV_IMP.1	Implementation representation
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ATE_DPT.1	Testing: basic design

All of these are met or exceeded in the EAL5 assurance package.

6.3 Security Requirements Rationale

6.3.1 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.

Table 8. Functional Requirement to TOE Security Objective Mapping

TOE SFRs / TOE Security objectives	OT.Lifecycle_Security	OT.SCD/SVD_Auth_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										
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					

TOE SFRs / TOE Security objectives	OT.Lifecycle_Security	OT.SCD/SVD_Auth_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
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			x					
FPT_EMSEC.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							

6.3.2 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 and FDP_ACF.1/SCD/SVD_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer.

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, FDP_ACF.1/Signature_Creation 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.

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 FDP_ACF.1/SCD_Import ensure that only authorised users can import SCD.

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 SFR FDP_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 used 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_EMSEC.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. FCS_COP.1/ENC and FCS_COP.1/MAC

strengthen Secure Messaging protocol with regards to integrity and confidentiality of data exported from the TOE. Thus OT.Sig_Secure is supported with regards to withstand attacks trying to forge signature data. 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_EMSEC.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.

7. TOE summary specification (ASE_TSS)

This set of TSFs manages the identification and/or authentication of the external user and enforces role separation.

7.1 SF.Access Control

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

7.2 SF.Administration

In Initialization Phase, this TSF provides Card initialization and pre-personalization services as per GlobalPlatform. This includes but is not restricted to card initialization, patch loading, applet installation and instantiation.

7.3 SF.Signatory Authentication

This TSF manages the identification and authentication of the Signatory and enforces role separation between the Signatory and the Administrator.

7.4 SF.Signature Creation

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

7.5 SF.Secure Messaging

Commands and responses are exchanged between the TOE and the external device.This TSF provides a secure communication channel between legitimate end points both of the TOE and the external device.

7.6 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.

7.7 SF.Protection

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

8. Additional Rationale

8.1 Dependencies Rationale

8.1.1 SAR Dependencies

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

Table 9. SAR Dependencies

Requirement	Dependencies
ADV_ARC.1	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	ADV_TDS.4, ADV_IMP.1
ADV_IMP.1	ADV_TDS.4, ALC_TAT.2
ADV_INT.2	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	ADV_FSP.5
AGD_OPE.1	ADV_FSP.5
AGD_PRE.1	No dependencies
ALC_CMC.4	ALC_CMS.5, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No dependencies
ALC_DEL.1	No dependencies
ALC_DVS.2	No dependencies
ALC_LCD.1	No dependencies
ALC_TAT.2	ADV_IMP.1
ASE_CCL.1	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependencies
ASE_INT.1	No dependencies
ASE_OBJ.2	ASE_SPD.1
ASE_REQ.2	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependencies
ASE_TSS.1	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	ATE_COV.2
ATE_IND.2	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	ADV_ARC.1, ADV_FSP.5, ADV_TDS.4, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1

8.1.2 Justification of Unsupported Dependencies

All dependencies are supported.

8.1.3 SFR Dependencies

Table 10. SFR Dependencies

Requirement	Dependencies
Functional Requirements	
FCS_CKM.1	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	FCS_CKM.1, FDP_ITC.1/SCD
FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FDP_ITC.1/SCD
FCS_COP.1/ENC	FCS_CKM.4, FDP_ITC.1
FCS_COP.1/MAC	FCS_CKM.4, FDP_ITC.1
FDP_ACC.1/SCD/SVD_Generation	FDP_ACF.1/SCD/SVD_Generation
FDP_ACC.1/SVD_Transfer	FDP_ACF.1/SVD_Transfer
FDP_ACC.1/SCD_Import	FDP_ACF.1/SCD_Import
FDP_ACC.1/Signature_Creation	FDP_ACF.1/Signature_Creation
FDP_ACF.1/SCD/SVD_Generation	FDP_ACC.1/ SCD/SVD_Generation, FMT_MSA.3
FDP_ACF.1/SVD_Transfer	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDP_ACF.1/SCD_Import	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_ACF.1/Signature_Creation	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_ITC.1/SCD	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_UCT.1/SCD	FTP_ITC.1/SCD, FDP_ACC.1/SCD_Import
FDP_RIP.1	No dependencies
FDP_SDI.2/Persistent	No dependencies
FDP_SDI.2/DTBS	No dependencies
FIA_AFL.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1
FIA_UID.1	No dependencies
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	FDP_ACC.1/SCD_Import, FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	FDP_ACC.1/ Signature _creation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD_Import, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1 FDP_ACC.1/SCD/SVD_Generation,
FMT_MSA.3	FMT_MSA.1/ Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	FDP_ACC.1/SCD_Import, FDP_ACC.1/Signature_Creation FDP_ACC.1/SCD/SVD_Generation,
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_SMF.1

FMT_SMF.1	No dependencies
FMT_SMR.1	FIA_UID.1
FTP_EMSEC.1	No dependencies
FPT_FLS.1	No dependencies
FPT_PHP.1	No dependencies
FPT_PHP.3	No dependencies
FPT_TST.1	No dependencies
FTP_ITC.1/SCD	No dependencies

8.2 Rationale for Extensions

Extensions are based on the Protection Profiles [4] [5] and have all been adopted by the developer of the TOE:

- FPT_EMSEC.1 ‘TOE emanation’

8.3 PP Claim Rationale

This ST includes all the security objectives and requirements claimed by the two claimed Protection Profiles [4] [5] and, all of the operations applied to the SFRs are in accordance with the requirements of these PPs. The security requirements in the ST is a super-set of the requirements from the claimed PPs.

8.3.1 PP compliancy

The TOE type is compliant with the claimed PPs: the TOE is a Secure Signature-Creation Device representing the SCD storage, SCD/SVD generation, and signature-creation component.

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

- SSCD of Type 2 represents the SCD storage and signature-creation component.
- SCD generated on an SCD/SVD generation component shall be exported to an SSCD Type 2 over a trusted channel.
- SSCD Type 3 is analogous to a combination of the SCD/SVD generation component and Type 2, but no transfer of the SCD between two devices is provided.
- SSCD Type 2 and Type 3 are personalized components; it means that they can be used for signature creation by one specific user – the signatory - only.

Actually, Type 2 and Type 3 are not necessarily to be considered mutually exclusive, as both PPs state.

The conformance to the PPs is strict.

9. Terminology

Term	Definition
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).
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 Representation	Data to be signed representation (DTBS-representation) means the representation data sent by the SCA to the TOE for signing and is - 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-representation, 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.
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.

Term	Definition
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-representation to the TOE, if the signatory indicates by specific non misinterpretable 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)
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)
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)
TS	Tessera Sanitaria
VAD	Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user’s biometric characteristics.

10. References

[1] Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-001 - Part 1: Introduction and general model, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-002 - Part 2: Security functional requirements, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-003 - Part 3: Security assurance requirements, Revision 4, September 2012.

[4] prEN 14169-2:2009 – Protection profiles for Secure signature creation device — Part 2: Device with key generation – Version: 1.03, 12/2009

[5] prEN 14169-3:2012 – Protection profiles for secure signature creation device — Part 3: Device with key import - Version: 1.0.2, 07/2012

[6] BSI-PP-0035-2007 – Security IC Platform Protection Profile – version 1.0 – EAL4+

[7] PKCS#1: RSA Cryptography Standard, Version 2.1

[8] Specifications for the Java Card 3 Platform, Version 3.0.4 Classic Edition, Sept. 2011
- Virtual Machine Specification [JCVM]
- Application Programming Interface [JCAPI]
- Runtime Environment Specification [JCRE]

[9] GlobalPlatform, Card Specification, Version 2.2.1, Jan. 2011 [GPC_SPE_034]
- GlobalPlatform Card ID Configuration, Version 1.0, Dec. 2011 [GPC_GUI_039]
- Confidential Card Content Management – Amendment A, v1.0.1, Jan 2011
- Secure Channel Protocol 03 – Amendment D, v1.1, Sept. 2009

[10] CCDB-2007-09-001 – Composite product evaluation for Smart Cards and similar devices – Version: 1.0, revision 1, September 2007

[11] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[12] 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.

[13] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[14] ISO/IEC 9796-2: Information technology — Security techniques — Signature Schemes giving message recovery — Part 2: Integer factorization based mechanisms, 2002

[15] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993

[16] Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006.

[17] FIPS PUB 180-2, FIPS Publication – Secure hash standard (+ Change Notice to include SHA-224), 2002, NIST

[18] FIPS PUB 46-3, FIPS Publication – Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. Department of Commerce/NIST

[19] IEEE 1363-2000 – IEEE Standard Specification for Public-Key Cryptography

[20] ISO/IEC 9797-1: 2011 Information technology -- Security techniques – Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher

[21] NXP Secure Smart Card Controller P6022y VB, Security Target, Rev. 2.2, 2018-11-27

[22] Crypto Library V3.1.x on P6022y VB, Security Target, Rev. 2.0, 2018-03-22

[23] Common Methodology for Information Technology Security Evaluation - Evaluation Methodology, Version 3.1 CCMB-2012-09-004, Revision 4, September 2012

[24] JCOP 3 P60, Security Target, Rev. 4.0, 2019-08-23

[25] ChipDoc v7b4 applet in SSCD configuration – Preparation and Operation Manual, Revision 1.9, 01 April 2020

[26] prEN 14169-1:2010 – Protection profiles for Secure signature creation device — Part 1: Overview, date 2012–01

[27] EN 419211-1:2011 – Protection profiles for Secure signature creation device — Part 1: Overview

[28] PKCS #1: RSA Cryptography Standards, Version 2.1, June 2002, RSA Laboratories

[29] ISO/IEC 14888-3:2015: Information technology – Security techniques – Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms, 2016

[30] ANSI X9.62-2005: Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute (ANSI), 2005.

[31] FIPS PUB 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/National Institute of Standards and Technology, 26 November 2001.

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.

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 accepts 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.

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

ICs with DPA Countermeasures functionality

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

11.4 Trademarks

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

12. List of figures

13. List of tables

14. Contents

For more information, visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 01 April 2020
Document identifier:

For more information, visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 01 April 2020
Document identifier: