NXP JAVA OS1 ChipDoc v1.0
SSCD
(J3K080/J2K080)

–

Security Target Lite

Version 1.8

August 20, 2015

athena Smartcard

Athena Smartcard Inc., 16615 Lark Ave, Suite 202, Los Gatos CA 95032

Contents

1. ST INTRODUCTION 4
1.1. ST IDENTIFICATION 4
1.2. COMPOSITE TOE 5
1.3. TOE OVERVIEW 5
2. TOE DESCRIPTION 6
2.1. GENERAL 6
2.2. TOE BOUNDARIES 7
2.3. CHIPDOC V1.0 - SECURE SIGNATURE CREATION DEVICE 8
2.4. TOE LIMITS 9
2.5. TOE GUIDANCE 10
2.6. TOE LIFECYCLE 11
3. CONFORMANCE CLAIMS 16
3.1. CC CONFORMANCE CLAIM 16
3.2. PP CLAIM 16
4. SECURITY PROBLEM DEFINITION 17
4.1. ASSETS 17
4.2. SUBJECTS 17
4.3. ASSUMPTIONS 18
4.4. THREATS 19
4.5. ORGANIZATIONAL SECURITY POLICIES 20
5. SECURITY OBJECTIVES 21
5.1. SOS FOR THE TOE 21
5.2. SOS FOR THE ENVIRONMENT 23
5.3. SECURITY OBJECTIVES RATIONALE 24
6. EXTENDED COMPONENTS DEFINITION 28
6.1. TOE EMANATION (FPT_EMSEC.1) 28
7. SECURITY REQUIREMENTS 29
7.1. TOE SECURITY FUNCTIONAL REQUIREMENTS 29
7.2. TOE SECURITY ASSURANCE REQUIREMENTS 37
7.3. SECURITY REQUIREMENTS RATIONALE 39
8. TOE SUMMARY SPECIFICATION 42
9. TERMINOLOGY 43
10. REFERENCES 45

List of Tables

TABLE 1 – SECURITY ENVIRONMENT TO SECURITY OBJECTIVES MAPPING 24
TABLE 2 – ASSURANCE REQUIREMENTS: EAL5 AUGMENTED 37
TABLE 3 – FUNCTIONAL REQUIREMENT TO TOE SECURITY OBJECTIVE MAPPING 40

List of Figures

FIGURE 1 – TOE FORM FACTOR 6
FIGURE 2 – TOE BOUNDARIES 7
FIGURE 3 - SSCD TYPES AND MODES OF OPERATION 8
FIGURE 4 - SCOPE OF THE SSCD, STRUCTURAL VIEW 10
FIGURE 5 – TOE LIFECYCLE 11

1. ST Introduction

1.1. ST Identification

ST title	NXP JAVA OS1 ChipDoc v1.0 SSCD (J3K080/J2K080)
Authors	Athena
ST Lite Version Number	1.8
Date of production	August 20, 2015
TOE Reference	ROM Mask Reference: OS755_ePassport_P60D080_002 IASECCv2 Applet Athena Name ChipDocv1.0 Version 0105 Build 0119 ROM Code reference: "v0005 b0019" IDProtect Duo v12 Athena Name NXP JAVA OS1 Release Date 0x4258 Release Level 0xFF02 ROM Code reference: OS755_ePassport_P60D080_002 P60D080JVC NXP Revision C Identification Number P60D080PX36/9C44230 Certificate BSI-DSZ-CC-0897-2013 Interfaces Contact only (J2K080) & Dual interface (J3K080) Crypto Library NXP Version 1.0 Certificate NSCIB-CC-12-36243-CR2
Common Criteria	CC version 3.1 Part 1: CCMB 2012-09-001 revision 4 [1] Part 2: CCMB 2012-09-002 revision 4 [2] Part 3: CCMB 2012-09-003 revision 4 [3]
PP Claim	Protection profiles for Secure signature creation device — Part 2: Device with key generation Version: 1.03, EAL 4+ Identification BSI-CC-PP-0059
	Protection profiles for secure signature creation device — Part 3: Device with key import Version: 1.0.2, EAL 4+ Identification BSI-CC-PP-0075

1.2. Composite TOE

In this Security Target, the name of the composite TOE developer (Athena Smartcard Solutions, Inc.) will be referenced as 'Athena'.

Operating System: Athena IDProtect Duo v12 (also known as "NXP JAVA OS1")

Java Card Applet: IASECCv2 (also known as "ChipDoc v1.0")

IDProtect with associated IASECCv2 applet are embedded on NXP P60D080JVC IC.

The composition analysis conducted in this section will use the words Platform to designate the NXP P60D080JVC IC [6, 7], Application to designate the two software components Athena IDProtect/OS755 (NXP OS1) and Athena IASECCv2 Applet (NXP ChipDoc v1.0), and Composite Product to designate the TOE.

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

Platform Developer	NXP
Platform Evaluator	TUV-IT
Platform Certification Body	BSI
Application Developer	Athena
Composite Product Integrator	NXP
Composite Product Evaluator	Serma Technologies
Composite Product Certification Body	ANSSI
Composite Product evaluation Sponsor	Athena

The platform was evaluated to CC EAL 5+ according to BSI-PP-0035-2007 [8] (see platform Security Target [10], IC certification report [9]).

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

1.3. TOE Overview

The TOE implements a Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC [15] 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.

NXP JAVA OS1 is a multi-application Java Card which supports RSA cryptography of up to 4096.

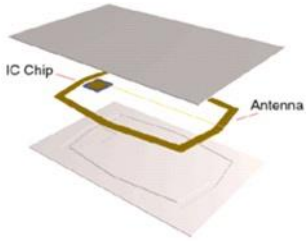
The TOE meets all the following requirements as defined in the European Directive (article 2.2):

(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

2. TOE Description

2.1. General

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

<table>
<tr><td colspan="3">1. Contactless interface cards and modules</td></tr>
<tr><td colspan="3"> 

(antenna embedded in plastic)</td></tr>
<tr><td colspan="2">2. Dual interface cards and modules</td><td>3. Contact only cards and modules</td></tr>
<tr><td>  (antenna embedded in plastic)</td><td colspan="2"> 

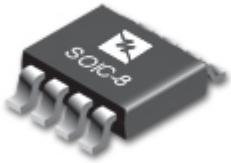
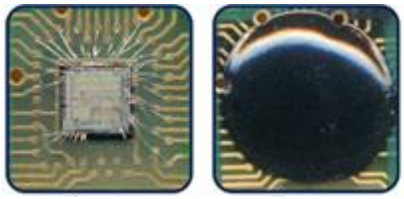
(contactless interface absent or disabled)</td></tr>
<tr><td>4. SOIC8 package</td><td>5. QFN44 package</td><td>6. Chip on Board (PCB)</td></tr>
<tr><td> 
</td><td> 
</td><td>  </td></tr>
</table>

Figure 1 – 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.

2.2. TOE Boundaries

The TOE boundaries are the following:

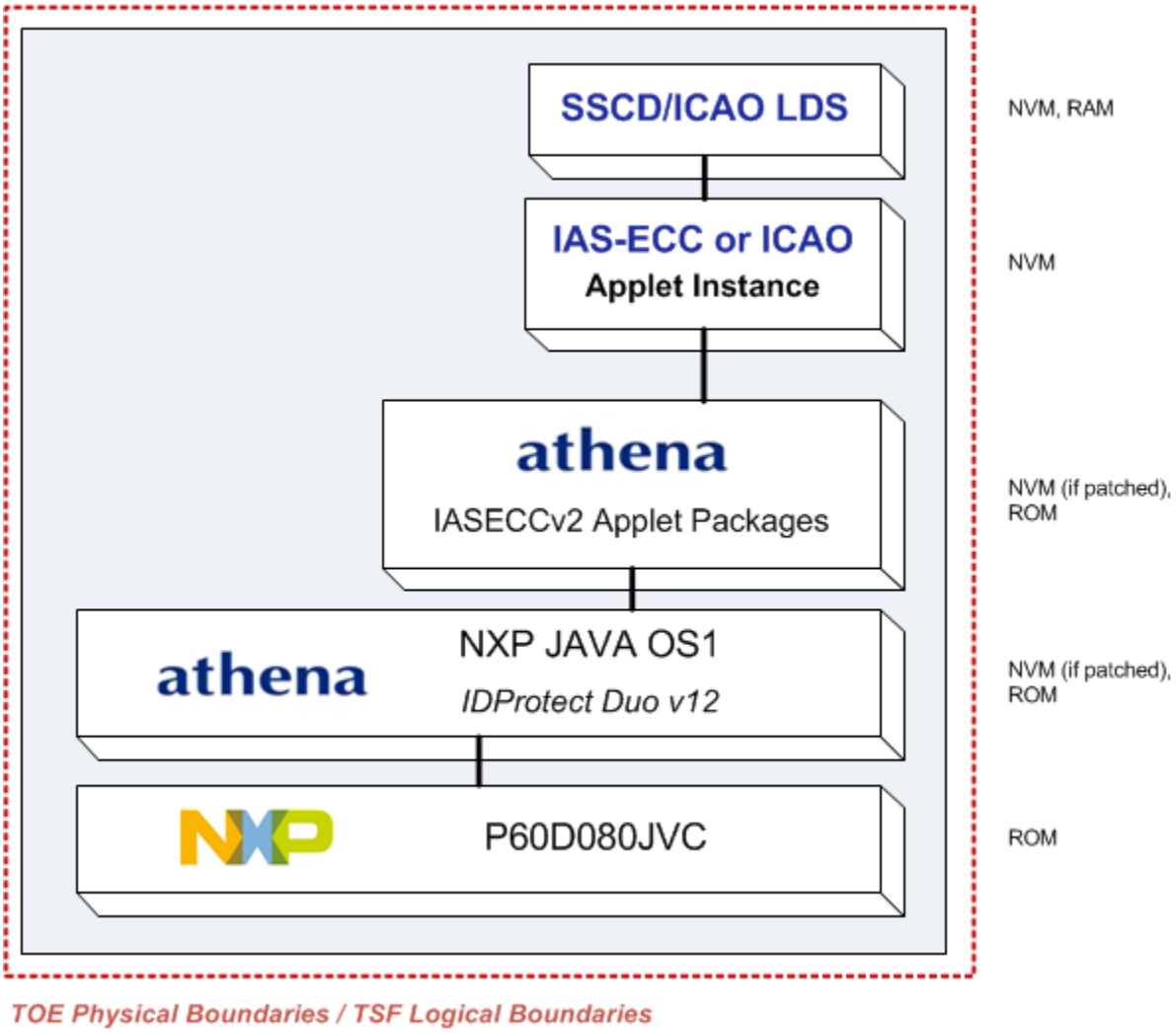


Figure 2 – TOE Boundaries

The IASECCv2 Applet package is the only applet in ROM. It could be instantiated into an ICAO applet instance or an IASECCv2 applet instance. Only the IASECCv2 applet instance is part of the TOE.

However, in a general aspect, JAVA OS1 (IDProtect Duo v12) Operating System enforces separation of the data between the applets and associated packages imposing logical separation of data using the Java Card™ Firewall [11-JCRE].

IASECCv2 Applet can also be instantiated in ICAO mode, and is then out of the scope of this TOE in this mode.

JAVA OS1 is a GlobalPlatform 2.2.1 and Java Card 3.0.4 compliant Operating System that provides applets with standard services as defined in the related GlobalPlatform [13] and Java Card specifications [12].

The portions of the Applet Packages and Operating System present in EEPROM are the patches.

The hardware platform on which the Operating System is implemented is the NXP P60D080JVC IC. This IC is certified according to CC EAL 6+ [9] with the Security Target compliant with BSI-PP-0035-2007 [8].

2.3. ChipDoc v1.0 - Secure Signature Creation Device

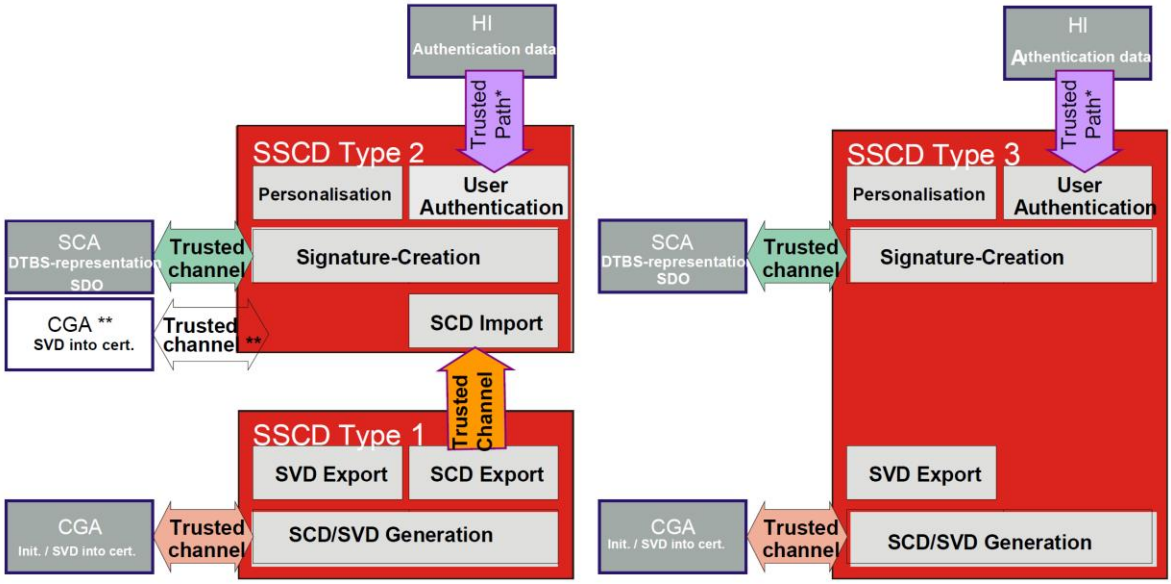
The following is an introduction to SSCD based on the SSCD Protection Profile [4] and [5].

The PP documents assume a well-defined process signature-creation to take place. The present chapter defines three possible SSCD implementations, referred to as 'SSCD types', as illustrated in Figure 3.

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). If the Human Interface (HI) for such signatory authentication is not provided by the SSCD, and thus a trusted path (e.g., a encrypted channel) between the SSCD and the SCA implementing to HI is to be provided. 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.

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



* The trusted path for user authentication will be required if the HI is not provided by the TOE itself

(e. g., it is provided by a SCA outside the SSCD)

** The trusted channel between the SSCD Type 2 and the CGA is required for cases where the SSCD type 2 holds the SVD and export of the SVD to the CGA for certification is provided

Figure 3 - SSCD types and modes of operation

2.4. 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 [15].The destruction of the SCD is mandatory before the TOE generate a new pair SCD/SVD or loads a new pair SCD/SVD.

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

The TOE described in this ST is a smart card operating system implemented on a smart card IC which is certified CC EAL 5+. The TOE includes embeddable software in the NVM of the IC and a file system including the digital signature application stored in EEPROM. Parts of the operating systems may be stored in EEPROM. NVM (Non Volatile Memory) corresponds to ROM memory for the NXP P60D080JVC IC [10, 8].

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 generation of the SCD/SVD key pair by means of a SSCD type 1 requires the export of the SCD into the TOE (Type 2). Vice versa, signature generation by means of the TOE (Type 2) requires that the SCD/SVD has been generated by and imported from an SSCD Type 1, or has been generated by the TOE itself. Consequently, there is interdependence where an SSCD Type 1 constitutes the environment of the TOE.

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 may provide an interface for user authentication by its own or implements IT measures 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 allows to implement a Human Interface (HI) for user authentication:

(i) by the TOE itself or

(ii) by 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.

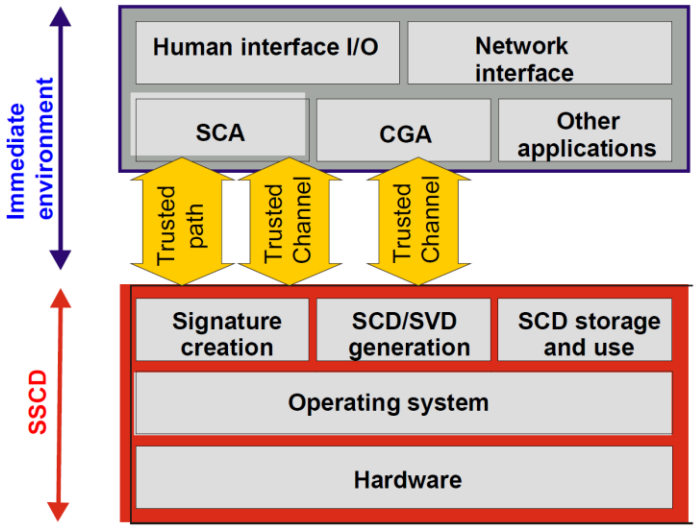


Figure 4 - Scope of the SSCD, structural view

Figure 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.

2.5. TOE Guidance

The TOE guidance comprises the following documentation:

Title	Date	Version
ChipDoc v1 SSCD – Preparation manual	*Consult certification report for applicable dates and versions*	
ChipDoc v1 SSCD – Operation manual		

2.6. TOE lifecycle

The TOE lifecycle is shown in Figure 5.

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

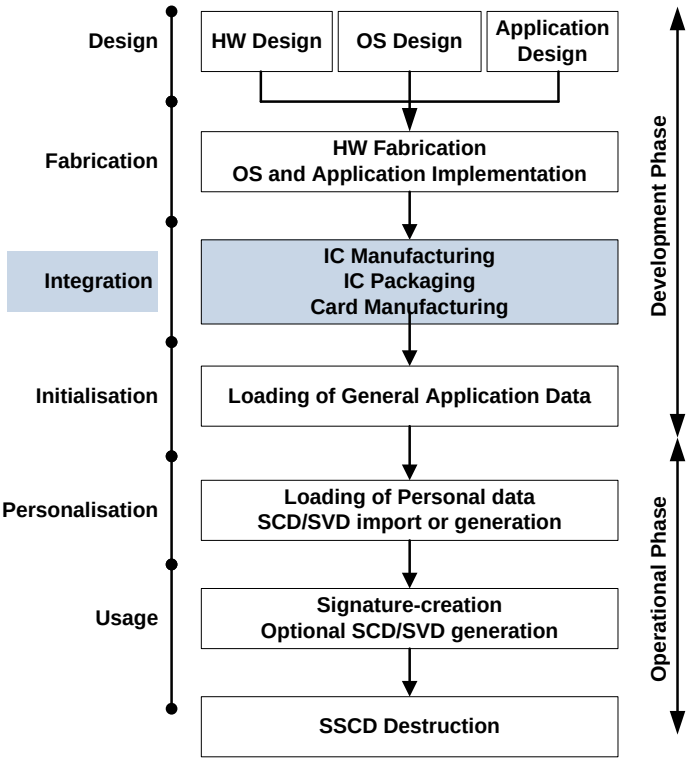


Figure 5 – TOE lifecycle

2.6.1. 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.

HW Design – NXP

OS Design – Athena Development departments – Livingston, Scotland
Application Design – Athena Development departments – Los Gatos, US

2.6.2. Fabrication Phase

HW Fabrication and OS & Application implementation – NXP

IC Manufacturing – NXP

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

2.6.3. Integration Phase

IC Manufacturing – NXP

IC Packaging – NXP

Card Manufacturing – NXP

This phase corresponds to the integration of the hardware and firmware components into the final product body. 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.

2.6.4. Initialization Phase

Athena sends to NXP the confidential information required to complete this phase. Initialization is done within NXP facilities used for the Common Criteria certified ICs (here the P60D080) production, under the governance of NXP. The TOE is protected during transfer by the confidential information which resides in the card during mask production (transport key).

The initialization phase consists in OS configuration, applet instantiation and/or applet and OS patching activities (in EEPROM). Creation of the application implies applet instantiation and the creation of MF and IASECCv2 ADF. 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).

Initialization – Initialization facility of Card Manufacturer (NXP).

The product becomes operational and is delivered after this initialization phase.

2.6.5. Personalization Phase

Personalization – after unlocking the product with the transport key, Athena 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.

2.6.6. Operational Phase

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

Usage – Where upon the card is delivered from the Customer (the Card Issuer) to the End User and the End User may use it for signature-creation including all supporting functionality (e.g., SCD storage and SCD use).

The product is considered in use phase.

2.6.7. 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 [15].

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

2.6.8. Features of IDProtect – Informational

Note: The features described in this section are provided by the IDProtect product family, they are not necessarily Security Functions of the TOE.

Java promises write once, run anywhere capability. Athena SCS IDProtect - Athena SCS Java Card technology and GlobalPlatform Operating System - fulfils that promise for the smart card industry.

JAVA OS1 (IDProtect Duo v12) is built to give you flexibility in the way you work: a blank canvas on which to create smart card products for all market sectors.

Central to JAVA OS1 is its compliance with the Java Card and GlobalPlatform standards; multiple compliant Java Card applets from any source will run securely on JAVA OS1 enabled silicon. Applets can be securely loaded and deleted post issuance thanks to GlobalPlatform compliant Issuer Security Domain implementation. Athena SCS uses its RapidPort architecture to ease the process of porting the system to different silicon platforms, including contactless, meaning it is already available on various devices from leading manufacturers.

2.6.8.1. GlobalPlatform

JAVA OS1 provides a Card Manager. This is a generic term for the three card management entities of a GlobalPlatform card; the GlobalPlatform Environment, Issuer Security Domain and Cardholder Verification Method Service Provider.

JAVA OS1 is compliant with GlobalPlatform Card Specification 2.2.1 [13]:

- GP 2.2.1 ID Profile
- GP 2.2 amendments:
  - A : Store Data
  - D : SCP 03, AES Tokens, AES DAPs and AES Receipts
  - E : Card Capability Information, Command Chaining, RSA variant 2 Tokens & DAPs, ECC Tokens & DAPs and PUT KEY for ECC Keys

GlobalPlatform 2.2.1	Information Technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange
Atomic Package and Application Deletion	Memory recovered and is reusable
Global PIN	A PIN that may be checked by all applets on a card, using CVM.verify(). Its value is usually set at personalization time
Secure Channel Protocol 01	SCP01 provides mutual authentication; integrity and data origin authentication; confidentiality
Secure Channel Protocol 02	Support for all SCP02 options
Secure Channel Protocol 03	Support for all SCP03 options
Repeated application install failure	The OPEN may keep track of the number of unsuccessful consecutive attempts of the Card Content load and installation process by a particular Application and the total number of such attempts by all applications. Actions may include such defensive measures as the locking or termination of the card
Applications boundary violations	The OPEN may also enable velocity checking against repeated failed attempts by an Application to allocate additional memory beyond its allowed limit as stored in the Open Platform Registry. The OPEN may choose to lock an Application which exhibits such behavior

2.6.8.2. Java Card

JAVA OS1 is compatible with the following Java Card standards [12] Version 3.0.4 Classic Edition, Sept. 2011:

- Runtime Environment Specification for the Java Card Platform,
- Application Programming Interface, Java Card Platform,
- Virtual Machine Specification for the Java Card Platform,

Data type *int* is optionally supported in the JCVM and is supported in JAVA OS1.

2.6.8.3. Security settings

Keys and PINs are stored encrypted	The OS does not store any Keys or PINs in plain text during computation
On card key generation	RSA keys indicated in the Key Pair list may be generated on the card
FIPS 140-2 Level 3	Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules FIPS PUB 140-2
FIPS approved DRBG	IDProtect supports the secure RNG specified in JC API and is FIPS approved
FIPS 140-2 Self Tests	Self-tests are performed to check that the HRNG and the DRBG are not blocked and that RSA Keys that are generated by the TOE are a consistent pair.
FIPS 140-2 KAT	Known Answer Tests performed at power up. The cryptographic function tests consist of computing from pre-recorded input data, and comparing the results with pre-recorded answers
FIPS 140-2 Software Integrity	Checks that no FIPS application present in EEPROM (packages) is corrupted. The error detecting code is FIPS approved

2.6.8.4. Communication

The interfaces of JAVA OS1 are:

- Contact
  - Physical: ISO/IEC 7816- 1 and 2
  - Electrical: ISO/IEC 7816- 3 and 4
- Contactless with a full support for ISO/IEC 14443 Type A protocol

JAVA OS1 provides the following communication features:

- Protocol T=0 with PPS for speed enhancement
- Protocol T=1 with PPS for speed enhancement with extended APDU length support.

2.6.8.5. Cryptography

JAVA OS1 supports the following cryptographic algorithms:

- AES: AES_128, AES_192, AES_256
- DES [20]: Single DES, 2 Key TDES, 3 Key TDES
- Elliptic Curves [18]:
    - Types: Finite Prime Field (EC_FP) and Binary Finite Field (EC_F2M)
    - Key pair generation
    - Key length: EC_FP = 192 to 521 bits
      EC_F2M = 163, 193, 233, 283 and 409
    - Signature Algorithm: ALG_ECDSA_SHA, ALG_ECDSA_SHA_224, ALG_ECDSA_SHA_256, ALG_ECDSA_RAW
- RSA:
    - Types: Standard and CRT
    - Key pair generation
    - Used Key length: up to RSA_4096 bits
    - Signature Algorithms: ALG_RSA_SHA_PKCS1, ALG_RSA_SHA_PKCS1_PSS, ALG_RSA_SHA_ISO9796 [15], ALG_RSA_SHA_256_PKCS1, ALG_RSA_SHA_256_PKCS1_PSS
    - Cipher Algorithms: ALG_RSA_NOPAD, ALG_RSA_PCKS1, ALG_RSA_PCKS1_OAEP
- Hash: SHA-1, SHA-224 [16], SHA-256, SHA-384, SHA-512, MD-5
- CRC: CRC-16 and CRC-32
- Additions: SEED, GOST
- RNG: PSEUDO and SECURE
- Biometrics:

Note that not all the Cryptographic algorithms, lengths and modes are involved in TOE Security Functions. Please refer to the relevant SFRs for a complete description of what cryptography is used by the TOE.

3. Conformance Claims

3.1. CC Conformance Claim

The ST claims compliance with the following references:

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

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

- FPT_EMSEC.1 'TOE emanation'

The assurance level for this ST is EAL 5 augmented with:

- AVA_VAN.5
- ALC_DVS.2

3.2. PP Claim

This ST claims strict compliance to the following Protection Profiles:

[4]	**Protection Profile — Secure Signature-Creation Device Type 2**
Version	1.03
Date	12/2009
Identification	prEN 14169-1:2009
Approved by	AFNOR
Registration	BSI-PP-0059

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

4. Security Problem Definition

4.1. Assets

SCD

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

SVD

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

DTBS and DTBS-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)

4.2. Subjects

This Security Target considers the following subjects:

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

4.3. Assumptions

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

A.CGA	*Trustworthy certification-generation application*

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

4.4. Threats

4.4.1. Threat agents

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

4.4.2. Threats to Security

T.Hack_Phys	*Physical attacks through the TOE interfaces*

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

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

An attacker can store, copy, the SCD outside the TOE. An attacker can 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.

4.5. 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.

5. Security Objectives

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

5.1. SOs 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_Gen	*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.

5.2. SOs for the Environment

Because JAVA OS1 SSCD is both SSCD type 2 and SSCD type3 means that the TOE environment consists of a CGA, an SCA, an SSCD type 1 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.HI_VAD	*Protection of the VAD*

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

OE.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 SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSVD Type1 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 SSCD Type1 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.

5.3. Security objectives rationale

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

5.3.1. Security Objectives Coverage

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

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

Table 1 – Security Environment to Security Objectives Mapping

5.3.2. Security Objectives Sufficiency

5.3.2.1. Policies and Security Objective Sufficiency

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

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

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

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

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

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

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

- **OT.Lifecycle_Security** requiring the TOE to detect flaws during the initialisation, personalisation and operational usage,
- **OT.SCD/SVD_Gen**, which limits invoke the generation of the SCD and the SVD to authorised users only,
- **OT.Sigy_SigF**, which requires the TOE to provide the signature generation function for the legitimate signatory only and to protect the SCD against the use of others.
- **OT.SCD_Auth_Imp,** which limits SCD import to authorised users only,
- **OE.SCD_Secrecy**, which ensures the confidentiality of the SCD during generation and export to the TOE, and deletes the SCD after export to the TOE. The CSP does not use the SCD for signature creation.

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

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

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

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

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

5.3.2.2. Threats and Security Objective Sufficiency

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

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

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

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

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

T.SigF_Misuse (*Misuse of the signature-creation function of the TOE*) addresses the threat of misuse of the TOE signature-creation function to create SDO by others than the signatory to create a digital signature on data for which the signatory has not expressed the intent to sign,. **OT.Lifecycle_Security** (*Lifecycle security*) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. **OT.Sigy_SigF**

(*Signature creation function for the legitimate signatory only*) ensures that the TOE provides the signature-generation function for the legitimate signatory only. **OE.DTBS_Intend** (*Data intended to be signed*) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and **OE.DTBS_Protect** counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. **OT.DTBS_Integrity_TOE** (*DTBS/R integrity inside the TOE*) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, **OE.HID_VAD** (*Protection of the VAD*) provides confidentiality and integrity of the VAD as needed by the authentication method employed. **OE.Signatory** ensures that the Signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the Signatory becomes control over the SSCD. **OE.Signatory** ensures also that the Signatory keeps his or her VAD confidential.

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

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

5.3.2.3. Assumptions and Security Objective Sufficiency

A.SCA (*Trustworthy signature-creation application***)** establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by **OE.DTBS_Intend** *(Data intended to be signed*) which ensures that the SCA generates the DTBS/R for the data that has been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

A.CGA (*Trustworthy certification-generation application***)** establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by **OE.CGA_QCert** (*Generation of qualified certificates*), which ensures the generation of qualified certificates and by **OE.SVD_Auth** (*Authenticity of the SVD*), which ensures the protection of the integrity and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

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

6. Extended Components Definition

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

- SFR FPT_EMSEC.1 'TOE emanation'

6.1. 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 TOE emanation	1

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*].**

7. Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE.
Security functional requirements components given in section 7.1, except FPT_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 7.2 is drawn from the security assurance components from Common Criteria part 3 [3].

7.1. TOE Security Functional Requirements

7.1.1. Cryptographic support (FCS)

7.1.1.1. Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm *RSA* and specified cryptographic key sizes *between 1024 bit and 2048 bit* that meet the following: *PKCS#1 v1.5 as per Algorithms and parameters for algorithms [11]*.

7.1.1.2. 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* 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.

7.1.1.3. Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *1024 bit, 1536 bit and 2048 bit* that meet the following: *RSA CRT with hashing SHA-1 or SHA-256 and with padding PKCS#1 v1.5 as per Algorithms and parameters for algorithms [11]*.

FCS_COP.1.1/ ENC The TSF shall perform *data encryption/decryption for Administrator and Signatory authentication and Secure Messaging* in accordance with a specified cryptographic algorithm *TDES CBC* and cryptographic key sizes *16 bytes* that meet the following: *FIPS PUB 46-3 Data Encryption Standard (DES) [22] and [24].*

FCS_COP.1.1/ MAC The TSF shall perform *Message Authentication Code for Secure Messaging* in accordance with a specified cryptographic algorithm *TDES MAC* and cryptographic key sizes *16 bytes* that meet the following: *FIPS PUB 46-3 Data Encryption Standard (DES) [22] and [24]*.

7.1.2. User data protection (FDP)

7.1.2.1. Subset access control (FDP_ACC.1)

FDP_ACC.1.1/ SVD Transfer SFP	The TSF shall enforce the SVD Transfer SFP on import and on export of SVD by User.

Application note:

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

FDP_ACC.1.1/ SCD_Import	The TSF shall enforce the SCD Import SFP on Import of SCD by User.
FDP_ACC.1.1/ SCD/SVD_Generation_SFP	The TSF shall enforce the SCD/SVD_Generation SFP on generation of SCD/SVD pair by User.
FDP_ACC.1.1/ Signature_Creation_SFP	The TSF shall enforce the Signature-creation SFP on (1) subjects: S.User, (2) objects: DTBS-representation, SCD, (3) operations: signature creation.

7.1.2.2. 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

Generation SFP

FDP_ACF.1.1/ SCD/SVD_Generation_SFP	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_SFP	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_SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ SCD/SVD_Generation_SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: S.User with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.

SVD Transfer SFP

FDP_ACF.1.1/ SVD Transfer SFP	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 SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *The user with the security attribute "role" set to "Administrator" or to "Signatory"* is allowed to export SVD.
FDP_ACF.1.3/ SVD Transfer SFP	The TSF shall explicitly authorise access of subjects to objects based On the following additional rules: none.
FDP_ACF.1.4/ SVD Transfer SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: none.

SCD Import SFP

FDP_ACF.1.1/ SCD Import SFP	The TSF shall enforce the SCD Import SFP to objects based on the following: General attribute and Initialisation attribute group.
FDP_ACF.1.2/ SCD Import SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".
FDP_ACF.1.3/ SCD Import SFP	The TSF shall explicitly authorise access of subjects to objects based On the following additional rules: none.
FDP_ACF.1.4/ SCD Import SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to import SCD.

Signature-creation SFP

FDP_ACF.1.1/ Signature Creation SFP	The TSF shall enforce the Signature-creation SFP to objects based on the following: General attribute and Signature-creation attribute group.
FDP_ACF.1.2/ Signature Creation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute "role" set to "Signatory" is allowed to create digital signatures for DTBS-representation with SCD which security attribute "SCD operational" is set to "yes"
FDP_ACF.1.3/ Signature Creation SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ Signature Creation SFP	The TSF shall explicitly deny access of subjects to objects based on the rules: S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no".

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

FDP_ITC.1.1/ SCD — The TSF shall enforce the SCD Import SFP when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/ SCD — The TSF shall enforce the following rules when importing SCD controlled under the SFP from outside the TOE: SCD shall be sent by an authorised SSCD.

Application note:

An SSCD of Type 1 is authorised to send SCD to an SSCD of Type 2, if it is designated to generate the SCD for this SSCD of Type 2 and to export the SCD for import into this SSCD of Type 2. Authorised SSCD of Type 1 is able to establish a trusted channel to the SSCD of Type 2 for SCD.

7.1.2.1. Basic data exchange confidentiality (FDP_UCT.1)

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

7.1.2.2. Subset residual information protection (FDP_RIP.1)

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

7.1.2.3. 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.2.1/ Persistent — The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: *integrity checked persistent data*.

FDP_SDI.2.2/ Persistent — Upon detection of a data integrity error, the TSF shall

1. prohibit the use of the altered data
2. inform the Signatory about integrity error.

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

FDP_SDI.2.1/ DTBS — The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: *integrity checked stored data*.

FDP_SDI.2.2/ DTBS — Upon detection of a data integrity error, the TSF shall

1. prohibit the use of the altered data
2. inform the Signatory about integrity error.

7.1.3. Identification and authentication (FIA)

7.1.3.1. Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when *10 consecutive* unsuccessful authentication attempts occur related to: *RAD authentication and PUK authentication*.

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

7.1.3.2. Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow

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

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

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

Application note:

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

7.1.3.3. Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow

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

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

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

7.1.4. Security management (FMT)

7.1.4.1. Management of security functions behaviour (FMT_MOF.1)

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

7.1.4.2. Management of security attributes (FMT_MSA.1)

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

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

7.1.4.3. Secure security attributes (FMT_MSA.2)

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

7.1.4.4. Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the SCD Import SFP, SCD/SVD Generation SFP, SVD Transfer SFP and Signature-creation 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.

7.1.4.1. 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 Adminsitrator 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 Signatory 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.Sigy 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.Sigy is currently authenticated, the security attribute “SCD operational” of the SCD shall be set to “yes” after import of the SCD as a single operation.

7.1.4.2. Management of TSF data (FMT_MTD.1)

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

Application note:

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

7.1.4.3. Specifications of Management Functions (FMT_SMF.1)

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

RAD creation, RAD Modification,

Enabling the signature creation function,

Modification of the security attribute SCD/SVD management, SCD

operational,

Change the default value of the security attribute SCD Identifier,
Access Condition Management

7.1.4.4. Security roles (FMT_SMR.1)

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

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

7.1.5. Protection of the TSF (FPT)

7.1.5.1. TOE Emanation (FPT_EMSEC.1)

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

FPT_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.

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

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *IC sensors failure detection (RNG failure, EEPROM failure, out of range temperature, clock and voltage of chip), failure from self test under FPT_TST*

7.1.5.3. Passive detection of physical attack (FPT_PHP.1)

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

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

7.1.5.4. Resistance to physical attack (FPT_PHP.3)

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

7.1.5.5. TSF testing (FPT_TST.1)

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

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.

7.1.6. Trusted path/channels (FTP)

7.1.6.1. Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SCD	The TSF shall provide a communication channel between itself and 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 SSCD type 1 for SVD import, the CGA for the SVD export, and the SCA for DTBS Import.

7.2. 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.

7.2.1. SARs Measures

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

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**

Table 2 – Assurance Requirements: EAL5 augmented

7.2.2. 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, though 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 of the security of the MRTD's development and manufacturing especially for the secure handling of the MRTD's material.

The component ALC_DVS.2 has no dependencies.

AVA_VAN.5 Vulnerability Assessment - Advanced methodical vulnerability analysis

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

The component AVA_VAN.5 has the following dependencies:

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.

7.3. Security Requirements Rationale

7.3.1. Security Requirement Coverage

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

TOE SFRs / TOE Security objectives	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Auth_Imp
FCS_CKM.1	X		X	X	X							
FCS_CKM.4	X				X							
FCS_COP.1	X					X						
FCS_COP.1/ENC	X					X						
FCS_COP.1/MAC	X					X						
FDP_ACC.1/ SCD/SVD_Generation_SFP	X	X										
FDP_ACC.1/ SVD_Transfer_SFP	X											
FDP_ACC.1/SCD_Import	X											X
FDP_ACC.1/Signature_Creation_SFP	X						X					
FDP_ACF.1/ SCD/SVD_Generation_SFP	X	X										
FDP_ACF.1/ SVD_Transfer_SFP	X											
FDP_ACF.1/SCD_Import	X	X										
FDP_ACF.1/Signature_Creation	X						X					
FDP_ITC.1/SCD	X											
FDP_UCT.1/SCD	X				X							
FDP_RIP.1					X		X					
FDP_SDI.2/Persistent				X	X	X						
FDP_SDI.2/DTBS							X	X				
FIA_AFL.1							X					
FIA_UAU.1		X					X					X
FIA_UID.1		X					X					X
FMT_MOF.1	X						X					
FMT_MSA.1/Admin	X	X										
FMT_MSA.1/Signatory	X						X					
FMT_MSA.2	X	X					X					
FMT_MSA.3	X	X					X					
FMT_MSA.4	X	X					X					
FMT_MTD.1/Admin	X						X					
FMT_MTD.1/Signatory	X						X					
FMT_SMR.1	X						X					
FMT_SMF.1	X						X					
FPT_EMSEC.1					X				X			
FPT_FLS.1					X							
FPT_PHP.1										X		

TOE SFRs / TOE Security objectives	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Auth_Imp
FPT_PHP.3					X						X	
FPT_TST.1	X				X	X						
FTP_ITC.1/SCD	X				X							

Table 3 – Functional Requirement to TOE Security Objective Mapping

7.3.2. Security Requirements Sufficiency

OT.Lifecycle_Security (Lifecycle security) is provided by the SFR as follows.
The SCD import is controlled by TSF according to FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import and FDP_ITC.1/SCD. The confidentiality of the SCD is protected during import according to FDP_UCT.1/SCD in the trusted channel FTP_ITC.1/SCD.
For SCD/SVD generation FCS_CKM.1, SCD usage FCS_COP.1 and SCD destruction FCS_CKM.4 ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer_SFP and FDP_ACF.1/SVD_Transfer_SFP.
The secure SCD usage is ensured cryptographically according to FCS_COP.1. The SCD usage is controlled by access control FDP_ACC.1/Signature_Creation_FSP, FDP_ACF.1/Signature_Creation_FSP which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory. The FMT_SMF.1 and FMT_SMR.1 defines security management rules and functions. The test functions FPT_TST.1 provides failure detection throughout the lifecycle. The SFR FCS_CKM.4 ensures a secure SCD destruction. Confidentiality is preserved with FCS_COP.1/ENC and integrity with FCS_COP.1/MAC.

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

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

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

OT.SCD_Secrecy (Secrecy of signature creation data) is provided by the security functions specified by the following SFR. FDP_UCT.1/SCD and FTP_ITC.1/SCD ensures the confidentiality for SCD import. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.
FCS_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.
The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).
The SFR FPT_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. 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_SFP and FDP_ACF.1/Signature_Creation_SFP 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.

8. TOE summary specification

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

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.

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.

This TSF also provides personalization functions to allow the Administrator to create and set the initial File System (LDS).

SF.Signatory Authentication

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

SF.Signature Creation

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

The SF generates digital signatures using RSA 1024 to 2048 bit and SHA-1 hashing calculated by the host. The signature is calculated based on PKCS#1 version 1.5 [11].

SF.Secure Messaging

Commands and responses are exchanged between the TOE and the external device.

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

SF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation, secure random generator, and data hashing.

SF.Protection

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

[More details disclosed upon request to support@athena-scs.com]

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.
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.

Term	Definition
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, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-002 -Part 2: Security functional requirements, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-003 -Part 3: Security assurance requirements, Version 3.1, Revision 4, September 2012.

[4] prEN 14169-1:2009 – 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] NXP P60D080JVC Technical Datasheet.

[7] NXP Toolbox Technical Datasheet.

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

[9] Certification Report BSI-DSZ-CC-0897-V2-2014 – for NXP Secure Smart Card Controller P60D080/052/040yVC – NXP Semiconductors Germany GmbH – v1.0

[10] NXP Secure Smart Card Controller P60D080/052/040yVC Security Target Lite – Rev 1.3 – 17 October 2013

[11] PKCS#1: RSA Cryptography Standard, Version 1.5

[12] 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]

[13] 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

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

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

[16] 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.

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

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

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

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

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

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

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

[24] ISO/IEC 9797-1:1999, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 1999