ID&TRUST DOCUMENTS

COMMON CRITERIA EAL4+

ID&TRUST SECURITY TARGET LITE
SECURE SIGNATURE CREATION DEVICE
HTCNS APPLET V1.03.

Revision History

Version	Date	Information
v1.0	29.04.2015.	First version – created from ST.

Contents

1 Security Target Introduction

1.1 Security Target Reference

Title: ID&Trust Security Target for Secure signature creation device

TOE: ID&Trust CNS Card: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust HTCNS Applet v1.03.

Author: ID&Trust Ltd.

Publication date: 13.04.2015.

CC version: 3.1 Revision 4

Assurance level: CC EAL4+, augmented with the following assurance component: AVA_VAN.5

Version number: v1.00.

TOE guidance documentation:

ID&Trust CNS Applet User's Guide 1.03

ID&Trust CNS Applet Administrator's Guide 1.03

ID&Trust CNS Applet Initialization and Configuration 1.03

Profile FileSystemCNS_21112005_with_DS

The Security Target defines the security requirements of a Secure Signature Creation Device (SSCD) for the generation of signature-creation data (SCD) and the creation of qualified electronic signatures. The TOE may implement additional functions and security requirements e.g. for editing and displaying the data to be signed (DTBS), but these additional functions and security requirements are not subject of this Security Target

Keywords: secure signature-creation device, electronic signature, digital signature

1.2 TOE Reference

The Security Target refers to the SSCD compliant configurations of the HTCNS applet. The HTCNS applet is a Java Card Application used exclusively on the NXP JCOP 2.4.2. R3 Platform, which is a CC EAL5+ certified product.

The TOE comprises:

I. Underlying Platform of the TOE, which is evaluated by Brightsight and certified by TÜV Rheinland Nederland B.V. at assurance level EAL5 augmented with ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2 under the certificate number C13-37761

Long Platform name: J3E081_M64, J3E081_M66, J2E081_M64 Secure Smart Card Controller Revision 3

Short name: JCOP 2.4.2 R3

It consists of:

a. Smart card Platform (SCP), which consists of:
   - Hardware Abstraction Layer with the Crypto Library,
   - Hardware Platform

b. Embedded software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager)

c. Native MIFARE application (physically always present but logical availability depends on configuration)
and

II. the Application Part of the TOE:
ID&Trust CNS Applet Version 1.03.

III. the associated guidance documentation.

1.3 TOE Overview

The TOE is an SSCD as a smart card which is able to generate signature creation data (SCD) and create qualified electronic signatures. The TOE protects the SCD and ensures that only an authorized signatory can use it.

The HTCNS applet is installed on the NXP JCOP v2.4.2 R3 Secure Smart Card Controller, which is an NXP SmartMX IC with JCOP 2.4.2 Java Card OS. The NXP J3E081_M64, J3E081_M66 and J2E081_M64. Smart Card Controller IC supporting contact and contactless interfaces.

The TOE is a multi-application smart card Platform for secure signature creation purposes supporting various algorithms.

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

it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

1.3.1 Non-TOE hardware/software/firmware

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet are needed to represent a complete electronic card, nevertheless these parts are not inevitable for the secure operation of the TOE

1.4 TOE Description

1.4.1 Product type

The TOE is the Smart Card Integrated Circuit with Embedded Software serving as an SSCD (Secure Signature Creation Device) in accordance to its functional specification. The smart card chip module can be embedded in a plastic card or other device (ex. an USB token) providing a physical interface between the terminal and the chip.

The TOE is defined by the following components:

Integrated Circuit (Smart Card Platform)

- Secure smart card controller:
  NXP Secure Smart Card Controllers P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s)
  Evaluation Level for the Smart Card Controller: EAL 5 augmented by ASE_TSS.2, AVA_VAN.5 and ALC_DVS.2, claiming conformance to the Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-CC-PP-0035-2007. Certification number: BSI-DSZ-CC-0857
- Crypto Library:
  Crypto Library V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s)
  Evaluation Level for the hardware Platform including the cryptographic library: CC EAL 5+ augmented with ALC_DVS.2 and AVA_VAN.5, claiming conformance to the Protection Profile "Bundesamt für Sicherheit in der Informationstechnik (BSI): Security IC Platform Protection Profile, Version 1.0, 15.06.2007; Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035". Certification number: BSI-DSZ-CC-0633-2010.

Embedded Software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager) and Native MIFARE application

- OS Name: JCOP 2.4.2 R3
- Product Identification: J3E081_M64, J3E081_M66 and J2E081_M64
- Evaluation Level CC EAL 5+ with ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2 according to Java Card System – Open Configuration Protection Profile, version 2.6, certified by ANSI,19.04.2010. Certification number: C13-37761.

SSCD applet – accomplishing the SSCD application and other applications

Applet Name: HTCNS

Applet Version: 1.03

SSCD application – implemented by an application profile

an ISO/IEC 7816-4 file system according to this ST.

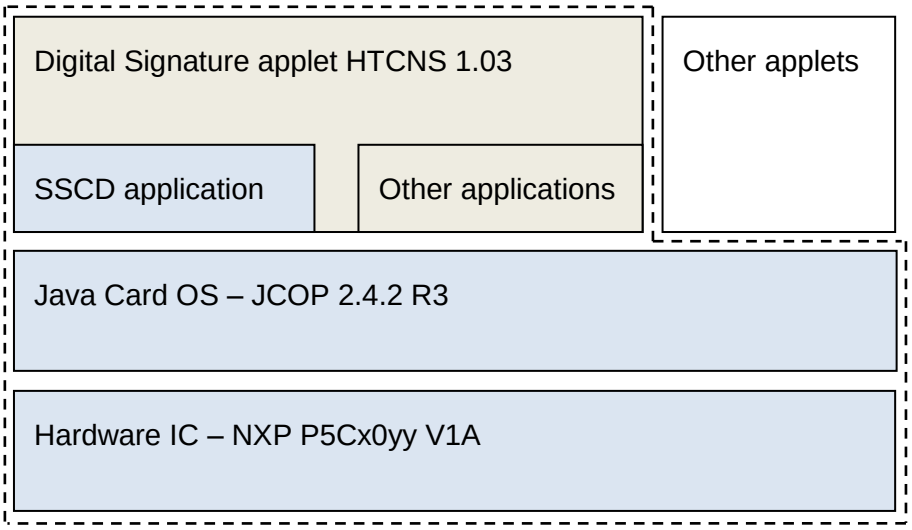


Figure 1 – TOE Boundaries

The product is compliant:

- with Java Card 3.0.1, excepting the following restrictions
- with Global Platform 2.2.1
- and with CNS – Carta Nazionale dei Servizi Functional Specification V1.1.6

The CNS File System profile is defined and documented as the Profile FileSystemCNS_21112005_with_DS_1.4 [15].

1.4.2 Operation of the TOE

The TOE is an SSCD which can work as a Type 3 SSCD which generates the Signature Creation Data.

The Composite part of the TOE is a digital signature applet (hereinafter referred to as the HTCNS applet) on a smart card IC having Java Card OS where the Java Card OS is masked in ROM and the digital signature applet loaded into EEPROM or can be masked in ROM also.

The Applet is linked to a card reader/writer (card terminal) via the HW and physical interfaces of the smart card. The smart card has contact type and contactless type interfaces.

The TOE may be applied to a contact type card reader/writer or to a contactless card reader/writer. The card reader/writer either is an intelligent device having the capability to use the TOE or it is connected to a computer such as a personal computer and allows application programs (APs) to use the TOE.

The contact type interface of the smart card is ISO/IEC 7816-3 compliant.

The contactless type interface of the smart card is ISO/IEC 14443 compliant.

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

The TOE is designed and produced in a secure environment.

The Operating System based on Java Card and Global Platform technology. Main responsibilities of the OS are:

- to provide interface between the IC and the applet
- to provide basic memory accessing and cryptographic services to the applet
- to provide functionalities for global management of the card (loading, installing and deleting applets) and ensure the security of the card (data integrity and physical attack counter-measures)
- the loading mechanism is prohibited after applet loading. Therefore no applet downloading can be performed after loading of the HTCNS applet

The applet is a high security product which provides the following services:

- a highly secure and configurable framework to store sensitive and user data, based on ISO/IEC 7816-4, ISO/IEC 7816-8 and ISO/IEC 7816-9
- trusted channel, based on CNS specification
- dynamic management of access control rules
- onboard RSA key pair generation (up to 2048 bits), compliant with ISO/IEC 7816-8
- all mandatory card services defined by CNS specification
- command interface is compliant with ISO/IEC 7816-4, and CNS specification
- symmetric device authentication based on CNS specification
- asymmetric device authentication based on CNS
- Card Holder verification based on PIN authentication
- RSA digital signature, compliant with ISO/IEC 7816-8

A functional overview of the TOE in its distinct operational environments:

— The preparation environment, where it interacts with a certification service provider through a certificate-generation application (CGA) to obtain a certificate for the signature verification data (SVD) corresponding with signature creation data (SCD) the TOE has generated. The TOE exports the SVD through a trusted channel allowing the CGA to check the authenticity of the SVD. The initialization environment interacts further with the TOE to personalize it with the initial value of

the reference-authentication data (RAD).

— The signing environment where it interacts with a signer through a signature-creation application (SCA) to sign data after authenticating the signer as its signatory. The signature-creation application provides the unique representation of data to be signed, thereof (DTBS/R) as input to the TOE signature-creation function and obtains the resulting digital signature. The TOE and the SCA communicate through a trusted channel to ensure the integrity of the DTBS respective DTBS/R.

— The management environments where it interacts with the user or an SSCD-Provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

The signing environment, the management environment and the preparation environment are secure and protect data exchanged with the TOE.

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case the TOE provides a function to identify each SCD and the SCA can provide an interface to the signer to select an SCD for use in the signature creation function of the SSCD. The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. The digital signature created by the TOE may be used to create an advanced electronic signature as defined in Article 5.1 of the directive[1]. Determining the state of the certificate as qualified is beyond the scope of this document.

The signature creation application is assumed to protect the integrity of the input it provides to the TOE signature creation function as being consistent with the user data authorized for signing by the signatory. Unless implicitly known to the TOE, the SCA indicates the kind of the signing input (as DTBS/R) it provides and computes any hash values required. The TOE may augment the DTBS/R with signature parameters it stores and then computes a hash value over the input as needed by the kind of input and the used cryptographic algorithm. The TOE and the SCA communicate through a trusted channel in order to protect the integrity of the DTBS/R.

The TOE stores signatory reference authentication data to authenticate a user as its signatory. The RAD is a password e.g. PIN, a biometric template or a combination of these. The TOE protects the confidentiality and integrity of the RAD. The TOE may provide a user interface to directly receive verification authentication data (VAD) from the user, alternatively, the TOE receive the VAD from the signature creation application.

A certification service provider and a SSCD-provisioning service provider interact with the TOE in the secure preparation environment to perform any preparation function of the TOE required before control of the TOE is given to the legitimate user. These functions may include:

- initializing the RAD,

- generating a key pair,

- storing personal information of the legitimate user.

The TOE and the CGA communicate through a trusted channel in order to protect the integrity and authenticity of the SVD exported from the TOE.

The TOE and the SCA communicate through a trusted channel to ensure the integrity of the DTBS respective DTBS/R.

1.4.3 TOE Definition

The TOE is a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD). The SSCD protects the SCD during its whole life cycle as to be used in a signature-creation process solely by its signatory.

The TOE provides the following functions:
(1) to generate signature-creation data (SCD) and the correspondent signature-verification data (SVD),
(2) to export the SVD for certification through a trusted channel to the CGA,
(3) to optionally, receive and store certificate info,
(4) to switch the TOE from a non-operational state to an operational state, and
(5) if in an operational state, to create digital signatures for data with the following steps:
  (a) select an SCD if multiple are present in the SSCD,
  (b) authenticate the signatory and determine its intent to sign,
  (c) receive the unique representation of data to be signed thereof (DTBS/R) through a trusted channel with SCA,
  (d) apply an appropriate cryptographic signature-creation function using the selected SCD to the DTBS/R.

The TOE may implement its function for digital signature creation to also conform to the specifications in ETSI TS 101 733 **(**CAdES**)** and ETSI TS 101 903 **(**XAdES**)**. In this case the TOE may provide additional supporting functions, e.g. to support receiving and/or validating a time stamp.

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

The TOE is prepared for the signatory's use by
(1) generating at least one SCD/SVD pair, and
(2) personalizing for the signatory by storing in the TOE:
  (a) the signatory's reference authentication data (RAD)
  (b) optionally, certificate info for at least one SCD in the TOE.

After preparation the SCD shall be in a non-operational state. Upon receiving a TOE the signatory shall verify its non-operational state and change the SCD state to operational.

After preparation the intended, legitimate user should be informed of the signatory's verification authentication data (VAD) required for use of the TOE in signing. If the VAD is a password or PIN, providing this information shall protect the confidentiality of the corresponding RAD. There is a special VAD, which can be used only once in the TOE lifetime, the Transport PIN, which has to be changed to Signature PIN in order to create digital signatures.

If continued use of an SCD is no longer required the TOE will disable an SCD it holds, e.g. by erasing it from memory.

1.4.4 TOE life cycle

1.4.4.1 General

The TOE life cycle below distinguishes stages for development, production, preparation and operational use. The development and production of the TOE (cf. CC part 1, para.139) together constitute the development phase of the TOE. The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class. The development phase ends with the delivery of the TOE to an SSCD-provisioning service provider. The functional integrity of the TOE shall be protected in delivering it to an SSCD-provisioning service provider.

The TOE operational use stage begins when the signatory performs the TOE operation to enable it for use in signing operations. Enabling the TOE for signing requires at least one key stored in its memory. The TOE life cycle ends when all keys stored in it have been rendered permanently unusable. Rendering a key in the SSCD unusable may include deletion of the any stored corresponding certificate info.

The Applet and the card together can only be interpreted as the TOE of this Security Target, if the Applet loaded on to the card Platform is instantiated by the correct methods described in

the Administrators Guide [13] and also configured using the correct profile, which is described in the Initialization and Configuration documentation [14]. This can be evaluated by a series of GET DATA command on the TOE data described in the User's Guide [12].

1.4.4.2 Preparation stage

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

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

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

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

Data required for inclusion in the SVD certificate at least includes ([1] **Annex** II):

(a) the SVD which correspond to SCD under the control of the signatory;
(b) the name of the signatory or a pseudonym, which is to be identified as such;
(c) an indication of the beginning and end of the period of validity of the certificate.

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

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

(1) establishing the sender as genuine SSCD
(2) establishing the integrity of the SVD to be certified as sent by the originating SSCD,
(3) establishing that the originating SSCD has been personalized for the legitimate user,
(4) establishing correspondence between SCD and SVD, and
(5) an assertion that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

The proof of correspondence between an SCD stored in the TOE and an SVD may be implicit in the security mechanisms applied by the CGA. Optionally, the TOE may support a function to provide an explicit proof of correspondence between an SCD it stores and an SVD realized by self-certification. Such a function may be performed implicitly in the SVD export function

and may be invoked in the preparation environment without explicit consent of the signatory[1].

Prior to generating the certificate the certification service provider shall assert the CNS of the signatory specified in the certification request as the legitimate user of the TOE.

1.4.4.3 Operational use stage

The operational phase of the Type 3 TOE starts when at least one SCD/SVD pair is generated, and when the signatory takes control over the TOE and makes the SCD operational. The signatory uses the TOE with a trustworthy SCA in a secured environment only. The SCA is assumed to protect the DTBS/R during the transmission to the TOE.

In this lifecycle stage the signatory can use the TOE to create advanced/qualified electronic signatures.

The signatory can also interact with the SSCD to perform management tasks, e.g. reset a RAD value or use counter if the password/PIN in the reference data has been lost or blocked. Such management tasks require a secure environment.

The signatory can render an SCD in the TOE permanently unusable. Rendering the last SCD in the TOE permanently unusable ends the life of the TOE as SSCD.

The TOE may support functions to generate additional signing keys. If the TOE supports these functions it shall support further functions to securely obtain certificates for the new keys. For an additional key the signatory may be allowed to choose the kind of certificate (qualified, or not) to obtain for the SVD of the new key. The signatory may also be allowed to choose some of the data in the certificate request for instance to use a pseudonym instead of the legal name in the certificate[2]. If the conditions to obtain a qualified certificate are met the new key can also be used to create advanced electronic signatures. The optional TOE functions for additional key generation and certification may require additional security functions in the TOE and an interaction with the SSCD-Provisioning service provider in an environment that is secure.

In the usage phase, SCD/SVD generation by the TOE and SVD export from the TOE may take place in the preparation stage and/or in the operational use stage. The TOE then provides a trusted channel to the CGA protecting the integrity of the SVD.

The TOE life cycle as SSCD ends when all SCD stored in the TOE are destructed. This may include deletion of the corresponding certificates.

1.4.5 TOE security functions

The following TOE ensured security functions are the most significant for its operational use:

Only entities possessing authorization can get access to the use of the signature creation data stored on the TOE and use functionality of card,

Verifying authenticity and integrity as well as securing confidentiality of data in the communication channel between the TOE and the entity connected,

Self-protection of the TOE security functionality and the data stored inside.

---

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

[2] The certificate request in this case will contain the name of the signatory as the requester, as for instance it may be signed by the signatory's existing SCD.

These are described below informally, and in detail in section 7.1.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target is conforming to the Common Criteria Part 1 version 3.1 Revision 4 [2]

This Security Target is conforming to Common Criteria Part 2 version 3.1 Revision 4 [3] extended.

This Security Target is conforming to the Common Criteria Part 3 version 3.1 Revision 4 [4].

2.2 PP Claim, Package Claim

This Security Target claims strict conformance to the following PP:

- Protection profiles for Secure signature creation device — Part 2: Device with key generation, BSI-CC-PP-0059 version 2.01 [5]

This ST is conforming to assurance package EAL4 augmented with AVA_VAN.5 defined in CC part 3 [4].

2.3 Conformance rationale

The ST is built on the PP-s referenced above, which according to the certifications conform to the CC version stated above.

This ST is conformant with Common Criteria Part 2 [3] extended due to additional components as stated in Protection Profile BSI-CC-PP-0059 version 2.01 [5].

This ST is conformant to Common Criteria Part 3 [4].

The current ST refines the Assets, threats, objectives and SFR of BSI-CC-PP-0059 version 2.01 [5].

The Security Target claims **strict conformance** to one PP: Protection Profile BSI-CC-PP-0059 version 2.01 [5].

The Target of Evaluation (TOE) is Secure Signature Creation Device (SSCD) for the generation of signature-creation data (SCD) and the creation of qualified electronic signatures. It fulfils requirements of directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a community framework for electronic signatures. [1] The Security Target refers to the SSCD compliant configurations of the HTCNS applet. The HTCNS applet is a Java Card Application used exclusively on the NXP JCOP 2.4.2. R3 Platform, which is a CC EAL5+ certified product.

The TOE is thus **consistent** with the **TOE type** in the PP.

The **security problem definition** of this security target is **consistent** with the statement of the security problem definition in the PP, as the security target claims strict conformance to the PP and no other threats. There is one added assumption, **A.Sec_Manufac**. It does not

affect the strict conformance.

The **security objectives** of the TOE of this security target are **consistent** with the statement of the security objectives in the PP as the security target claims strict conformance to the PP. There are two security objectives added, **OT.TOE_TC_SVD_Exp** (Trusted channel for SVD), and **OT.TOE_TC_DTBS_Imp** (Trusted channel for DTBS). These security objectives do not affect the strict conformance.

The **security objectives** for the operational environment in this security target include all security objectives for the oprational environment from the PP, except OE.DTBS_Protect. This ST adapts OE.DTBS_Protect to the support provided by the TOE by the security functionality (cf. OT.TOE_TC_DTBS_Imp) provided by the TOE and changes it into OE.SCA_TC_DTBS_Exp. There is one objective added, **OE.CGA_TC_SVD_Imp.** These security objectives do not affect the strict conformance.

The **security requirements** of this security target are **consistent** with the statement of the security requirements in the PP as the security target claims strict conformance to the PP. There are the following SFRs added in this security target: **FDP_DAU.2/SVD, FTP_ITC.1/SVD, FDP_UIT.1/DTBS and FTP_ITC.1/DTBS**

2.4 Statement of compatibility

2.4.1 Security Functionalities

The following table contains the security functionalities of the Platform ST and of this ST, showing which Functionality correspond to the Platform ST and which has no correspondence. This statement is compliant to the requirements of [11].

A classification of TSFs of the Platform-ST has been made. Each TSF has been classified as ‘relevant’ or ‘not relevant’ for this ST

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant	Not relevant	Remarks
SF.AccessControl	TSF.AccessControl	X		enforces the access control
SF.Audit	TSF.Platform	X		Audit functionality
SF.CryptoKey	TSF.Crypto	X		Cryptographic key management
SF.CryptoOperation	TSF.Platform, TSF.Crypto Creation	X		Cryptographic operation Used by calling Platform Security Functionalities
SF.I&A	TSF.IdentificationAndAuthentication	X		Identification and authentication
SF.SecureManagement	TSF.Platform	X		Secure management of TOE resources

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant	Not relevant	Remarks
SF.PIN	TSF.AccessControl	X		PIN management Used by calling Access Control TSF
SF.LoadIntegrity	-		X	Package integrity check
SF.Transaction	-		X	Transaction management
SF.Hardware	TSF.Platform	X		TSF of the underlying Platform Used by calling Platform Security Functionalities
SF.CryptoLib	TSF.Platform	X		TSF of the certified crypto library Used by calling Platform Security Functionalities

Table 1 Classification of Platform-TSFs

All listed TSFs of the Platform-ST are relevant for this ST.

Application note 1 (by the ST author) The TSF.Platform Security functionality in the above list represents functionalities which are not directly used in the HTCNS Applet, they are implicitly invoked by calls to the Platform, respectively the JCOP operating system. These functions are called altogether as TSF.Platform.

2.4.1.1 Threats

The following threats of this ST are directly related to JCOP Platform functionality:

- T.Hack_Phys
- T.SCD_Divulg
- T.SVD_Forgery

These threats will be mapped to the following Platform-ST threats:

- T.PHYSICAL
- T.CONFID-APPLI-DATA
- T.SID.1

The following table shows the mapping of the threats.

This ST		T.SCD_Divulg	T.Hack_Phys	T.SVD_Forgery
Platform ST	T.PHYSICAL		X	
	T.CONFID-APPLI-DATA	X		
	T.SID.1			X

Table 2 Mapping of Threats

The T.Hack_Phys matches to T.PHYSICAL, as physical TOE interfaces like emanations, probing, environmental stress and tampering are used to exploit vulnerabilities.

T.SVD_Forgery matches T_SID.1, because both are about identity usurpation.

T.SCD_Divulg matches T.CONFID-APPLI-DATA as physical TOE interfaces like emanations, probing, environmental stress and tampering could be used to exploit exploit information leaking from the TOE during its usage in order to disclose confidential SCD data.

The following threats:

- T.SEC_BOX_BORDER
- T.OS_OPERATE
- T.RND
- T.INTEG-APPLI-CODE.LOAD
- T.INTEG-APPLI-DATA
- T.INTEG-APPLI-DATA.LOAD
- T.INSTALL
- T.RESOURCES T.CONFID-JCS-CODE
- T.CONFID-JCS-DATA
- T.DELETION
- T.EXE-CODE.1
- T.EXE-CODE.2
- T.EXE-CODE-REMOTE
- T.INTEG-APPLI-CODE
- T.INTEG-JCS-CODE
- T.INTEG-JCS-DATA
- T.NATIVE
- T.OBJ-DELETION
- T.SID.2

have no correspondence to the threats of this ST. They are assessed, and found that there is also no contradiction related to this ST.

2.4.2 OSPS

None of the OSPs of this ST are applicable to the JCOP Platform and therefore not mappable for the Platform-ST.

The OSP-s from the Platform ST OSP.VERIFICATION and OSP.PROCESS-TOE does not

deal with any additional security components.

2.4.3 Assumptions

The Assumptions of the Platform ST are categorized according to the [11], as IrPA, CfPA and SgPA. There is also a comment column with respective remarks.

Assumption	Classification of assumptions	Comment
A.APPLET	CfPA	The Java Card specification explicitly "does not include support for native methods" ([21], §3.3) outside the API.
A.VERIFICATION	CfPA	The OT.Lifecycle_Security fulfils the Assumption.
A.USE_DIAG	SgPA	OT.SCD_Secrecy OT.SCD_Unique OT.SCD_SVD_Corresp, OE.CGA_Qcert, OT.TOE_TC_SVD_Exp, OT.TOE_TC_DTBS_Imp, OE.CGA_TC_SVD_Imp, OE.SCA_TC_DTBS_Exp and OE.HID_VAD provides the necessary ensurance.
A.USE_KEYS	CfPA	The objective OE.SVD_Auth covers this assumption.
A.PROCESS-SEC-IC	SgPA	The assumption A.Sec_Manufac and the related objective OE.Sec_Manufac covers this assumption.

Table 3 Mapping of assumptions

A.Sec_Manufac of this ST is included to assume that the Platform arrives to the user with correctly working functions. This have no contradiction to the Platform ST.

In case of SgPA Assumptions, the assumptions are fulfilled when all the requirements belonging to the listed objective are conformant.

2.4.4 Security objectives

These Platform-ST objectives can be mapped to this STs objectives as shown in the following table.

Objective from the Platform ST	Objective from this ST
OT.CIPHER	OT.Sig_Secure
OT.SCP.IC	OT.Tamper_ID, OT.EMSEC_Design
OT.RND	OT.SCD_Unique
OT.KEY-MNGT	OT.SCD/SVD_Auth_Gen, OT.SCD/SVD_Auth_Gen, OT.SCD_SVD_Corresp, OT.Sig_Secure
OT.PIN-MNGT	OT.Sigy_SigF

Table 4 Mapping of security objectives for the TOE

The following Platform-ST objectives are not relevant for or cannot be mapped to the TOE of this ST:

- OT.IDENTIFICATION
- OT.SCP.RECOVERY
- OT.EXT-MEM
- OT.FIREWALL
- OT_SID
- O.CARD-MANAGEMENT
- OT.INSTALL
- OT.TRANSACTION
- OT.NATIVE
- OT.REMOTE
- OT.OBJ-DELETION
- OT.DELETION
- OT.SEC_BOX_FW
- OT.GLOBAL_ARRAYS_INTEG
- OT.GLOBAL_ARRAYS_CONFID
- OT.REALLOCATION
- OT.RESOURCES
- OT.ALARM
- OT.OPERATE
- OT.MF_FW
- OT.LOAD
- OT.SCP.SUPPORT

cannot be mapped because these are out of scope.

The objectives for the operational environment can be mapped as follows:

Objective from the Platform ST	Objective from this ST
OE.USE_DIAG	OE.HID_VAD, OE.CGA_TC_SVD_Imp, OE.SCA_TC_DTBS_Exp
OE.USE_KEYS	OE.HID_VAD, OE.CGA_TC_SVD_Imp, OE.SCA_TC_DTBS_Exp
OE.PROCESS_SEC_IC	OE.Sec_Manufac
OE.APPLET	OT.Lifecycle_Security
OE.VERIFICATION	OT.Lifecycle_Security, OE.Sec_Manufac

Table 5 Mapping of security objectives of the environment

There is no conflict between security objectives of this ST and the Platform-ST.

2.4.5 Security requirements

The Security Requirements of the Platform ST can be mapped as follows:

Platform SFR	Corresponding TOE SFR	Remarks
FDP_ACC.2/FIREWALL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/FIREWALL	No Correspondence	Out of scope (Platform functionality)

Platform SFR	Corresponding TOE SFR	Remarks
		No contradiction to this ST
FDP_IFC.1/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_IFF.1/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/OBJECTS	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/JCRE	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.2/FIREWALL_JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/FIREWALL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMR.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCS_CKM.1	FCS.CKM.1	The FCS_CKM.1.1 corresponds to the FCS_CKM.1 requirement of the Platform since they contain overlapping requirements.
FCS_CKM.2	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCS_CKM.3	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCS_CKM.4	FCS_CKM.4	The requirements are equivalent (physically overwriting the keys with zeros).
FCS_COP.1	FCS_COP.1	FCS_COP.1 of the Platform matches the equivalent SFR of the TOE.
FDP_RIP.1/ABORT	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/APDU	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/bArray	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST

Platform SFR	Corresponding TOE SFR	Remarks
FDP_RIP.1/KEYS	FDP_RIP.1	FDP_RIP.1 matches the equivalent SFR of the Platform-ST.
FDP_RIP.1/TRANSIENT	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ROL.1/FIREWALL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FAU_ARP.1	FPT_PHP.1 FPT_PHP.3 FPT_TST.1	The Security Alarms requirement FAU_ARP.1 of the Platform corresponds to the FPT_PHP.1, FPT_PHP.3 and FPT_TST.1 of this ST about physical resistance.
FDP_SDI.2	FDP_SDI.2/Persistent FDP_SDI.2/DTBS	The FDP_SDI.2 requirement corresponds to the same requirement, meaning that the integrity is checked by the Platform.
FPR_UNO.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1	FPT_FLS.1	FPT_FLS.1 matches to the equivalent SFR of the Platform-ST.
FPT_TDC.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_ATD.1/AID	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_UID.2/AID	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_USB.1/AID	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MTD.1/JCRE	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
MT_MTD.3/JCRE	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ITC.2/Installer	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMR.1/Installer	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/Installer	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_RCV.3/Installer	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.2/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/ADEL	No Correspondence	Out of scope (Platform functionality)

Platform SFR	Corresponding TOE SFR	Remarks
		No contradiction to this ST
FDP_RIP.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMR.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.2/JCRMI	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.2.2/JCRMI	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/JCRMI	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/ODEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/ODEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCO_NRO.2/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_IFC.2/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_IFF.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_UIT.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_UID.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMR.1/CM	No Correspondence	Out of scope (Platform functionality)

Platform SFR	Corresponding TOE SFR	Remarks
		No contradiction to this ST
FTP_ITC.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FRU_FLT.2/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_PHP.3/SCP	FPT_PHP.3	The FPT_PHP.3 of this ST matches the FPT_PHP.3/SCP of the Platform ST.
hFDP_ACC.1/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.1/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_AFL.1/PIN	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FTP_ITC.1/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FAU_SAS.1/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCS_RNG.1	FCS_CKM.1	Out of scope (Platform functionality)

Platform SFR	Corresponding TOE SFR	Remarks
		No contradiction to this ST
FCS_RNG.1/RNG2	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_EMSEC.1	FPT_EMS.1	FPT_EMS.1 matches the FPT_EMSEC.1 of the Platform-ST
FDP_ACC.2/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST

Table 6 Mapping of Security requirements

2.4.6 Assurance requirements

This ST requires EAL 4 according to Common Criteria V3.1 R3 augmented by AVA_VAN.5.

The Platform-ST requires EAL 5 according to Common Criteria V3.1 R3 augmented by: ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2.

As EAL 5 covers all assurance requirements of EAL 4 all non-augmented parts of this ST will match to the Platform-ST assurance requirements.

2.5 Analysis

Overall there is no conflict between security requirements of this ST and the Platform-ST.

3 Security Problem Definition

3.1 Assets, users and threat agents

The Common Criteria define assets as entities that the owner of the TOE presumably places value upon. The term “asset” is used to describe the threats in the operational environment of the TOE.

Assets and objects:

1. 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.

2. 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.

3. DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the digital signature must be maintained.

User and subjects acting for users:

1. User: End user of the TOE who can be identified as Administrator or Signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

2. Administrator: User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.

3. Signatory: User who hold the TOE and use it on his own behalf or on behalf of the natural or legal person or entity They represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

Threat agents:

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

3.2 Threats

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

An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature creation in the TOE.

T.SCD_Derive *Derive the signature creation data*

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

T.Hack_Phys *Physical attacks through the TOE interfaces*

An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

T.SVD_Forgery *Forgery of the signature verification data*

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

T.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.DTBS_Forgery *Forgery of the DTBS/R*

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

T.Sig_Forgery *Forgery of the electronic signature*

An attacker forges a signed data object, maybe using an electronic signature which has been 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 created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

3.3 Organizational Security Policies

P.CSP_QCert *Qualified certificate*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. **the directive**, article 2, clause 9, and Annex **I**) for the SVD generated by the SSCD. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

P.QSign *Qualified electronic signatures*

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. **the directive**, article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to **the directive** Annex I)[3]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic 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 meets the requirements for an SSCD laid down in **Annex** III of **the directive** [1]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

P.Sig_Non-Repud *Non-repudiation of signatures*

The life cycle of the SSCD, the SCD and the SVD shall be implemented in a way that the

[3] It is a non-qualified advanced electronic signature if it is based on a non-qualified certificate for the SVD.

signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

3.4 Assumptions

A.CGA *Trustworthy certification generation application*

The CGA protects the authenticity of the signatory's name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

A.SCA *Trustworthy signature creation application*

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

The ST contains other Assumptions, not in defined in the PP, justified by the fact that the TOE is divided to two parts. The TOE Part I. is developed by NXP at the NXP sites, which are already certified at the EAL5+ assurance level.

A.Sec_Manufac Protection during ROM-coding, Packaging, and JCOP Personalization

It is assumed that security procedures are used correctly by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

4 Security Objectives

4.1 Security Objectives for the TOE

OT.Lifecycle_Security *Lifecycle security*

The TOE shall detect flaws during the initialization, personalization and operational usage. The TOE shall securely destroy the SCD on demand of the signatory

Application note 2 (Application Note 1 from [5]): The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

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

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

OT.SCD_Unique *Uniqueness of the signature creation data*

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation shall practically occur only once and shall not be reconstructable from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible.

OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*

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

OT.SCD_Secrecy *Secrecy of the signature creation data*

The secrecy of an SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential.

Application note 3 (Application Note 2 from [5]): The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and by destruction.

OT.Sig_Secure *Cryptographic security of the electronic signature*

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

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

The TOE shall provide the digital signature creation 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.DTBS_Integrity_TOE DTBS/R integrity inside the TOE

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

OT.EMSEC_Design *Provide physical-emanation security*

The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

OT.Tamper_ID *Tamper detection*

The TOE shall provide system features that detect physical tampering of its components, and uses those features to limit security breaches

OT.Tamper_Resistance *Tamper resistance*

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

OT.TOE_TC_SVD_Exp *TOE Trusted channel for SVD export*

The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the TOE.

OT.TOE_TC_DTBS_Imp *Trusted channel of TOE for DTBS import*

The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE must not generate electronic signatures with the SCD for altered DTBS.

Application note 4: This security objective for the TOE is partly covering OE.DTBS_Protect. While OE.DTBS_Protect requires only the operational environment to protect DTBS, this requirement requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore this requirement re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

4.2 Security Objectives for the Operational Environment

OE.SVD_Auth *Authenticity of the SVD*

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

OE.CGA_QCert *Generation of qualified certificates*

The CGA shall generate a qualified certificate that includes(amongst others)

(a) the name of the signatory controlling the TOE,
(b) the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
(c) the advanced signature of the CSP.

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

OE.SSCD_Prov_Service *Authentic SSCD provided by SSCD-provisioning service*

The SSCD-provisioning service shall initialize and personalize for the signatory an authentic copy of the TOE and deliver this copy as SSCD to the signatory.

OE.HID_VAD *Protection of the VAD*

If an external device provides the human interface for user authentication, this device shall

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

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

The signatory shall use a trustworthy SCA that

- 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.

Application note 5 (Application Note 3 from [5]): The SCA should be able to support advanced electronic signatures. Currently, there exist three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CAdES, XAdES and PAdES. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.

OE.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 shall keep their VAD confidential

OE.Sec_Manufac *Protection during ROM-coding, Packaging, JCOP Personalization*

An Environmental Objective is that security procedures are used correctly by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

OE.CGA_TC_SVD_Imp CGA trusted channel for SVD import

The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the SSCD.

OE.SCA_TC_DTBS_Exp *Trusted channel of SCA for DTBS export*

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

Application note 6: This security objective for the environment is partly covering OE.DTBS_Protect. While OE.DTBS_Protect requires only the operational environment to protect DTBS, this requirement requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore this requirement re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

4.3 Security Objectives Rationale

4.3.1 Security Objectives Backtracking

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_SVD_Exp	OT.TOE_TC_DTBS_Imp	OE.CGA_Qcert	OE.SVD_ Auth	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.Signatory	OE.Sec-Manufac	OE.CGA_TC_SVD_Imp	OE.SCA_TC_DTBS_Exp
T.SCD_Divulg					X																	
T.SCD_Derive		X				X																
T.Hack_Phys					X				X	X	X											
T.SVD_Forgery				X								X			X						X	
T.SigF_Misuse	X						X	X					X				X	X	X			X
T.DTBS_Forgery								X					X					X				X
T.Sig_Forgery			X			X								X								
P.CSP_Qcert	X			X										X								
P.Qsign						X	X							X				X				
P.Sigy_SSCD	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
A.CGA														X	X							
A.SCA																		X				
A.Sec-Manufac																				X		

Table 7 Mapping of security problem definition to security objectives

4.3.2 Security Objectives Sufficiency

4.3.2.1 Countering of threats by security objectives

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 Directive**. This threat is countered by OT.SCD_Secrecy, which assures the secrecy of the SCD used for signature creation.

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_Auth_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD-pair. OT.Sig_Secure ensures cryptographically secure electronic 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 for the generation of the certificate. T.SVD_Forgery is addressed by OT.SCD_SVD_Corresp, which ensures 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 and verification of 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. Additionally T.SVD_Forgery is addressed by OT.TOE_TC_SVD_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA_TC_SVD_Imp, which provides verification of SVD authenticity by the CGA.

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 an electronic signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of Annex III. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialization, personalization 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. The combination of OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission from the SCA to 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 their VAD confidential.

T.DTBS_Forgery (*Forgery of the DTBS/R***)** addresses the threat arising from modifications of the DTBS/R sent to the TOE for signing which than does not correspond to the DTBS/R corresponding to the DTBS the signatory intends to sign. The threat T.DTBS_Forgery is addressed by the security objectives OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS), which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE. The TOE counters internally this threat by the means of OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensuring the integrity of the DTBS/R inside the TOE. The TOE IT environment also 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.

T.Sig_Forgery (*Forgery of the electronic signature***)** deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique and OE.CGA_Qcert address this threat in general. OT.Sig_Secure (*Cryptographic security of the electronic signature*) ensures by means of robust cryptographic techniques that the signed data and the electronic 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 concerning a forged signature.

4.3.2.2 Enforcement of OSPs by security objectives

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

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialization, personalization and operational usage,
- OT.SCD_SVD_Corresp, which requires to ensure the correspondence between the SVD and the SCD during their generation,
- 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 creation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE creates electronic signatures, which 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. 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 creation can practically occur only once;
- OT.SCD_Unique, OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(a) of Annex III by the requirements to ensure secrecy of the SCD. OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of the SCD against specific attacks;
- OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE;
- OT.Sigy_SigF meets the requirement in paragraph 1(c) of Annex III by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others;
- OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of Annex III as the TOE must not alter the DTBS/R.
- The CSP will use the TOE security feature (addressed by the security objective OT.TOE_TC_SVD_Exp) to check whether the received SVD is sent by this SSCD as required by OE.CGA_TC_SVD_Imp. Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

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

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

- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialization, personalization and operational usage,
- OT.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorized users only, and
- OT.Sigy_SigF, which requires the TOE to provide the signature creation function for

the legitimate signatory only and to protect the SCD against the use of others.

OE.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, initialized and personalized 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 their 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 ensures the aspects of signatory's sole control over and responsibility for the electronic signatures created with the TOE.

OE.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, initialized and personalized as SSCD from the SSCD-provisioning service.

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.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 their VAD confidential. OE.DTBS_Intend (SCA sends data intended to be signed), OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE), OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) and OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) ensure that the TOE creates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure (Cryptographic security of the electronic signature) ensure that only this SCD may create a valid electronic 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.

The TOE security feature addressed by the security objective OT.TOE_TC_SVD_Exp enables the verification whether the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA_TC_SVD_Imp.

4.3.2.3 Upkeep of assumptions by security objectives

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 of the data that have 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 of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

Also adding to the rationale the additional assumption (**A.Sec_Manufac)** covers the periods of the lifecycle of the TOE where it is in the influence of the Manufacturer, NXP. The

A.Sec_Manufac assumptions can be mapped to the respective objective OE.Sec_Manufac.

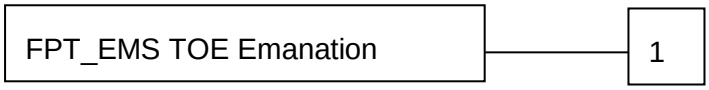
5 Extended Component Definition

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation. The definition of the family FPT_EMS is taken from the *Protection Profile Secure Signature Creation Device* [5].

FPT_EMS TOE Emanation

Family behaviour: This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMS.1 TOE Emanation has two constituents:

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMS.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1 There are no management activities foreseen.

Audit: FPT_EMS.1 There are no actions identified that must be auditable if **FAU_GEN** (*Security audit data generation*) is included in a protection profile or security target.

FPT_EMS.1 *TOE Emanation*

Hierarchical to: No other components

Dependencies: No dependencies.

FPT_EMS.1.1

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

FPT_EMS.1.2

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

6 Security Requirements

6.1 TOE Security Functional Requirements

6.1.1 Use of requirement specifications

Common Criteria allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration.* Each of these operations is used in this ST and the underlying PP. The footnotes in this ST indicate the operations of the PP and the ST as well.

A **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is either (i) denoted by the word "refinement" in **bold** text and the added or changed words are in bold text, or (ii) included in text as **bold** text and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

A **selection** operation is used to select one or more options provided by the CC or the underlying PP in stating a requirement. A selection that has been made is indicated as underlined text and the original text of the component is given by a footnote.

An **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment that that has been made is indicated as double underlined text and the original text of the component is given by a footnote.

An **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

6.1.2 Cryptographic support (FCS)

Application note 7 (Application Note 4 from [5]): Member states of the European Union have specified entities as responsible for accreditation and supervision of the evaluation process for products conforming to this standard and for determining admissible algorithms and algorithm parameters (The Directive: 1.1b and 3.4).

FCS_CKM.1 *Cryptographic key generation* (from [5])

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate an **SCD/SVD** pair in accordance with a specified cryptographic key generation algorithm RSA or RSA CRT[4] and specified cryptographic key sizes 1976-2048 bits[5] that meet the following:[17] [6]

Application note 8 (Application Note 5 from [5]): Applied.

Application note 9 (by the ST author): The underlying Platform supports RSA and RSA-CRT generation algorithms and cryptographic key sizes 512 bits to 2048 bits with equal security measures. However, to fend off attackers with high attack potential an adequate key

[4] [assignment: *cryptographic key generation algorithm*]
[5] [assignment*: cryptographic key sizes*]
[6] [assignment*: list of standards*]

length must be used.

FCS_CKM.4 *Cryptographic key destruction* (from [5])

Hierarchical to: No other components.

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

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting of memory[7] that meets the following: none.[8]

Application note 10 (Application Note 6 from [5]): Applied.

FCS_COP.1 *Cryptographic operation* (from [5])

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

The TSF shall perform digital signature creation[9] in accordance with a specified cryptographic algorithm RSA or RSA CRT with PKCS#1v1.5 1976-2048 bits[10,11] that meet the following: [17][12].

Application note 11 (Application Note 7 from [5]): Applied.

Application note 12 (by the ST author): The underlying Platform supports RSA and RSA-CRT digital signature algorithms and cryptographic key sizes 512 bits to 2048 bits with equal security measures. However, to fend off attackers with high attack potential an adequate key length must be used.

6.1.3 User data protection (FDP)

The security attributes and related status for the subjects and objects are:

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin – S.User acts as S.Admin R.Sigy – S.User acts as S.Sigy
S.User	SCD/SVD Management	authorized, not authorized

[7] [assignment: *cryptographic key destruction method*]
[8] [assignment: *list of standards*]
[9] [assignment: list of cryptographic operations]
[10] [assignment: *cryptographic algorithm*]
[11] [assignment: *cryptographic key sizes*]
[12] [assignment: *list of standards*]

SCD	SCD Operational	no, yes
SCD	SCD Identifier	arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

Table 8 Subjects and security attributes for access control

Application note 13 (Application Note 8 from [5]): Applied.

FDP_ACC.1/Signature_Creation *Subset access control* (from [5])

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Signature_Creation

The TSF shall enforce the Signature Creation SFP[13] on

(1) subjects: S.User,

(2) objects: DTBS/R, SCD,

(3) operations: signature creation.[14]

FDP_ACC.1/SCD/SVD_Generation *Subset access control* (from [5])

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/SCD/SVD_Generation

The TSF shall enforce the SCD/SVD_Generation_SFP[15] on

(1) subjects: S.User,

(2) objects: SCD, SVD,

(3) operations: generation of SCD/SVD pair[16]

FDP_ACF.1/SCD/SVD_Generation *Security attribute based access control* (from [5])

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/SCD/SVD_Generation

The TSF shall enforce the SCD/SVD_Generation_SFP[17] to objects based on the following: the user S.User is associated with the security attribute "SCD / SVD Management"[18].

[13] [assignment: *access control SFP*]
[14] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[15] [assignment: *access control SFP*]
[16] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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 “authorized” is allowed to generate SCD/SVD pair[19]

FDP_ACF.1.3/SCD/SVD_Generation

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[20].

FDP_ACF.1.4/ SCD/SVD_Generation

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

S.User with the security attribute “SCD / SVD management” set to “not authorized” is not allowed to generate SCD/SVD pair[21].

FDP_ACC.1/SVD_Transfer *Subset access control* (from [5])

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/SVD_Transfer

The TSF shall enforce the SVD_Transfer_SFP[22] on

(1) subjects: S.User,

(2) objects: SVD

(3) operations: export[23].

FDP_ACF.1/SVD_Transfer *Security attribute based access control* (from [5])

Hierarchical to: No other components.

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

FDP_ACF.1.1/SVD_Transfer

The TSF shall enforce the SVD_Transfer_SFP[24] to objects based on the following:

(1) the S.User is associated with the security attribute Role,

(2) the SVD [25].

---

[17] [assignment: *access control SFP*]
[18] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[19] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[20] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[21] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[22] [assignment: *access control SFP*]
[23] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[24] [assignment: *access control SFP*]

FDP_ACF.1.2/SVD_Transfer

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [R.Admin], [R.Sigy][26] is allowed to export SVD[27].

FDP_ACF.1.3/SVD_Transfer

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[28].

FDP_ACF.1.4/SVD_Transfer
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[29].

Application note 13 (Application Note 9 from [5]): Applied.

FDP_ACF.1/Signature-creation *Security attribute based access control* (from [5])

Hierarchical to: No other components.

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

FDP_ACF.1.1/Signature-creation

The TSF shall enforce the Signature-creation_SFP[30] to objects based on the following:

(1) the user S.User is associated with the security attribute "Role" and

(2) the SCD with the security attribute "SCD Operational"[31].

FDP_ACF.1.2/Signature-creation

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

R.Sigy is allowed to create digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes"[32].

FDP_ACF.1.3/Signature-creation

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[33].

FDP_ACF.1.4/Signature-creation

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

---

[25] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[26] [selection: R.Admin, R.Sigy]
[27] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]].
[28] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]
[29] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[30] [assignment: *access control SFP*]
[31] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[32] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[33] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

S.User is not allowed to create digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no"[34].

FDP_DAU.2/SVD Data Authentication with Identity of Guarantor

Hierarchical to: FDP_DAU.1 Basic Data Authentication

Dependencies: FIA_UID.1 Timing of identification

FDP_DAU.2.1/SVD

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of SVD[35].

FDP_DAU.2.2/SVD

The TSF shall provide CGA[36] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

FDP_RIP.1 *Subset residual information protection* (from [5])

Hierarchical to: No other components.

Dependencies: No dependencies.

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[37] the following objects: SCD[38].

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

1. SCD

2. SVD (if persistently stored by the TOE).

The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data":

FDP_SDI.2/Persistent *Stored data integrity monitoring and action* (from [5])

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies

FDP_SDI.2.1/Persistent

The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[39] on all objects, based on the following attributes: integrity checked stored data[40].

FDP_SDI.2.2/Persistent

Upon detection of a data integrity error, the TSF shall

(1) prohibit the use of the altered data

[34] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[35] [assignment: list of objects or information types]
[36] [assignment: list of subjects]
[37] [selection: *allocation of the resource to, deallocation of the resource from*]
[38] [assignment: *list of objects*]
[39] [assignment: *integrity errors*]
[40] [assignment: *user data attributes*]

(2) inform the S.Sigy about integrity error[41].

FDP_SDI.2/DTBS *Stored data integrity monitoring and action* (from [5])

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/DTBS

The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[42] on all objects, based on the following attributes: integrity checked stored DTBS[43].

FDP_SDI.2.2/DTBS

Upon detection of a data integrity error, the TSF shall

(1) prohibit the use of the altered data

(2) inform the S.Sigy about integrity error[44].

Application note 14 (Application Note 10 from [5]): Applied.

Application note 15 (by the ST author): There is no stored DTBS in the TOE, because the card only receives and immediately signs hash (DTBS/R), not the DTBS.

FDP_UIT.1/DTBS Data exchange integrity

Hierarchical to: No other components.

Dependencies:

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

FDP_UIT.1.1/DTBS

The TSF shall enforce the Signature Creation SFP[45] to receive[46] user data in a manner protected from modification and insertion[47] errors.

FDP_UIT.1.2/DTBS

The TSF shall be able to determine on receipt of user data, whether modification and insertion[48] has occurred.

6.1.4 Identification and authentication (FIA)

FIA_UID.1 *Timing of identification* (from [5])

Hierarchical to: No other components.

Dependencies: No dependencies.

---

[41] [assignment: *action to be taken*]
[42] [assignment: *integrity errors*]
[43] [assignment: *user data attributes*]
[44] [assignment: *action to be taken*]
[45] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[46] [selection: *transmit, receive*]
[47] [selection: modification, deletion, insertion, replay]
[48] [selection: modification, deletion, insertion, replay]

FIA_UID.1.1

The TSF shall allow

(1) Self-test according to FPT_TST.1,

(2) none[49][50]

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.

Application note 16 (Application Note 11 from [5]): Applied.

FIA_UAU.1 *Timing of authentication* (from [5])

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

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 channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD,

(4) none[51][52]

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 17 (Application Note 12 from [5]): Applied.

FIA_AFL.1 *Authentication failure handling* (from [5])

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

The TSF shall detect when an administrator configurable positive integer within 3-15[53] [54], unsuccessful authentication attempts occur related to consecutive failed authentication attempts[55]

[49] [assignment: *list of TSF-mediated actions*]
[50] [assignment: *list of additional TSF-mediated actions]*
[51] [assignment: *list of TSF-mediated actions*]
[52] [assignment: *list of additional TSF-mediated actions]*
[53] [assignment: positive integer number]
[54] [selection: [assignment: positive integer number] an administrator configurable positive integer within [assignment: range of acceptable values]]
[55] [assignment: list of authentication events]

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met[56], the TSF shall block RAD[57]

Application note 18 (Application Note 13 from [5]): Applied.

6.1.5 Security management (FMT)

FMT_SMR.1 *Security roles* (from [5])

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles R.Admin and R.Sigy[58].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

FMT_SMF.1 *Specification of management functions* (from [5])

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1

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

(1) Creation and modification of RAD,

(2) Enabling the signature-creation function,

(3) Modification of the security attribute SCD/SVD management, SCD operational,

(4) Change the default value of the security attribute SCD Identifier,

(5) Unblock the RAD[5960].

Application note 19: **(Application Note 14 from [5]):** Applied.

FMT_MOF.1 *Management of security functions behaviour* (from [5])

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1

The TSF shall restrict the ability to enable[61] the functions signature-creation function[62] to R.Sigy[63].

---

[56] [selection: met ,surpassed]
[57] [assignment: list of actions]
[58] [assignment: the authorized identified roles]
[59] [assignment: *list of security management functions to be provided by the TSF*]
[60] [assignment: *list of other security management functions to be provided by the TSF*]
[61] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
[62] [assignment: *list of functions*]

FMT_MSA.1/Admin *Management of security attributes* (from [5])

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Admin

The TSF shall enforce the *SCD/SVD_Generation_SFP*[64] to restrict the ability to modify[65] the security attributes SCD / SVD management[66] to R.Admin[67].

FMT_MSA.1/Signatory *Management of security attributes* (from [5])

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Signatory

The TSF shall enforce the Signature-creation_SFP[68] to restrict the ability to modify[69] the security attributes SCD operational[70] to R.Sigy[71].

FMT_MSA.2 *Secure security attributes* (from [5])

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for SCD / SVD Management and SCD operational[72].

Application note 20 (Application Note 15 from [5]): Applied.

FMT_MSA.3 *Static attribute initialization* (from [5])

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1

The TSF shall enforce the SCD/SVD_Generation_SFP, SVD_Transfer_SFP and Signature-

---

[63] [assignment: *the authorized identified roles*]
[64] [assignment: *access control SFP(s), information flow control SFP(s)*]
[65] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[66] [assignment: *list of security attributes*]
[67] [assignment: *the authorized identified roles*]
[68] [assignment: *access control SFP(s), information flow control SFP(s)*]
[69] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[70] [assignment: *list of security attributes*]
[71] [assignment: *the authorized identified roles*]
[72] [assignment: *list of security attributes*]

creation_SFP[73] to provide restrictive[74] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the R.Admin[75] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.4 *Security attribute value inheritance* (from [5])

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_MSA.4.1

The TSF shall use the following rules to set the value of security attributes:

(1) If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation.

(2) If S.Sigy successfully generates an SCD/SVD pair the security attribute "SCD operational of the SCD" shall be set to "yes" as a single operation.[76]

Application note 21 (Application Note 16 from [5]): Applied.

FMT_MTD.1/Admin *Management of TSF data* (from [5])

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Admin

The TSF shall restrict the ability to create[77] the RAD[78] to R.Admin[79].

FMT_MTD.1/Signatory *Management of TSF data* (from [5])

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Signatory

The TSF shall restrict the ability to modify, unblock[8081] the RAD[82] to R.Sigy[83].

---

[73] [assignment: *access control SFP, information flow control SFP*]
[74] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
[75] [assignment: the authorized identified roles
[76] [assignment: *rules for setting the values of security attributes*]
[77] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[78] [assignment: *list of TSF data*]
[79] [assignment: *the authorized identified roles*]
[80] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[81] [assignment: other operations]
[82] [assignment: *list of TSF data*]
[83] [assignment: *the authorized identified roles*]

Application note 22 (Application Note 17 from [5]):: Applied

6.1.6 Protection of the TSF (FPT)

FPT_EMS.1 *TOE Emanation* (from [5])

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1

The TOE shall not emit variations in power consumption or timing during command execution][84] in excess of non-useful information[85] enabling access to RAD[86] and SCD[87].

FPT_EMS.1.2

The TSF shall ensure unauthorized users[88] are unable to use the following interface electrical contacts and contactless interface[89] to gain access to RAD[90] and SCD[91].

Application note 23 (Application Note 18 from [5]): Applied.

FPT_FLS.1 *Failure with preservation of secure state* (from [5])

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1

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

(1) self-test according to FPT_TST fails,

(2) Failure detected by TSF according to FPT_TST.1[92].

Application note 24: **(Application Note 19 from [5])**: Applied.

FPT_PHP.1 *Passive detection of physical attack* (from [5])

Hierarchical to: No other components.

Dependencies: No dependencies

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

---

[84] [assignment: *types of emissions*]
[85] [assignment: specified limits]
[86] [assignment*: list of types of TSF data*]
[87] [assignment*: list of types of user data*]
[88] [assignment: type of users]
[89] [assignment: type of connection]
[90] [assignment*: list of types of TSF data*]
[91] [assignment*: list of types of user data*]
[92] [assignment*: list of types of failures in the TSF*]

FPT_PHP.3 *Resistance to physical attack* (from [5])

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_PHP.3.1

The TSF shall resist physical manipulation and physical probing [93] to the Hardware Platform[94]by responding automatically such that the SFRs are always enforced.

Application note 25 (Application Note 20 from [5]): Applied.

FPT_TST.1 *TSF testing* (from [5])

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TST.1.1

The TSF shall run a suite of self-tests during initial start-up[95] to demonstrate the correct operation of the TSF[96]

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of TSF data[97].

FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of TSF[98]

Application note 26 (Application Note 21 from [5]): Applied.

6.1.7 Trusted path/Channels (FTP)

FTP_ITC.1/DTBS Inter-TSF trusted channel – Signature creation Application

Hierarchical to: No other components

Dependencies: No dependencies

FTP_ITC.1.1/DTBS

The TSF shall provide a communication channel between itself and another trusted IT product SCA that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/DTBS

The TSF shall permit the remote trusted IT product[99] to initiate communication via the trusted channel.

---

[93] [assignment: physical tampering scenarios]
[94] [assignment: *list of TSF devices/elements*]
[95] [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions[assignment: conditions under which self-test should occur]]
[96] [selection: *[assignment: parts of TSF], the TSF*]
[97] [selection: *[assignment: parts of TSF data], TSF data*]
[98] [selection: *[assignment: parts of TSF], TSF*]

FTP_ITC.1.3/DTBS

The TSF or the SCA shall initiate communication via the trusted channel for

1. Signature creation,
2. none[100][101]

FTP_ITC.1/SVD Inter-TSF trusted channel – CGA

Hierarchical to: No other components

Dependencies: No dependencies

FTP_ITC.1.1/SVD

The TSF shall provide a communication channel between itself and another trusted IT product CGA that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SVD

The TSF shall permit the remote trusted IT product[102] to initiate communication via the trusted channel.

FTP_ITC.1.3/SVD

The TSF or the CGA shall initiate communication via the trusted channel for

1. data Authentication with Identity of Guarantor according to FDP_DAU.2/SVD.
2. none[103][104]

6.2 TOE Security Assurance Requirements

Assurance Class	**Assurance components**
ADV: Development	ADV_ARC.1 Architectural Design with domain separation and non-bypassability
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage

[99] [selection: *the TSF, another trusted IT product*]
[100] [assignment: list of functions for which a trusted channel is required]
[101] [assignment: list of other functions for which a trusted channel is required]
[102] [selection: *the TSF, another trusted IT product*]
[103] [assignment: list of functions for which a trusted channel is required]
[104] [assignment: list of other functions for which a trusted channel is required]

	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 9 Security Assurance Requirements: EAL4 augmented with AVA_VAN.5

6.3 Security Requirements Rationale

6.3.1 Security Requirement Coverage

	OT.Lifecycle Security	OT.SCD/SVD_Auth Gen	OT.SCD Unique	OT.SCD SVD Corresp	OT.SCD Secrecy	OT.Sig Secure	OT.Sigy SigF	OT.DTBS Integrity TOE	OT.EMSEC Design	OT.Tamper ID	OT.Tamper Resistance	OT.TOE_TC_SVD_Exp	OT.TOE_TC_DTBS_Imp
FCS_CKM.1	X		X	X	X								
FCS_CKM.4	X				X								
FCS_COP.1	X					X							
FDP_ACC.1/SCD/SVD_Generation	X	X											
FDP_ACC.1/SVD_Transfer	X											X	
FDP_ACC.1/Signature-Creation	X						X						
FDP_ACF.1/SCD/SVD_Generation	X	X											
FDP_ACF.1/SVD_Transfer	X											X	
FDP_ACF.1/Signature-creation	X						X						
FDP_DAU.2/SVD												X	
FDP_RIP.1					X		X						
FDP_SDI.2/Persistent				X	X	X							
FDP_SDI.2/DTBS							X	X					
FDP_UIT.1/DTBS													X
FIA_AFL.1.							X						

FIA_UAU.1		X					X						
FIA_UID.1		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			X						
FMT_MTD.1/Admin	X						X						
FMT_MTD.1/Signatory	X						X						
FMT_SMR.1	X						X						
FMT_SMF.1	X			X			X						
FPT_EMS.1					X				X				
FPT_FLS.1					X								
FPT_PHP.1										X			
FPT_PHP.3					X						X		
FPT_TST.1	X				X	X							
FTP_ITC.1/DTBS													X
FTP_ITC.1/SVD												X	

Table 10 Mapping of functional requirements to security objectives for the TOE

6.3.2 TOE Security Requirements Sufficiency

OT.Lifecycle_Security (*Lifecycle security*) is provided by the SFR for SCD/SVD generation FCS_CKM.1, SCD usage FCS_COP.1 and SCD destruction FCS_CKM.4 ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer. The SCD usage is ensured by access control FDP_ACC.1/Signature-creation, FDP_ACF.1/Signature-creation which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMF.1 and FMT_SMR.1. The test functions FPT_TST.1 provides failure detection throughout the lifecycle.

OT.SCD/SVD_Auth_Gen (Authorized 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 authorized functions. The SFR FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute initialization. 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. 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_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.

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).

SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Sig_Secure (*Cryptographic security of the digital signature*) is provided by the cryptographic algorithms specified by FCS_COP.1, which ensures 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 ensure self-tests ensuring correct signature-creation.

OT.Sigy_SigF (*Signature creation function for the legitimate signatory only*) is provided by an SFR for identification authentication and access control.

FIA_UAU.1 and FIA_UID.1 ensure that no signature generation 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. 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 and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature-creation process).

The security functions specified by FDP_ACC.1/Signature-creation and FDP_ACF.1/Signature-creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. 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. FMT_MOF.1 restricts the ability to enable the signature-creation function to the signatory. FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

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

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

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

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

OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) is provided by FTP_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by FDP_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS.

OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export) requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA, which is directly provided by

- The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer.
- FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor), which requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.
- FTP_ITC.1/SVD Inter-TSF trusted channel), which requires the TOE to provide a trusted channel to the CGA.

6.4 Satisfaction of dependencies of security requirements

The following table provides an overview how the dependencies of the security functional requirements are solved and a justification why some dependencies are not being satisfied.

Functional requirement	Dependencies	Satisfied by
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FDP_ACC.1/SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACC.1/SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACF.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3

Functional requirement	Dependencies	Satisfied by
FDP_ACF.1/SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDP_DAU.2/SVD	FIA_UID1.	FIA_UID.1
FDR_RIP.1	No dependencies	n/a
FDP_SDI.2/Persistent	No dependencies	n/a
FDP_SDI.2/DTBS	No dependencies	n/a
FDP_UIT.1/DTBS	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	n/a
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1,	FMT_SMR.1,

Functional requirement	Dependencies	Satisfied by
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_FLS.1	No dependencies	n/a
FPT_PHP.1	No dependencies	n/a
FPT_PHP.3	No dependencies	n/a
FPT_TST.1	No dependencies	n/a
FTP_ITC.1/DTBS	No dependencies	n/a
FTP_ITC.1/SVD	No dependencies	n/a

Table 11 Functional Requirements Dependencies

Assurance requirement(s)	Dependencies	Satisfied by
EAL4 package	(dependencies of EAL4 package are not reproduced here)	By construction, all dependencies are satisfied in a CC EAL package
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1 (all are included in EAL4 package)

Table 12 Satisfaction of dependencies of security assurance requirements

6.5 Rationale for chosen security assurance requirements

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

AVA_VAN.5 Advanced methodical vulnerability analysis

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

7 TOE Summary Specification

7.1 TOE Security Functions

Description of TOE Security Functions:

TSF.AccessControl

TSF.IdentificationAndAuthentication

TSF.Crypto

TSF.TrustedChannel

TSF Platform

7.1.1 TSF.AccessControl

This function provides the access controls to data in the file system, initialization, personalization and pre-personalization data. During earlier life phases, when the applet may not be present yet, the Platform TSFs, SF.AccessControl and SF.I&A are responsible for managing the accesses correctly.

This TSF allows the maintenance of Signatory and Administrator users, and they access rights depending on the identification and authentication.

The TSF provides functionality for the following SFRs:

- FDP_ACC.1/Signature_Creation: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FDP_ACC.1/SCD/SVD_Generation: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FDP_ACC.1/SVD_Transfer: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FDP_ACF.1/SCD/SVD_Generation: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FDP_ACF.1/SVD_Transfer: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FDP_ACF.1/Signature-creation: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FDP_RIP.1: The SFR requires that 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: signature creation data (SCD). This is ensured by TSF.AccessControl and also TSF_Platform.
- FIA_AFL.1: This SFR requires a detection of unsuccessful authentication attempts. It is realized by TSF.IdentificationAndAuthentication and TSF.AccessControl.

- FIA_UID.1: The requirement is about identification and authentication, what shall be accessed before and after it. It is realized by TSF.IdentificationAndAuthentication and TSF.AccessControl.
- FIA_UAU.1: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF.IdentificationAndAuthentication and TSF.AccessControl.
- FMT_MOF.1: This SFR requires the access control to signature-creation to the signatory, and is realized TSF.AccessControl.
- FMT_MSA.1/Admin: Requires that the SCD/SVD generation SFP to modify query the SCD/SVD management to the Administrator. It is realized by TSF.AccessControl.
- FMT_MSA.1/Signatory: Requires access control restrictions to modify the SCD operational security attributes to the signatory. This is realized by TSF.AccessControl.
- FMT_MTD.1/Admin: This SFR requires RAD creation access control to the Administrator. It is realized by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FMT_MTD.1/Signatory: This SFR requires RAD modification access control to the Signatory. It is realized by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FMT_SMR.1: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.

7.1.2 TSF.IdentificationAndAuthentication

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

7.1.2.1 Administrator Authentication

The Manufacturer and Personalization Agent is identified through the relevant access rights during the initialization and personalization of the TOE. During these phases the storage area affected is a write-only-once area, and the access right is granted to the Manufacturer and Personalization Agent, while the applet may not be present yet, the Platform TSFs, SF.AccessControl and SF.I&A are responsible for managing the accesses correctly. The management of data in the write-only-once storage area is based on the Platform security functionality SF.Securemanagement. The audit functions are provided by the Platform security function SF.Audit. Access during operational phase is only read-only.

This part of the TSF provides functionality for the following SFRs:

- FMT_SMR.1: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FMT_SMF.1: Requires the capability to perform management functions. It is realized by TSF.IdentificationAndAuthentication.
- FMT_MSA.3: Requires the capability to perform authentication controls. This is realized by TSF.IdentificationAndAuthentication.
- FMT_MSA.4: Requires the capability to differentiate between actions made by certain users. It is realized by TSF.IdentificationAndAuthentication.

7.1.2.2 User Authentication

This security function provides authentication of the users during Operational Phase.

This part of the TSF provides functionality for the following SFRs:

- FDP_ACC.1/Signature_Creation: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FDP_ACC.1/SCD/SVD_Generation: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FDP_ACC.1/SVD_Transfer: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FDP_ACF.1/SCD/SVD_Generation: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FDP_ACF.1/SVD_Transfer: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FDP_ACF.1/Signature-creation: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FIA_UID.1: The requirement is about identification and authentication, what shall be accessed before and after it. It is realized by TSF.IdentificationAndAuthentication and TSF.AccessControl.
- FIA_UAU.1: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF.IdentificationAndAuthentication and TSF.AccessControl.
- This SFR requires a detection of unsuccessful authentication attempts. It is realized by TSF.IdentificationAndAuthentication and TSF.AccessControl.
- FMT_MSA.3: Requires the capability to perform authentication controls. This is realized by TSF.IdentificationAndAuthentication.
- FMT_SMR.1: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FMT_MTD.1/Signatory: This SFR requires RAD modification access control to the Signatory. It is realized by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.
- FMT_SMR.1: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.IdentificationAndAuthentication.

7.1.3 TSF.TrustedChannel

The TSF is responsible for the command and response exchanges between the TOE and the external devices.

Various data and processes such as DTBSs, signatures, public keys, identification and

authentication data, SVD Transfer or other user data are embedded in command and response frames. The TSF.TrustedChannel function is capable of providing a secure communication channel between legitimate end points both of the TOE and the external device. The secure communication channels are supported with cryptographic functions and provide assured identification of its end points and protection of the channel data from modification or disclosure.

The cases when the TOE uses trusted channel are the following:

- import of the DTBS/R from the SCA intended to be signed by the TOE (ENC+MAC)
- SVD export (ENC)
- data Authentication with Identity of Guarantor

This function is responsible for confidentiality, data integrity and data authenticity. It provides functionality for:

- FDP_DAU.2/SVD: This requirement is about the capability to generate evidence about the validity of the SVD, and the CGA that shall be able to verify the validity and the identity of the user that generated the evidence. This is provided by TSF.TrustedChannel.
- FDP_UIT.1/DTBS: This requirement enforces Signature Creation SFP to receive user data protected from modification and insertion errors, and also to be able to determine whether modification and insertion has occurred. This is provided by TSF.TrustedChannel.
- FTP_ITC.1/DTBS: This requirement is about the Trusted Channel which is provided by the TSF_TrustedChannel.
- FTP_ITC.1/SVD: This requirement is about the Trusted Channel which is provided by the TSF_TrustedChannel.

7.1.4 TSF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation and deletion, secure random generator. The TSF makes use of the Platform TSF SF.CryptoKey.

It provides functionality for:

- FCS_CKM.1: The SFR requires generation of cryptographic keys. It is realized by TSF.Crypto.
- FCS.CKM.4: Requires the cryptographic key destruction according to a specified cryptographic method. This is realized by TSF.Crypto.
- FCS_COP.1.: Requires a use of cryptographic operation. It is provided by TSF.Crypto and TSF.Platform.

7.1.5 TSF.Platform

There are security functionalities based on the security functionalities of the certified cryptographic library and the certified IC platform. This TSF covers those functionalities.

This Security Function is responsible for protection of the TSF data, user data, applet data and TSF functionality. The TSF.Platform function is composed of software implementations of test and security functions.

The Platform provides the following security functionality:

- SF.AccessControl - enforces the access control
- SF.Audit - Audit functionality
- SF.CryptoKey - Cryptographic key management
- SF.CryptoOperation - Cryptographic operation
- SF.I&A - Identification and authentication
- SF.SecureManagement - Secure management of TOE resources
- SF.PIN - PIN management
- SF.LoadIntegrity - Package integrity check
- SF.Transaction - Transaction management
- SF.Hardware - TSF of the underlying IC
- SF.CryptoLib - TSF of the crypto library

These provide functionality for the following SFRs:

- FCS_CKM.1: The cryptographic key generation uses the Platform functionality, thus also provided by TSF.Platform.
- FCS_CKM.4: The required cryptographic key destruction method uses the Platform functionality, that is why it is also provided by TSF.Platform.
- FCS_COP.1: The cryptographic operation required by this SFR uses the Platform functionality, thus also provided by TSF.Platform.
- FDP_SDI.2/Persistent: Requires data integrity monitoring and prohibits the use of altered data. It is provided by TSF.Platform.
- FDP_SDI.2/DTBS: Requires data integrity monitoring and prohibits the use of altered data. It is provided by TSF.Platform.
- FPT_FLS.1: The requirement requires the preservation of a secure state when detecting failures. This is provided by TSF.Platform.
- FPT_PHP.1: Requires detection of physical attack. This is realized by TSF.Platform.
- FPT_PHP.3: Requires resistance to physical manipulation and probing to the Platform. This is realized by the TSF.Platform.
- FPT_TST.1: Requires self-test and capability to verify integrity of TSF and TSF data. This is also provided by the Platform, thus realized by the TSF.Platform.
- FPT_EMS.1: Requires that the TOE does not emit variations in power consumption or timing during command execution, and ensures that unauthorized users are unable to use the electrical contact interface to gain access to RAD and SCD. This is mainly realized with TSF.Platform, together with the following of Javacard platform guidelines.
- FDP_RIP.1: The SFR requires that 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: signature creation data (SCD). This is ensured by TSF.AccessControl and also TSF_Platform.

7.2 Fulfilment of the SFRs

TOE SFR / Security Function	TSF.AccessControl	TSF.IdentificationAndAuthentication	TSF.TrustedChannel	TSF.Crypto	TSF.Platform
FCS_CKM.1				X	X
FCS_CKM.4				X	X
FCS_COP.1				X	X
FDP_ACC.1/Signature_Creation	X	X			
FDP_ACC.1/SCD/SVD_Generation	X	X			
FDP_ACF.1/SCD/SVD_Generation	X	X			
FDP_ACC.1/SVD_Transfer	X	X			
FDP_ACF.1/SVD_Transfer	X	X			
FDP_ACF.1/Signature-creation	X	X			
FDP_DAU.2/SVD			X		
FDP_RIP.1	X				X
FDP_SDI.2/Persistent					X
FDP_SDI.2/DTBS					X
FDP_UIT.1/DTBS			X		
FIA_UID.1	X	X			
FIA_UAU.1	X	X			
FIA_AFL.1	X	X			
FMT_SMR.1	X	X			
FMT_SMF.1		X			

TOE SFR / Security Function	TSF.AccessControl	TSF.IdentificationAndAuthentication	TSF.TrustedChannel	TSF.Crypto	TSF.Platform
FMT_MOF.1	X				
FMT_MSA.1/Admin	X				
FMT_MSA.1/Signatory	X				
FMT_MSA.2		X			
FMT_MSA.3		X			
FMT_MSA.4		X			
FMT_MTD.1/Admin	X	X			
FMT_MTD.1/Signatory		X			
FPT_EMS.1					X
FPT_FLS.1					X
FPT_PHP.1					X
FPT_PHP.3					X
FPT_TST.1					X
FTP_ITC.1/DTBS			X		
FTP_ITC.1/SVD			X		

Table 13: Mapping of SFRs to mechanisms of TOE

7.2.1 Correspondence of SFR and TOE mechanisms

Each TOE security functional requirement is implemented by at least one TOE mechanism. In section 7.1 the implementing of the TOE security functional requirement is described in form of the TOE mechanism.

8 References

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

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, CCMB-2012-09-001, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 4, CCMB-2012-09-002, September 2012

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, CCMB-2012-09-003, September 2012

[5] Protection profiles for Secure signature creation device — Part 2: Device with key generation, BSI-CC-PP-0059 version 2.01

[6] ETSI Technical Specification 101 733: CMS Advanced Electronic Signatures (CAdES), V.1.7.4, 2008-07

[7] ETSI Technical Specification 101903: XML Advanced Electronic Signatures (XAdES), V.1.3.2, 2006-03

[8] CEN/TS 15480-2 – Identification card systems - European Citizen Card - Part 2: Logical data structures and card services

[9] ISO/IEC 24727-2 – Identification cards — Integrated circuit card programming interfaces — Part 2: Generic card interface

[10] SECURE HASH STANDARD, Federal Information Processing Standards Publication 180-4, October, 2008

[11] CCDB-2012-04-001 Composite product evaluation for Smart Cards and similar devices April 2012 Version 1.2 Mandatory Technical document

[12] ID&Trust CNS Applet User's Guide

[13] ID&Trust CNS Applet Administrator's Guide

[14] ID&Trust CNS Applet Initialization and Configuration

[15] Profile FileSystemCNS_21112005_with_DS

[16] NXP J3E081_M64, J3E081_M66, J2E081_M64, J3E041_M66, J3E016_M66, J3E016_M64, J3E041_M64 Secure Smart Card Controller Revision 3 Security Target Rev. 01.00 — 24th July 2013

[17] [Digital Signature Standard (DSS) - FIPS PUB 186-3, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, June, 2009

[18] CNS – Carta Nazionale dei Servizi Functional Specification V1.1.6 2/04/2011

[19] C.I.E. – Carta di Identitŕ Elettronica Functional Specification Version 2.0 2008/02/04

[20] DDU – Documento Unificato Functional Specification V1.0.0 20/04/2014

[21] Runtime Environment Specification Java Card(tm) Platform, Version 3.0.1 Classic Edition, May 2009, Sun Microsystems, Inc

9 Abbreviations

CC	Common Criteria
CGA	Certification generation application
DTBS	Data to be signed
DTBS/R	Unique representation of data to be signed
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
RAD	Reference authentication data
SCA	Signature-creation application
SCD	Signature-creation data
SCS	Signature-creation system
SDO	Signed data object
SFP	Security Function Policy
SSCD	Secure signature-creation device
ST	Security Target
SVD	Signature-verification data
TOE	Target of Evaluation
TSF	TOE Security Functionality
VAD	Verification authentication data