Security Target

for JPKI applet on JCOP 8.9

Version 1.0

Contents

1. Introduction

The Japanese Public Key Infrastructure (JPKI), a substitute name for the Public Certification Service for Individuals operated by the Japan Agency for Local Authority Information Systems (J-LIS). JPKI provides public ID authentication for user identification and provides document signing and user authentication. JPKI issue two kinds of electronic certificate, one is electronic certificate for signing and another is electronic certificate for user certification.

1.1. ST reference

Table 1-1 ST reference

ST reference	
Title	Security Target for JPKI applet on JCOP 8.9
Version	1.0
Authors	FeliCa Networks, Inc.
Reference	SJP-CC-FN-240924-001

1.2. TOE reference

Table 1-2 TOE reference

TOE reference	
TOE name	JPKI applet on JCOP 8.9
TOE version	V1.0
TOE developer	FeliCa Networks, Inc.
Product Type	Secure Signature Creation Device representing the SCD/SVD storage, SCD/SVD generation, and signature creation component
Platform Name	NXP JCOP 8.9 on SN300 Secure Element JCOP-eSE 8.9 R1.06.01.1.1
Platform certification number	NSCIB-CC-2300099-01
IC Name	NXP SN300 B5 Series
IC certification number	NSCIB-CC-2300083-01

1.3. Definitions

Table 1-3 Definitions

Definition	
Administrator	user who performs TOE initialisation, TOE personalisation, or other TOE administrative functions
Advanced electronic signature	digital signature which meets specific requirements in laws relating to Japanese Public Key Infrastructure.

Authentication data	information used to verify the claimed identity of a user
Certificate	digital signature used as electronic attestation binding an SVD to a person confirming the identity of that person as legitimate signer
Certificate info	information associated with a SCD/SVD pair that may be stored in a SSCD
Certificate generation application CGA	collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate
Certification service provider CSP	entity that issues certificates or provides other services related to electronic signatures. In this ST, CSP is called as SP-TSM.
Data to be signed DTBS	all electronic data to be signed including a user message and signature attributes
Data to be signed or its unique representation DTBS/R	data received by a SSCD as input in a single signature creation operation
Individual Number Card	a plastic card embedded with IC chip, and the holder's name, address, date of birth, sex, and Individual Number is printed on the face of the card.
JPKI application	a mobile phone application responsible for CGA and SCA.
Legitimate user	user of a SSCD who gains possession of it from an SSCD - provisioning service provider and who can be authenticated by the SSCD as its signatory
Qualified certificate	public key certificate that meets the requirements laid down in laws relating to Japanese Public Key Infrastructure and that is provided by a CSP that fulfils the requirements laid down in laws relating to Japanese Public Key Infrastructure
Qualified electronic signature	advanced electronic signature that has been created with an SSCD with a key certified with a qualified certificate
Reference authentication data RAD	data persistently stored by the TOE for authentication of a user as authorised for a particular role
Secure Channel Protocol '03'	a protocol from GlobalPlatform for mutual authentication and encrypted transport. The protocol allows for C-MAC, C-ENC, R-MAC and R-ENC modes of encryption and authentication of data
Secure Signature Creation Device SSCD	hardware or software that is used in creating an electronic signature
Secure Element Issuer Trusted Service Manager SEI-TSM	entity that loads JPKI applet on the secure element in the mobile phone

Signatory	legitimate user of an SSCD associated with it in the certificate of the signature verification and who is authorised by the SSCD to operate the signature creation function
Signature attribute	additional information that is signed together with a user message
Signature creation application SCA	application complementing an SSCD with a user interface with the purpose to create an electronic signature
Signature creation data SCD	private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature. JPKI applet has two SCDs, which are “the private key for signing” and “the private key for user certification”.
Signature creation system	complete system that creates an electronic signature consists of the SCA and the SSCD
Signature verification data SVD	public cryptographic key that can be used to verify an electronic signature. JPKI applet has two SVDs, which are “the public key for signing” and “the public key for user certification”.
SSCD-provisioning service	service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD
User	entity (human user or external IT entity) outside the TOE that interacts with the TOE
User Message	data determined by the signatory as the correct input for signing
Verification authentication data VAD	data provided as input to a SSCD for authentication by cognition or by data derived from a user’s biometric characteristics

1.4. **TOE Overview**

The TOE, JPKI applet on JCOP 8.9, is a Java Card system that provides a secure signature creation device (SSCD) with key generation for creating an electronic signature and authenticating users. The TOE is embedded as a secure element (eSE) on the mobile phone.

1.4.1. TOE description

The following figure illustrates the physical scope of the TOE (indicated in yellow).;

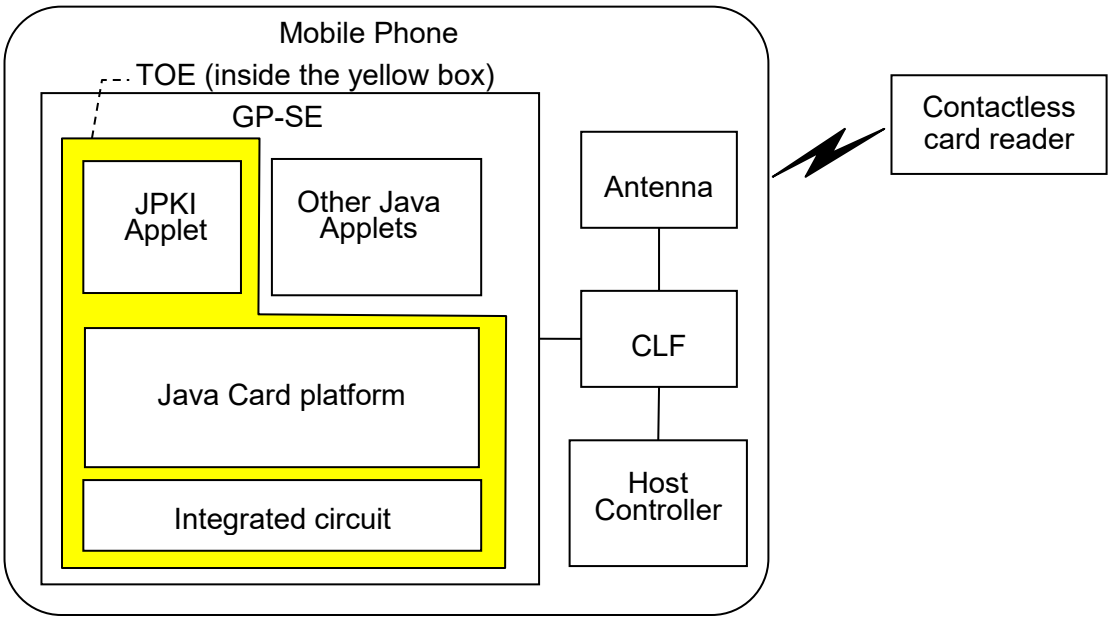

Figure 1-1 TOE physical scope

The components of the TOE are explained as follows:

- JPKI applet constitutes the part of the TOE that is responsible for generating a key pair for digital signature and for user certification. It manages the access control to use the signature creation function and executes the cryptographic operation for generating an electronic signature. JPKI applet is installed as a post-issuance in the operational environment.
- JCOP 8.9 is a Java Card Platform that manages and executes applets. It provides APIs for developing applets in accordance with the Java Card specification [JP-SPEC]. Java Card Platform has GlobalPlatform packages providing a common interface to communicate with a smart card and manage applications in a secure way according to the GP specifications [GP]. The Java Card Platform has been certified by Common Criteria in conformance with Java Card System Protection Profile - Open Configuration [JC-PP]
- SN300 is an integrated circuit that is the hardware platform of the TOE. The hardware platform provides the basic cryptographic functionalities and includes security detectors, sensors, and circuitry to protect the TOE. The integrated circuit has been certified by Common Criteria against [BSI-PP-0084].
- The associated guidance documentations are as follows:
  - Commercial Applet for Mobile JPKI Projects External Interface Specification [JPKI-IF]
  - JPKI applet Installation procedure [JPKI-IP]
  - JPKI applet Delivery and acceptance procedure [JPKI-PRE]
  - JPKI applet User guidance [JPKI-UGM]

- **Table 1-4 The components of the TOE**

Name		Version	Form of delivery	Delivery method
Hardware	NXP SN300 B5 Series	SN300_SE B5.1.002 JD	eSE HW	By courier
Software	NXP JCOP 8.9 on SN300 Secure Element	JCOP-eSE 8.9 R1.06.01.1.1	embedded in the above	By courier
	JPKI applet	1.0	binary	Procedures in accordance with [JPKI-PRE].
Guidance	JPKI applet, Delivery and acceptance procedure	1.1	PDF	Procedures in accordance with [JPKI-PRE].
	JPKI applet, Installation procedure	1.6	PDF	Procedures in accordance with [JPKI-PRE].
	JPKI applet User guidance	1.3	PDF	Procedures in accordance with [JPKI-PRE].
	Commercial Applet for Mobile JPKI Projects External Interface Specification	1.0	PDF	Procedures in accordance with [JPKI-PRE].

1.4.2. Operation and major security features

This section presents a functional overview of the TOE in its distinct operational environments.

- The preparation environment where JPKI application interacts with the SEI-TSM to load JPKI applet, and where the TOE interacts with a certification service provider (SP-TSM) to obtain a certificate for the signature verification data (SVD) corresponding with the signature creation data (SCD) generated by the TOE.
- The signing environment where it interacts with a signer through JPKI application to sign data after authenticating the signer as its signatory. The signature creation application (SCA) provides the data to be signed, or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting digital signature.

The TOE performs the following functions:

- to generate SCD for digital signature and the correspondent SVD;
- to generate SCD for user certification and the correspondent SVD;
- to prove the identity as SSCD to SP-TSM;
- to export the SVDs for certification through a trusted channel to the CGA;
- to receive and store certificate info;

- to switch the TOE from a non-operational state to an operational state; and
- to create digital signatures through the following steps:
  A) select a SCD for digital signature in the SSCD,
  B) authenticate the signatory and determine its intent to sign,
  C) receive DTBS,
  D) apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS.
- to authenticate user for user certification through the following steps:
  A) select a SCD for user certification in the SSCD,
  B) authenticate the signatory and determine its intent to sign,
  C) receive DTBS,
  D) apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS.

The TOE provides the following functions that are not defined in the PP:

- to import a public key for external authentication as RAD and authenticate a user as its signatory by using the public key.
- to generate hash to authenticate itself by the SP-TSM,
- to generate random number meeting the quality metric depending on purposes.

1.5. **Lifecycle**

The TOE life cycle distinguishes phases for development and usage. The development phase is subject of CC evaluation according to ALC class. The development phase ends with the delivery of the TOE (the delivery of the eSE to a mobile phone manufacturer and delivery of JPKI applet to SEI-TSM). The eSE is delivered to a mobile phone user. The usage phase has two stages: the JPKI preparation stage and JPKI operational use stage, in usage phase. JPKI applet is loaded and installed by SEI-TSM in the JPKI preparation stage. The TOE lifecycle and the two stages are described in the following figure and sections.

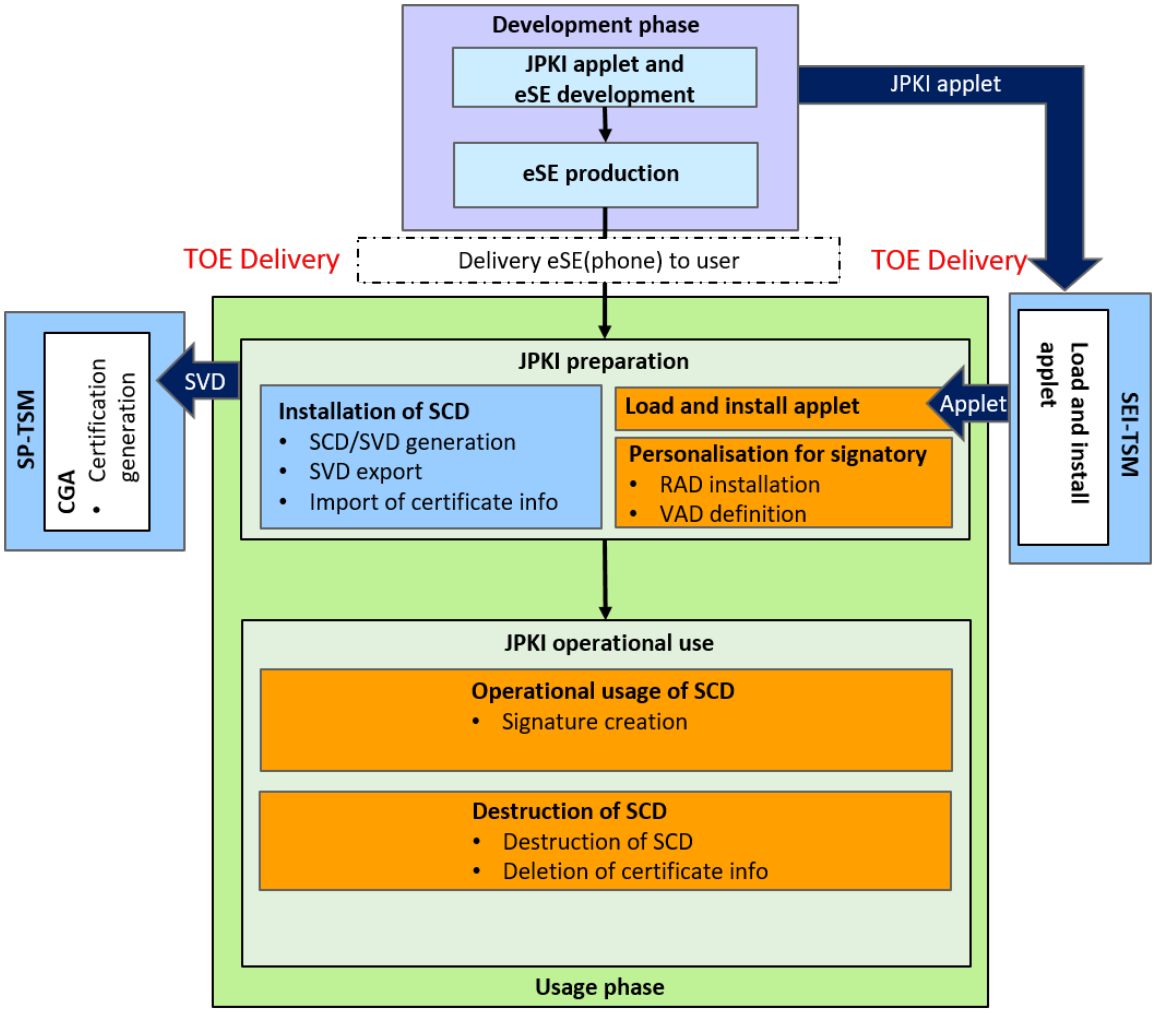

Figure 1-2 TOE lifecycle

1.5.1. JPKI preparation stage

During JPKI preparation stage, SEI-TSM performs the following tasks:

- Load and install JPKI applet to the eSE embedded in the mobile phone held by the user.
- Generate a temporary password and store it as RAD in the TOE

After installing JPKI applet, SP-TSM performs the following tasks:

- Obtain information on the intended recipient of the device as required for the preparation process and identification as a legitimate user by authenticating the user's Individual Number Card.
- Perform the mutual authentication with the TOE and establish the secure channel between SP-TSM and the TOE.
- Request the TOE to generate SCD/SVD pairs for digital signature and user certification
- Request the TOE to export SVD from the TOE and import certificate information corresponding to the SVD to the TOE via a secure channel between the TOE and SP-TSM.
- Change RAD to a password specified by the legitimate user.

1.5.2. JPKI operational use stage

In this lifecycle stage, the signatory can use the TOE to create electronic signatures.
The JPKI operational use stage begins when the signatory has obtained the TOE and SCD/SVD pair and set RAD. Enabling the TOE for signing requires at least one set of SCD stored in its memory.
The TOE can store 2 types of RAD; one is password and another is public key for external authentication using biometric. When the signatory selects biometric authentication to authenticate oneself, public key for external authentication is imported as a RAD.
RAD is locked when wrong RAD is entered to specified number of times. Only the administrator can be unlocked via a secure channel between the TOE and SP-TSM.
The TOE has the functionality to generate the hash to authenticate itself by the SP-TSM.
The signatory can render an SCD/SVD in the TOE permanently unusable on demand. Rendering the last SCD/SVD in the TOE permanently unusable ends the life of the TOE as SSCD.
The TOE have the functionality to generate random numbers meeting the quality metric depending on purposes.

2. Conformance claims

2.1. CC conformance claim

The evaluation is based on the following:

- "Common Criteria for Information Technology Security Evaluation", Version 3.1 Release 5 (composed of Parts 1-3, [CC Part 1], [CC Part 2], and [CC Part 3])
- "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1 [CC CEM]

This Security Target claims the following conformances:

- [CC Part 2] extended
- [CC Part 3] conformant

2.2. Package claim

This Security Target claims conformance to the assurance package:

- Evaluation Assurance Level 4 (EAL4) augmented with ALC_DVS.2 and AVA_VAN.5

2.3. PP claim

This Security Target and the TOE claim strict conformance to the following Protection Profiles (PP):

- Protection profiles for secure signature creation device - Part 2: Device with key generation [SSCD2]
- Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application [SSCD4]

2.4. PP claim rationale

This ST includes all the security problem definition, the security objectives and requirements claimed by section 2.3, and all the operations applied to the SFRs are in accordance with the requirements of these PPs.

3. Security problem definition

3.1. Assets

CC defines 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 has been taken from [SSCD2] adding some descriptions for JPKI.

Table 3-1 Assets and objects

Assets	Description
SCD	private key used to perform an electronic signature operation. The confidentiality, integrity and signatory’s sole control over the use of the SCD shall be maintained. In JPKI, SCD corresponds “the private key for digital signature” and “the private key for user certification”.
SVD	public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported shall be maintained. In JPKI, SVD corresponds “the public key for digital signature” and “the public key for user certification”.
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 electronic signature shall be maintained.
Public key	This public key is imported and stored in the TOE, and used to authenticate as user as its signatory.

3.2. Subjects

Table 3-2 Subjects

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

3.3. Threats

Threats are as defined in [SSCD2] and [SSCD4].

Table 3-3 Threats

Threats	Description
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 that 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.

3.4. Organisational security policies

Organisational security policies are as defined in [SSCD2] and [SSCD4]. P.RND and P.Hash are additional operational security policies in this ST.

Table 3-4 Organisational security policies (OSP)

OSP	Description
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). 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 their 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. 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 lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.
P.RND	**Sufficient quality of random numbers** The TSF generates random numbers to be used for the TSF itself. The quality of random numbers is sufficient to prevent prediction by an attacker.
P.Hash	**Capability of hash calculator** The TSF calculates a secure hash value to be used for device authentication by SP-TSM

Application note：SSCD PP is for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures as generally recognised standard for electronic-signature products in the Official Journal of the European Communities. The ST is for use by the Japanese Government in accordance with laws relating to Japanese Public Key Infrastructure.

3.5. **Assumptions**

Assumptions are as defined in [SSCD2].

Table 3-5 Assumptions

Assumptions	Description
A.CGA	**Trustworthy certificate 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.

4. Security objectives

4.1. Security objectives for the TOE

Security objectives for the TOE are as defined in [SSCD2] and [SSCD4]. OT.RND and OT.Hash are additional ecurity objectives for the TOE in this ST.

Table 4-1 Security objectives for the TOE

Security objectives for the TOE	Description
OT.Lifecycle_Security	**Lifecycle security** The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall securely destroy the SCD on demand of the signatory. **Application note:** 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	**Authorised SCD/SVD generation** The TOE shall provide security features to ensure that authorised users only may invoke the generation of the SCD and the SVD
OT.SCD_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 the SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential. **Application note:** The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and secure 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 shall 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 emanations 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 resist physical tampering with specified system devices and components.
OT.TOE_SSCD_Auth	**Authentication proof as SSCD** The TOE shall hold unique identity and authentication data as SSCD and provide security mechanisms to identify and to authenticate itself as SSCD.
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.RND	**Provide sufficient quality of random numbers** The TSF shall generate random numbers meeting the quality metric depending on purposes. Furthermore, the TSF shall prevent itself from leaking information so that an attacker cannot guess the random number generated.
OT.Hash	**Provide capability of hash calculation** The TSF shall provide capability of hash calculation meeting the standard algorithm.

4.2. Security objectives for the operational environment

Security objectives for the operational environment are as defined in [SSCD2] and [SSCD4].

Table 4-2 Security objectives for the operational environment

Security objectives for the operational environment	Description
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.Dev_Prov_Service	**Authentic SSCD provided by SSCD-provisioning service** The SSCD-provisioning service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, personalises the TOE for the legitimate user as signatory, links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the signatory. Note: This objective replaces OE.SSCD_Prov_Service from the core PP, which is possible as it does not imply any additional requirements for the operational environment when compared to OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_Service).
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.
OE.DTBS_Protect	**SCA protects the data intended to be signed** The operational environment shall ensure that the DTBS/R cannot be altered in transit between the SCA and the TOE. In particular, if the TOE requires a trusted channel for import of the DTBS/R, the SCA shall support usage of this trusted channel.
OE.Signatory	**Security obligation of the signatory** The signatory shall check 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.CGA_SSCD_Auth	**Pre-initialisation of the TOE for SSCD authentication** The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSCD, successfully proved this identity as SSCD to the CGA, and whether this identity is linked to the legitimate holder of the device as applicant for the certificate.

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.

4.3. **Security objectives rationale**

The following table provides an overview for security objectives coverage.

Table 4-3 Mapping of security problem definition to security objectives

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.RND	OT.Hash	OE.CGA_QCert	OE.SVD_Auth	OE.Dev_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.CGA_SSCD_Auth	OE.CGA_TC_SVD_Imp
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		
T.DTBS_Forgery								X												X	X			
T.Sig_Forgery			X			X										X								
P.CSP_QCert	X			X								X				X							X	
P.QSign						X	X									X				X				
P.Sigy_SSCD	X	X	X		X	X	X	X	X		X	X	X					X					X	X
P.Sig_Non-Repud	X		X	X	X	X	X	X	X	X	X	X	X			X	X	X		X	X	X	X	X
P.RND														X										
P.Hash															X									
A.CGA																X	X							
A.SCA																				X				

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

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

T.Sig_Forgery (*Forgery of the 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.

P.CSP_QCert (*CSP generates qualified certificates*) provides that the TOE and the SCA may be employed to sign data with (qualified) electronic signatures, as defined by the Directive, article 5, paragraph 1. Directive, recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The **OE.CGA_QCert** addresses the requirement of qualified (or advanced) electronic signatures as being based on qualified (or non-qualified) certificates. According to **OT.TOE_SSCD_Auth** the copies of the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD to prove this identity as SSCD to the CGA. The **OE.CGA_SSCD_Auth** ensures that the SP checks the proof of the device presented of the applicant that it is a SSCD. The **OT.SCD_SVD_Corresp** ensures that the SVD exported by the TOE to the CGA corresponds to the SCD stored in the TOE and used by the signatory. The **OT.Lifecycle_Security** ensures that the TOE detects flaws during the initialisation, personalisation and operational usage.

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 of the Directive. The paragraph 1(a) of Annex III is ensured by **OT.SCD_Unique** requiring that the SCD used for signature creation can practically occurs only once. The **OT.SCD_Secrecy OT.Sig_Secure** and **OT.EMSEC_Design** and **OT.Tamper_Resistance** address the secrecy of the SCD (cf. paragraph 1(a) of Annex III). **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 shall not alter the DTBS/R. The usage of SCD under sole control of the signatory is ensured by **OT.Lifecycle_Security**, **OT.SCD/SVD_Auth_Gen** and **OT.Sigy_SigF**.

OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised TOE from an SSCD-provisioning service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD-provisioning service, the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD in the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives **OT.TOE_SSCD_Auth** and **OT.TOE_TC_SVD_Exp**) to check whether the device presented is a SSCD linked to the applicant as required by **OE.CGA_SSCD_Auth** and 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.

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, initialised and personalised 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). The TOE security feature addressed by the security objectives **OT.TOE_SSCD_Auth** and **OT.TOE_TC_SVD_Exp** supported by **OE.Dev_Prov_Service** enables the verification whether the device presented by the applicant is a SSCD as required by **OE.CGA_SSCD_Auth** and the received SVD is sent by the device holding the corresponding SCD as required by **OE.CGA_TC_SVD_Imp**. **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, OE.DTBS_Protect** and **OT.DTBS_Integrity_TOE** ensure that the TOE generates 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** ensure that only this SCD may generate 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.

P.RND (*Sufficient quality of random numbers*) requires the TOE to provide good quality of random numbers. If **OT.RND** is enforced, random numbers with a quality sufficient for the TSF will be generated, and it will prevent an attacker from retrieving information helpful to guess random numbers.

P.Hash (*Capability of hash calculator*) requires the TOE to provide capability of hash calculation. If **OT.Hash** is enforced, hash is calculated in accordance with the standard algorithm.

A.CGA (*Trustworthy certificate 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.

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.

Application note: SSCD PP is for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures as generally recognised standard for electronic-signature products in the Official Journal of the European Communities. The ST is for use by the Japanese Government in accordance with laws relating to Japanese Public Key Infrastructure.

5. Extended components definition

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined in [SSCD2]. This ST uses the component FPT_EMS.1 as defined in [SSCD2]. The additional family FIA_API (Authentication Proof of Identity) of the Class FIA (Identification and authentication) is defined in [SSCD4]. This ST uses the component FIA_API.1 as defined in [SSCD4]. The additional family FCS_RNG (Generation of random numbers) of Class FCS (Cryptographic support) is defined in [PP-PN]. This ST uses the component FCS_RNG as defined in [PP-PN].

6. Security requirements

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

6.1. Security functional requirements

The Security Objectives result in a set of Security Functional Requirements (SFRs).

Section 6.1.2 and 6.1.3 describes the SFRs which are defined in the PPs [SSCD2] and [SSCD4], respectively. Section 6.1.4 describes the additional SFRs in this ST.

About the notation used for Security Functional Requirements (SFRs):

Refinements are denoted as **bold**.

Selections are denoted as underlined text.

Assignments are denoted as **underlined text and bold**.

Iterations are denoted by showing a slash "/".

6.1.1. User data protection (FDP)

Table 6-1 : Subjects and security attributes for access control

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	authorised, not authorised
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)

Application note: S.User with the security attribute 'Role' set to 'R.Sigy' is allowed to destroy the SCD.

6.1.2. Security assurance requirements taken from the PP Part 2

FCS_CKM.1/SCD **Cryptographic key generation**

FCS_CKM.1.1/SCD The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic key sizes **2048 bit** that meet the following: **[PKCS #1] and [FIPS 186-4]**.

FCS_CKM.4/SCD **Cryptographic key destruction**

FCS_CKM.4.1/SCD The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **either overwriting with new SCD/SVD pair or deleting SCD/SVD pair when JPKI applet deletion** that meets the following: **none**.

Application note: The destruction of the SCD is done at least on demand of the signatory.

FCS_COP.1/SCD	**Cryptographic operation**
FCS_COP.1.1/SCD	The TSF shall perform **digital signature creation** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **2048 bit** that meet the following: **RSASSA-PKCS1-v1_5** [PKCS #1].

FDP_ACC.1/SCD/SVD_Generation	**Subset access control**
FDP_ACC.1.1/ SCD/SVD_Generation	The TSF shall enforce the **SCD/SVD Generation SFP** on: **(1) subjects: S.User,** **(2) objects: SCD, SVD,** **(3) operations: generation of SCD/SVD pair.**

FDP_ACF.1/SCD/SVD_Generation	**Security attribute based access control**
FDP_ACF.1.1/ SCD/SVD_Generation	The TSF shall enforce the **SCD/SVD Generation SFP** to objects based on the following: **the user S.User is associated with the security attribute "SCD / SVD Management"**.
FDP_ACF.1.2/ SCD/SVD_Generation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.User with the security attribute "SCD / SVD Management" set to "authorised" is allowed to generate SCD/SVD pair**.
FDP_ACF.1.3/ SCD/SVD_Generation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**
FDP_ACF.1.4/ SCD/SVD_Generation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair**.

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

FDP_ACF.1/SVD_Transfer	**Security attribute based access control**
FDP_ACF.1.1/ SVD_Transfer	The TSF shall enforce the **SVD Transfer SFP** to objects based on the following: **(1) the S.User is associated with the security attribute Role,** **(2) the SVD.**
FDP_ACF.1.2/ SVD_Transfer	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **R.Admin** is allowed to export SVD.
FDP_ACF.1.3/ SVD_Transfer	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

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

FDP_ACC.1/Signature_Creation	**Subset access control**
FDP_ACC.1.1/Signature_Creation	The TSF shall enforce the **Signature Creation SFP** on: **(1) subjects: S.User,** **(2) objects: DTBS/R, SCD,** **(3) operations: signature creation.**

FDP_ACF.1/Signature_Creation	**Security attribute based access control**
FDP_ACF.1.1/Signature_Creation	The TSF shall enforce the **Signature Creation SFP** 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".**
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 electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes".**
FDP_ACF.1.3/Signature_Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.
FDP_ACF.1.4/Signature_Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no"**.

FDP_RIP.1	**Subset residual information protection**
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from the following objects: **SCD**.

FDP_SDI.2/Persistent	**Stored data integrity monitoring and action**
FDP_SDI.2.1/Persistent	The TSF shall monitor user data stored in containers controlled by the TSF for **integrity error** on all objects, based on the following attributes: **integrity checked stored data**.
FDP_SDI.2.2/Persistent	Upon detection of a data integrity error, the TSF shall: **(1) prohibit the use of the altered data,** **(2) inform the S.Sigy about integrity error**.

FDP_SDI.2/DTBS	**Stored data integrity monitoring and action**
FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored in containers controlled by the TSF for **integrity error** on all objects, based on the following attributes: **integrity checked stored DTBS**.

FDP_SDI.2.2/DTBS	Upon detection of a data integrity error, the TSF shall: **(1) prohibit the use of the altered data,** **(2) inform the S.Sigy about integrity error**.
FIA_UID.1	**Timing of identification**
FIA_UID.1.1	The TSF shall allow: **(1) self-test according to FPT_TST.1,** **(2) establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD,** **(3) select File, read some file without authentication and generate random number** 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.
FIA_UAU.1	**Timing of authentication**
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) select File, read file without authentication, and generate random number** 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.
FIA_AFL.1	**Authentication failure handling**
FIA_AFL.1.1	The TSF shall detect when 5 in user authentication for digital signature or 3 in user authentication for user certification unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met, the TSF shall **block RAD**.
FMT_SMR.1	**Security roles**
FMT_SMR.1.1	The TSF shall maintain the roles **R.Admin and R.Sigy**.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

FMT_SMF.1	**Security management functions**
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) none**.
FMT_MOF.1	**Management of security functions behaviour**
FMT_MOF.1.1	The TSF shall restrict the ability to enable the functions **signature creation function** to **R.Sigy**.
FMT_MSA.1/Admin	**Management of security attributes**
FMT_MSA.1.1/Admin	The TSF shall enforce the **SCD/SVD Generation SFP** to restrict the ability to modify the security attributes **SCD / SVD management** to **R.Admin**.
FMT_MSA.1/Signatory	**Management of security attributes**
FMT_MSA.1.1/Signatory	The TSF shall enforce the **Signature Creation SFP** to restrict the ability to modify the security attributes **SCD operational** to **R.Sigy**.
FMT_MSA.2	**Secure security attributes**
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for **SCD / SVD Management and SCD operational**.
FMT_MSA.3	**Static attribute initialisation**
FMT_MSA.3.1	The TSF shall enforce the **SCD/SVD Generation SFP, SVD Transfer SFP and Signature Creation SFP** to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the **R.Admin** to specify alternative initial values to override the default values when an object or information is created.
FMT_MSA.4	**Security attribute value inheritance**
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**. Application note: The TOE does not support generating an SCD/SVD pair by signatory alone, therefore rule (2) is not relevant.

FMT_MTD.1/Admin	**Management of TSF data**
FMT_MTD.1.1/Admin	The TSF shall restrict the ability to create the **RAD** to **R.Admin**.

Application note: The RAD can be unblocked by only Admin.

FMT_MTD.1/Signatory	**Management of TSF data**
FMT_MTD.1.1/Signatory	The TSF shall restrict the ability to modify **and none** the **RAD** to **R.Sigy**.
FPT_EMS.1	**TOE Emanation**
FPT_EMS.1.1	The TOE shall not emit **side channel emission** in excess of **limits specified by the state-of-the-art attacks on smart card IC** enabling access to **RAD** and **SCD**.
FPT_EMS.1.2	The TSF shall ensure **any users** are unable to use the following interface **physical chip contact or contactless I/O** to gain access to **RAD** and **SCD**.
FPT_FLS.1	**Failure with preservation of secure state**
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: **(1) self-test according to FPT_TST fails,** **(2) IC environmental sensors detection (Temperature out of range, Supply Voltage of chip)** **(3) IC internal error detection sensors failure (Parity, RNG, operation)**
FPT_PHP.1	**Passive detection of physical attack**
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.
FPT_PHP.3	**Resistance to physical attack**
FPT_PHP.3.1	The TSF shall resist **physical manipulation and physical probing** to the **hardware of the TOE and software composing the TSF** by responding automatically such that the SFRs are always enforced.
FPT_TST.1	**TSF testing**
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up or before running a secure operation to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of TSF.

6.1.3. Security functional requirements taken from the PP Part 4

FIA_API.1	**Authentication Proof of Identity**
FIA_API.1.1	The TSF shall provide an **device authentication mechanism** to prove the identity of the **SSCD**.
FDP_DAU.2/SVD	**Data Authentication with Identity of Guarantor**
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**.
FDP_DAU.2.2/SVD	The TSF shall provide **CGA** with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.
FTP_ITC.1/SVD	**Inter-TSF trusted channel**
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 ensured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/SVD	The TSF shall permit another trusted IT product 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 FIA_API.1 and FDP_DAU.2/SVD,** **(2) import of certificate info from the CGA.**

Application note: Trusted channel mandates both a successful device authentication and an active secure messaging session. The TOE provides a device authentication mechanism and secure messaging session in accordance with GlobalPlatform Technology Secure Channel Protocol '03' [GP-D]. The established secure messaging session along with device authentication helps identify the SSCD itself as required by FIA_API.1.

6.1.4. Security functional requirements defined in the ST

FCS_CKM.4/Ext_Auth	**Cryptographic key destruction**
FCS_CKM.4.1/Ext_Auth	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **either overwriting with new key for external authentication or deleting key for external authentication when JPKI applet deletion** that meets the following: **none**.
FCS_COP.1/Ext_Auth	**Cryptographic operation**
FCS_COP.1.1/Ext_Auth	The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **2048 bit** that meet the following: **RSASSA-PKCS1-v1_5** [PKCS #1].
FCS_COP.1/Hash	**Cryptographic operation**
FCS_COP.1.1/Hash	The TSF shall perform **hash calculation** in accordance with a specified cryptographic algorithm **SHA-256** and cryptographic key sizes **none** that meet the following: **FIPS180-4**.

FCS_RNG.1	**Random number generator**
FCS_RNG.1.1	The TSF shall provide a deterministic random number generator [DRG.3][AIS20] that implements: • **(DRG.3.1) If initialized with a random seed using a PTRNG of class PTG.2 (as defined in [AIS20]) as random source, the internal state of the RNG shall have at least 256 bit of entropy.** • **(DRG.3.2) The RNG provides forward secrecy (as defined in [AIS20]).** • **(DRG.3.3) The RNG provides enhanced backward secrecy even if the current internal state is known (as defined in [AIS20])** .
FCS_RNG.1.2	The TSF shall provide random numbers that meet • **(DRG.3.4) The RNG, initialized with a random seed using a PTRNG of class PTG.2 (as defined in [AIS20]) as random source, generates output for which for AES-mode 2^{48} and for TDEA-mode 2^{35} strings of bit length 128 are mutually different with probability at least 1-2^{24}** • **(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A (as defined in [AIS20])**.
FDP_ACC.1/Ext_Auth	**Subset access control**
FDP_ACC.1.1/Ext_Auth	The TSF shall enforce the **public key import SFP** on **(1) subjects: S.User,** **(2) objects: public key,** **(3) operations: write**
FDP_ACF.1/Ext_Auth	**Security attribute based access control**
FDP_ACF.1.1/Ext_Auth	The TSF shall enforce the **public key import SFP** 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"**
FDP_ACF.1.2/Ext_Auth	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 import the public key for External authentication with SCD which security attribute "SCD operational" is set to "yes".**
FDP_ACF.1.3/Ext_Auth	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**
FDP_ACF.1.4/Ext_Auth	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User is not allowed to import the public key for External authentication which security attribute "SCD operational" is set to "no"**.
FDP_ITC.1/Ext_Auth	**Import of user data without security attributes**
FDP_ITC.1.1/Ext_Auth	The TSF shall enforce the **public key import SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/Ext_Auth The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

FIA_UAU.4 Single-use authentication mechanism

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to **External authentication using public key**.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide

(1) Password authentication,

(2) External authentication using public key

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **following rules:**

(1) Default authentication mechanism is "Password authentication",

(2) If the user activates alternative methods via SCA, "External authentication using public key" is used.

FMT_MSA.1/Ext_Auth Management of security attributes

FMT_MSA.1.1/Ext_Auth The TSF shall enforce the **public key import SFP** to restrict the ability to modify the security attributes **SCD operational** to **R.Sigy**.

FMT_MSA.3/Ext_Auth Static attribute initialisation

FMT_MSA.3.1/Ext_Auth The TSF shall enforce the **public key import SFP** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Ext_Auth The TSF shall allow the **R.Admin** to specify alternative initial values to override the default values when an object or information is created.

6.2. Security assurance requirements

The Security Assurance Requirements for the TOE are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by the component ALC_DVS.2 and AVA_VAN.5. The assurance requirements are shown in the following table.

Table 6-2 Assurance requirements: EAL4 augmented with ALC_DVS.2 and AVA_VAN.5

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
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency 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

6.3. **Security functional requirements rationale**

6.3.1. Security requirement coverage

Table 6-3 Functional requirement to TOE security objective mapping

	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_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.RND	OT.Hash
FCS_CKM.1/SCD	X		X	X	X										
FCS_CKM.4/SCD	X				X										
FCS_COP.1/SCD	X					X									
FDP_ACC.1/SCD/SVD_ Generation	X	X													
FDP_ACF.1/SCD/SVD_ Generation	X	X													
FDP_ACC.1/SVD_Tran sfer	X												X		
FDP_ACF.1/SVD_Trans fer	X												X		
FDP_ACC.1/Signature_ Creation	X						X								
FDP_ACF.1/Signature_ Creation	X						X								
FDP_RIP.1					X		X								
FDP_SDI.2/Persistent				X	X	X									
FDP_SDI.2/DTBS							X	X							
FIA_AFL.1							X								
FIA_UAU.1		X					X					X			
FIA_UID.1		X					X								
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/Signaory	X						X								

FMT_SMR.1	X						X								
FMT_SMF.1	X						X								
FPT_EMS.1					X				X						
FPT_FLS.1					X										
FPT_PHP.1										X					
FPT_PHP.3					X						X				
FPT_TST.1	X				X	X									
FIA_API.1												X			
FDP_DAU.2/SVD													X		
FTP_ITC.1/SVD													X		
FCS_CKM.4.1/Ext_Auth							X								
FCS_COP.1.1/Ext_Auth							X								
FCS_COP.1/Hash															X
FCS_RNG.1														X	
FDP_ACC.1.1/Ext_Auth							X								
FDP_ACF.1.1/Ext_Auth							X								
FDP_ITC.1/Ext_Auth							X								
FIA_UAU.4							X								
FIA_UAU.5							X								
FMT_MSA.1/Ext_Auth							X								
FMT_MSA.3/Ext_Auth							X								

OT.Lifecycle_Security (Lifecycle security) is provided by the SFR for SCD/SVD generation FCS_CKM.1, SCD usage FCS_COP.1 and SCD/SVD destruction FCS_CKM.4 which ensure cryptographically secure lifecycle of the SCD/SVD. 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_AFC.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 (Authorised SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The SFR FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute initialisation. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute “SCD operational” of the SCD.

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

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

OT.SCD_Secrecy (Secrecy of signature creation data) is provided by the security functions specified by the following SFR. 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 electronic 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 ensures 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 creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. 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. To authenticate user for user certification, user can activate alternative authentication methods in accordance with FIA_UAU.5. FIA_UAU.4 makes sure that unique authentication sessions shall be used every time. The authentication method is provided by the cryptographic algorithms specified by FCS_COP.1/Ext_Auth, which ensures the verification of the user. The cryptographic key is imported in accordance with FDP_ITC.1/Ext_Auth and FDP_RIP.1 and FCS_CKM.4/Ext_Auth ensure that residual information on the key is destroyed after the the key has been use for verification of user and that destruction of the key leaves no residual information. FDP_ACC.1/Ext_Auth and FDP_ACF.1/Ext_Auth provide access control based on the security attributes managed according to the FMT_MSA.1/Ext_Auth and FMT_MSA.3/Ext_Auth. These ensure that the key import process is restricted 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_SSCD_Auth (Authentication proof as SSCD) requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by FIA_API.1 (Authentication Proof of Identity). The SFR FIA_UAU.1 allows (additionally to the core PP) establishment of the trusted channel before (human) user is authenticated.

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.

OT.RND (Provide sufficient quality of random numbers) requires countermeasures that a random number to be generated has sufficient quality and makes it difficult to be guessed by an attacker. FCS_RNG.1 requires generation of random numbers satisfying a quality metric needed.

OT.Hash (*Provide capability of hash calculation*) requires capability of the hash calculation. FCS_COP.1/Hash requires calculation of hash that meet the secure hash standard.

Table 6-4 Satisfaction of dependencies of security functional requirements

SFRs	Dependencies	Satisfied by
FCS_CKM.1/SCD	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/SCD, FCS_CKM.4/SCD
FCS_CKM.4/SCD	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/SCD
FCS_COP.1/SCD	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/SCD, FCS_CKM.4/SCD
FDP_ACC.1/SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACF.1/SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACC.1/SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACF.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_RIP.1	No dependencies	n/a
FDP_SDI.2/Persistent	No dependencies	n/a
FDP_SDI.2/DTBS	No dependencies	n/a
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	No dependencies	n/a

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_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
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_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_SMF.1	No dependencies	n/a
FPT_EMS.1	No dependencies	n/a
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
FIA_API.1	No dependencies	n/a
FDP_DAU.2/SVD	FIA_UID.1	FIA_UID.1
FTP_ITC.1/SVD	No dependencies	n/a
FCS_CKM.4.1/Ext_Auth	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1/Ext_Auth
FCS_COP.1.1/Ext_Auth	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FDP_ITC.1/Ext_Auth, FCS_CKM.4.1/Ext_Auth
FCS_COP.1.1/Hash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Non-satisfied dependency because no key generation and destruction for hash necessary
FCS_RNG.1	No dependencies	n/a
FDP_ACC.1.1/Ext_Auth	FDP_ACF.1	FDP_ACF.1.1/Ext_Auth
FDP_ACF.1.1/Ext_Auth	FDP_ACC.1, FMT_MSA.3	FDP_ACF.1.1/Ext_Auth, FMT_MSA.3/Ext_Auth
FDP_ITC.1/Ext_Auth	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3	FDP_ACF.1.1/Ext_Auth, FMT_MSA.3/Ext_Auth

FIA_UAU.4	No dependencies	n/a
FIA_UAU.5	No dependencies	n/a
FMT_MSA.1/Ext_Auth	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1.1/Ext_Auth, FMT_SMR.1, FMT_SMF.1
FMT_MSA.3/Ext_Auth	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Ext_Auth, FMT_SMR.1

6.4. **Security assurance requirements rationale**

To meet the assurance expectations of customers, the assurance level EAL4 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 are chosen. The assurance level of EAL4 is selected because it provides a sufficient level of assurance for this type of TOE, which is expected to protect high value assets. Explanation of the security assurance component ALC_DVS.2 and AVA_VAN.5 follows:

- ALC_DVS.2 Sufficiency of security measures: This Security Target selects ALC_DVS.2 instead of ALC_DVS.1 because it verifies the security measures that provide the necessary level of protection to maintain the confidentiality and integrity of the TOE and its user data.
- AVA_VAN.5 Highly resistant: The TOE might be in danger of high-level attacks such as those it might encounter in a university laboratory. Therefore, AVA_VAN.5 is augmented to confirm that TOE has a high level of resistance against such attacks.

7. TOE summary specification

This section describes how the TOE is intended to comply with the Security Functional Requirements.

Table 7-1 Summary specification of the security functional requirements in the TOE

SFR	Summary specification
Security assurance requirements taken from the PP Part 2	
FCS_CKM.1/SCD	The TOE provides the RSA key generation algorithm and specified cryptographic key size of 2048 bit according to [PKCS #1] and [FIPS 186-4].
FCS_CKM.4/SCD	Deletion of the cryptographic key for signature creation requires either overwriting it with a new key or deleting the key when JPKI applet deletion. The destruction of the SCD is done at least on demand of the signatory.
FCS_COP.1/SCD	The TOE provides the cryptographic operation for digital signature creation in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes 2048 bit that meet the following: RSASSA-PKCS1-v1_5.
FDP_ACC.1/SCD/SVD_Generation	The TOE provides the access control to generate SCD/SVD against S.User associated with the security attribute “SCD / SVD Management”. S.User with the security attribute “SCD / SVD Management” set to “authorised” is allowed to generate SCD/SVD pairs.
FDP_ACF.1/SCD/SVD_Generation	
FDP_ACC.1/SVD_Transfer	The TOE provides the access control to transfer SVD against S.User associated with the security attribute Role. R.Admin is allowed to export SVD.
FDP_ACF.1/SVD_Transfer	
FDP_ACC.1/Signature_Creation	The TOE provides the access control to create an electronic signature against S.User associated with the security attribute “Role” and the SCD with the security attribute “SCD Operational”. R.Sigy is allowed to create electronic signatures for DTBS/R with SCD in which the security attribute “SCD operational” is set to “yes.”
FDP_ACF.1/Signature_Creation	
FDP_RIP.1	Any previous information content of a resource is made unavailable upon the de-allocation of the resource from the cryptographic buffer.
FDP_SDI.2/Persistent	The TOE monitors user data stored in containers controlled by the TOE for integrity errors on all objects, based on the following attributes: integrity checked stored data. Upon detection of a data integrity error, the TOE prohibits the sending of the altered data and informs the S.Sigy about the integrity error.
FDP_SDI.2/DTBS	The TOE monitors user data stored in containers controlled by the TOE for integrity error on all objects, based on following attributes: integrity checked stored DTBS. Upon detection of a data integrity error, the TOE prohibits the send of the altered data and informs the S.Sigy about integrity error.

SFR	Summary specification
FIA_AFL.1	If the counter reaches its maximum value, the RAD is blocked and cannot be used anymore.
FIA_UAU.1	No signature creation function can be invoked before the signatory is identified and authenticated. TOE allows self-test according to FPT_TST, selecting File, reading some files without authentication, and generating random numbers before the user is authenticated.
FIA_UID.1	
FMT_MOF.1	Only authenticated signatory can create digital signature.
FMT_MSA.1/Admin	The SCD usage is ensured by access control which is based on the security attribute secure TSF management according to these SFRs. The security attributes of the authenticated user are provided by FMT_MSA.2, and FMT_MSA.3 for static attribute initialisation. The security attribute SCD/SVD management can be modified by R.Admin only by FMT_MSA.1/Admin. The security attribute SCD operational can be modified by R.Sigy only by FMT_MSA.1/Signatory. The security attribute SCD operational can be modified by R.Sigy only by FMT_MSA.4. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. Administrator can create the RAD, and signatory can modify the RAD.
FMT_MSA.1/Signatory	
FMT_MSA.2	
FMT_MSA.3	
FMT_MSA.4	
FMT_MTD.1/Admin	
FMT_MTD.1/Signatory	
FMT_SMR.1	FMT_SMR.1 and FMT_SMF.1 list management functions and the role. The administrator and signatory roles are distinguished by security conditions. The TOE provides the following management functions: The creation and modification of the RAD, enables the signature creation function, modification of the security attribute SCD/SVD management, SCD operational, and modification of the default value of the security attribute SCD Identifier.
FMT_SMF.1	
FPT_EMS.1	Leakage of confidential data through side channels is prevented by the security features of the platform.
FPT_FLS.1	In case self-test fails or a physical attack is detected, the TOE resets the session and returns an error.
FPT_PHP.1	Detection of physical attack and resistance to physical attack

SFR	Summary specification
FPT_PHP.3	are achieved by platform functionalities.
FPT_TST.1	Self-testing is provided by the Java Card platform during initial start-up or before running a secure operation.
Security assurance requirements taken from the PP Part 4	
FIA_API.1	The TOE provides a device authentication mechanism in accordance with [GP_D] to prove the identity of the SSCD.
FDP_DAU.2/SVD	The TOE provides a capability to generate evidence that can be used as a guarantee of the validity of SVD. SVD is sent to CGA via a trusted channel in accordance with FTP_ITC.1/SVD.
FTP_ITC.1/SVD	FTP_ITC.1/SVD requires the TSF to enforce a trusted channel established by the CGA to export the SVD to the CGA in accordance with [GP_D]. Moreover, the TSF requires the use of the same trusted channel for the import of certificate info from the CGA.
Security assurance requirements defined in the ST	
FCS_CKM.4.1/Ext_Auth	Deletion of the cryptographic key for signature creation requires either overwriting it with a new key for External authentication or deleting the key when JPKI Applet deletion.
FCS_COP.1.1/Ext_Auth	The TOE provides the cryptographic operation for digital signature verification for External authentication in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes 2048 bit that meet the following: RSASSA-PKCS1-v1_5.
FCS_COP.1/Hash	The TOE provides the cryptographic operation for hash calculation in accordance with a specified cryptographic algorithm SHA-256 that meets the following: FIPS 180-4. . The hash is used for device authentication by SP-TSM
FCS_RNG.1	The TSF shall provide a deterministic random number generator, and the quality metrics of the random numbers shall meet class DRG.3 of AIS 20. The random number is used in External authentication.
FDP_ACC.1.1/Ext_Auth	The TOE provides the access control to write a public key for External authentication against S.User associated with the security attribute “Role” and the SCD with the security attribute “SCD Operational”. R.Sigy is allowed to write a public key for External authentication with the security attribute “SCD operational” set to “yes.”
FDP_ACF.1.1/Ext_Auth	
FDP_ITC.1/Ext_Auth	A public key for External authentication is imported in accordance with the public key import SFP.

SFR	Summary specification
FIA_UAU.4	The random numbers are generated anew each time External authentication using a public key for External authentication is started and are discarded each time the TOE exits the authenticated state.
FIA_UAU.5	The TOE provides multiple authentication mechanisms. The default authentication mechanism is “Password authentication”. If the user activates alternative methods via SCA, “External authentication with public key” is used.
FMT_MSA.1/Ext_Auth	The security attribute SCD operational can be modified by R.Sigy only.
FMT_MSA.3/Ext_Auth	The TOE enforces the public key for External authentication import SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allow the R.Admin to specify alternative initial values to override the default values when an object or information is created.

8. References

[AIS20] Anwendungshinweise und Interpretationen zum Schema (AIS), Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[BSI-PP-0084] Security IC Platform Protection Profile with augmentation Packages– BSI-CC-PP-0084-2014

[CC CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, CCMB-2017-04-004, April 2017.

[CC Part 1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017

[CC Part 2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017

[CC Part 3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017.

[FIPS 186-4] FIPS PUB 186-4-2013: Digital Signature Standard, Federal Information Processing Standards Publication, 2013, July, National Institute of Standards and Technology

[GP] GlobalPlatform Card Specification 2.3.1, GPC_SPE_034, March 2018.

[GP_D] GlobalPlatform Card Technology Secure Channel Protocol ’03’ - Amendment D v1.2, GPC_SPE_014, April 2020.

[JC-PP] Java card protection profile - open configuration n, published by oracle, inc., Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0099-V2-2020, Version 3.1.

[JC-SPEC] Java Card Platform Virtual Machine Specification, Classic Edition Version 3.1:2021

[JPKI-IF] Commercial Applet for Mobile JPKI Projects External Interface Specification Version 1.0

[JPKI-IP] JPKI applet Installation procedure Version 1.2

[JPKI-PRE] JPKI applet Delivery and acceptance procedure Version 1.0

[JPKI-UGM] JPKI applet User guidance Version 1.0

[PKCS #1] PKCS #1: RSA Cryptography Standard, Version 2.2, October 27, 2012, RSA Laboratories

[PP-PN] Personal Number card protection profile version, certified under the reference JISEC ITC-4485, version 1.00, April 2014

[SP800-22] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Revised: April 2010

[SSCD2] BSI-CC-PP-0059-2009-MA-02 Common Criteria Protection Profile: EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, CEN/ISSS - Information Society Standardization System, 18 May 2013

[SSCD4] BSI-CC-PP-0071-2012-MA-01 Common Criteria Protection Profile: EN 419211-4:2013 - Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application, CEN/ISSS - Information Society Standardization System, 12 October 2013