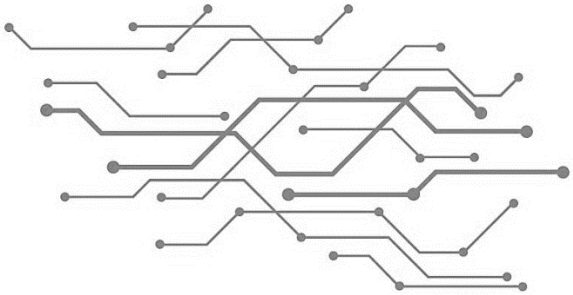

Security Target Lite

AKD eID 2.0 SSCD

Abstract

This document is the security target for the Common Criteria certification of the smart card AKD eID 2.0 SSCD as a qualified signature creation device and qualified seal creation device in accordance with Article 29 and Article 39 of Regulation (EU) No. 910/2014.

Keywords

Common Criteria, Security Target, Secure Signature Creation Device, SSCD, Qualified Electronic Signature/Seal Creation Device, QSCD

Document Information

Author: VBM, AKD d.o.o.
Title: Security Target Lite AKD eID 2.0 SSCD
Version: v2.4
Date: 20.09.2024.
Company: AKD d.o.o., Savska cesta 31, 10000 Zagreb, Croatia
Classification: Public

Document History:

Version	Date	Author	Descriptoin
2.1	20.05.2024.	VBM, AKD d.o.o.	ST-lite based on ST version 2.1, sanitised for publication.
2.2	01.07.2024.	VBM, AKD d.o.o.	ST-lite based on ST version 2.2, updated references.
2.3	02.09.2024.	VBM, AKD d.o.o.	ST-lite based on ST version 2.3, updated certification IDs.
2.4.	20.09.2024.	VBM, AKD d.o.o.	The alignment corrections.

CONTENTS

1. Introduction

1.1. ST and TOE reference

Document Title	Security Target Lite AKD eID 2.0 SSCD
Document Version	v2.4
Author	AKD d.o.o., VBM
PP Conformance:	EN 419 211 - Protection profiles for secure signature creation device - Part 2: Device with Key Generation, BSI-CC-PP-0059-2009-MA-02, [PP SSCD-2] - Part 3: Device with key import, BSI-CC-PP-0075-2012-MA-01, [PP SSCD-3] - Part 4: Extension for device with key generation and trusted channel to certificate generation application, BSI-CC-PP-0071-2012-MA-01, [PP SSCD-4] - Part 5: Extension for device with key generation and trusted channel to signature creation application, BSI-CC-PP-0072-2012-MA-01, [PP SSCD-5] - Part 6: Extension for device with key import and trusted channel to signature creation application, BSI-CC-PP-0076-2013-MA-01, [PP SSCD-6] Note: The term ”Core PPs” refers to Part 2 and Part 3
CC Version	Version 3.1. Revision 5. April 2017
Assurance level	EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 (EAL 4+)
Keywords	common criteria, security target, qualified signature creation device, qualified seal creation device, secure signature creation device, electronic signature, digital signature, key generation, key import, trusted communication
TOE Name	AKD eID 2.0 SSCD
TOE Developer	AKD d.o.o.
Platform	NXP JCOP 4.5 P71, NSCIB-CC-2300127-01-CR

This Security Target defines the security objectives and requirements for the Secure Signature Creation Device (SSCD) based on the requirements and recommendations of Regulation (EU) No 910/2014 [eIDAS Regulation].

The focus of this ST is on meeting the requirements for Qualified Signature Creation Devices and Qualified Seal Creation Devices according to Art. 29 and Art. 39 [eIDAS Regulation].

The eIDAS Regulation and the Implementing Decision (EU) 2016/650 [eIDAS Dis] assume compliance with these requirements if a QSCD has been evaluated according to the Common Criteria (version 3.1) and complies with one or more of the above EN 419 211 protection profiles for secure signature creation devices (PPs).

These protection profiles refer to the “*Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures*” with the term “the directive” [The Directive] which was repealed by the [eIDAS Regulation]. References to the repealed Directive shall be understood as references to the eIDAS regulation.

The target of the evaluation is the AKD eID 2.0 SSCD, which is contact/ contactless/dual interface smart card product intended for use as Secure Signature Creation Device (SSCD) or Qualified Signature Creation Device (QSCD).

The TOE combined security features of the mentioned protection profiles using the platform cryptographic operations and security features. All that enables the following product functionalities:

- On chip and external key generation
- Advanced or qualified digital signature
- Certificate information application
- Knowledge based user authentication with two PINs and one PUK
- Secure Messaging
- Symmetric or asymmetric device authentication
- Administrator role authentication and post issuance management of the card
- Signature Generation for SSL Client/Server Authentication
- Encryption key decipherment
- Certificate verification
- Self protection

The application interfaces to the TOE are implemented as is specified in [EN 419212]:

- User verification (PIN, Password or biometric) as described in [EN 419212]-2, clause 6,
- Signature creation as described in [EN 419212]-2, clause 7.1,
- Password-based authentication protocols as described in [EN 419212]-2, clause 8,
- Secure Messaging (AES in CMAC mode and AES in CBC mode) as described in [EN 419212]-2, clause 9,
- Key Generation as described in [EN 419212]-2, clause 10,
- Device authentication with privacy protection, as described in [EN 419212]-3, clause 3.6,
- Symmetric authentication scheme, as described in [EN 419212]-3, clause 3.8,
- Verification of card verifiable certificates as described in [EN 419212-3, clause 5.

All cryptographic algorithms, parameters and key sizes used by TOE are agreed and recommended by [SOG-IS] and [ETSI TS 119 312].

1.2. TOE overview

1.2.1. Usage and major security features of the TOE

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

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

(1) to generate or to import 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 SSCD 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 data to be signed or a unique representation 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 can be used for digital signature creation to conform to the specifications in ETSI EN 319 122 (CAdES), ETSI EN 319 132 (XAdES) and ETSI EN 319 142 (PAdES).

The TOE is prepared for the signatory's use by:

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

After preparation the SCD cannot be used before the signatory becomes into sole control over the SSCD.

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, the means of providing this information is expected to protect the confidentiality and the integrity of the corresponding RAD.

If the use of an SCD is no longer required, then it shall be destroyed (e.g. by erasing it from memory) as well as the associated certificate info, if any exists.

1.2.2. TOE description

User authentication

The user authentication is based on verification authentication data (VAD) checking mechanism.

Verification data to protect the use of the private key for signature creation is used on TOE. If there are multiple private keys for signature creation on TOE, their use can optionally be protected by different verification data.

The following methods of user verification are available:

- Knowledge based, where the user must enter a PIN /password that is compared to the VAD applied in the TOE
- Biometric based, where biometric data are converted to a password format and sent by the interface device, which is compared to the VAD applied in the TOE (match-on-card mechanism).

PACE with MRZ or CAN can also be used for user authentication (similar to PIN verification) in combination with establishing a secure channel with the connected user interface.

The TOE provides functions to create, verify, modify and unblock PIN, PUK, password, biometric data, MRZ or CAN.

To avoid brute-force attacks, a retry counter can be assigned to the PIN, PUK, password, biometric data, MRZ or CAN.

During the personalization of the TOE, knowledge, biometric and PACE authentication can be configured.

Device authentication

Device authentication is (mutual authentication) of the reading device and of the TOE.

The TOE implements the following device authentication protocols:

a) Password Based authentication (PACE) with generic mapping based on ECDH key agreement with provision of secure channel by secure messaging.
b) Asymmetric device authentication which comprises following mechanisms:
   - Elliptic curve Diffie-Hellman (ECDH) key exchange provides session keys for establishment of a secure channel,
   - Terminal Authentication provides a mechanism for restricting access to the TOE,
   - Chip Authentication verifies the authenticity of the TOE and
   - Secure authentication using Card Verifiable Certificates (CVC) and digital signatures.
c) Symmetric authentication using AES.

Secure messaging

Secure messaging session establishment begins with an device authentication.

The SM session always includes data confidentiality AND integrity. Data confidentiality only, or data integrity only are not supported. The SM policy for incoming data and outgoing data is the same.

The TOE implements the following:

- Data encryption/decryption AES in CBC mode.
- Message authentication code AES in CMAC mode.

Role authentication

Role authentication assigns different access rights to the administrator and signatory. When an entity wants to get authenticated to the ICC to gain access rights he has to prove it with a secret key or certificate presented during device authentication.

The TOE supports two mechanisms: symmetric role authentication and an asymmetric role authentication. In asymmetric role authentication Public keys are transported through Card Verifiable Certificates (CVC).

The TOE may grant different access rights to different entities to:

- install an SCD, generated outside the device in a trusted environment and communicated over a secure communication link,
- generate an SCD,
- disable an SCD it holds, e.g. by erasing it from memory,
- modify or unblock the PIN/PUK,
- create, extend or modify certificate info or card holder data stored in the device, and
- create SVD for an SCD stored and export it for certification by a CGA protected by trusted communication.

Crypto functions

The following cryptographic mechanisms are used:

a) Key generation with Brainpool or NIST elliptic curves 256 and 384 bits
b) Signature generation EC-DSA with SHA-256 or SHA-384,
c) AES CBC mode for data en-/decryption and AES in CMAC mode for message authentication code (for secure messaging),
d) AES 128 and 256 bits data encryption/decryption (for symmetric authentication),
e) ECDH key agreement with Brainpool or NIST elliptic curves 256 and 384 bits (for asymmetric device authentication) and

f) ECDH key agreement with with Brainpool or NIST elliptic curves 256 and 384 bits and generic mapping (for PACE).

All cryptographic functions of TOE are provided by the platform, i.e., either by the cryptographic library or by the operating system.

Self-protection

Self-protection provides the security protection of the TOE that implements the platform's security features such as:

- Applet firewall to enforcing access rules between different applets present on card,
- Secure deletion and executing the Java codes and APDU commands,
- Rollback mechanism and access control policy for the platform management functions,
- Protection against physical tampering and leakage.

1.2.3. The scope of the TOE

The TOE is made up of:

- NXP JCOP 4.5 P71 Java Card platform [CR Java]
- AKD eID 2.0 SSCD application
- The associated guidance document [USR_AKDeID]

The NXP JCOP 4.5 P71 Java Card platform is based on the NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), [CR IC].

The figure below shows the components of the TOE and its boundaries (red dashed line).

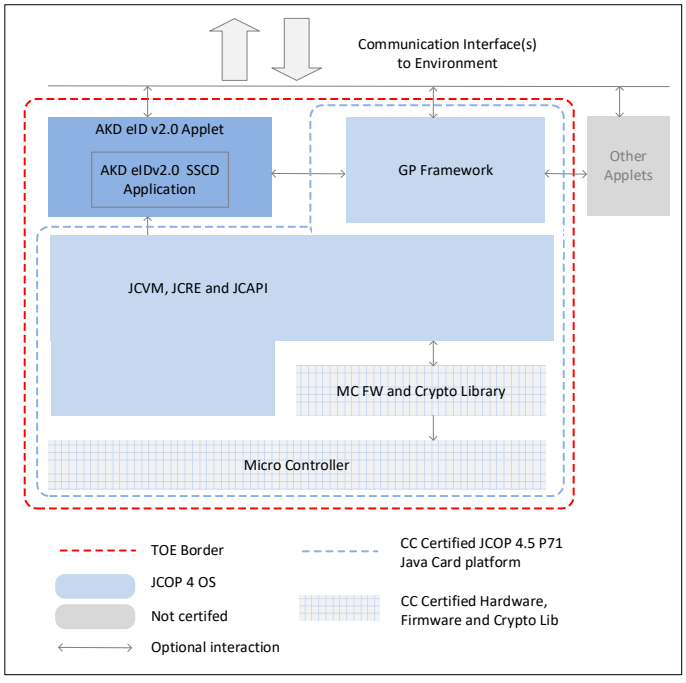

Figure 1 – Components of the TOE

The AKD eID 2.0 SSCD can be present as a stand-alone applet, but the TOE allows several additional multipurpose applets to be installed on a single card.

The AKD eID 2.0 SSCD can be combined with the national ICAO MRTD applets for identity cards and residence permits according to [ID Regulation] and [C2018 7767 final] or with other certified and non-certified applets such as eHealthcare, eDriving licence or access control. It is understood that support for such applets is optional and not included in this TOE.

The TOE supports a logical data structure for the European Citizen Card according to [CEN15480-2] and [PKCS#15], which allows several different applications to be present on the applet at the same time. All these applications operate independently and do not affect the functionality of TOE.

The AKD eID 2.0 SSCD is loaded last and no applet can be loaded in post-issuance. All bytecodes are verified before loading to ensure that each bytecode is valid at execution time.

The TOE supports contact-based T=1 (according ISO/IEC 7816-3) and contactless T=CL (according to ISO/IEC 14443) communication protocols.

The TOE can be delivered on smart card.

1.2.4. Non-TOE hardware/software/firmware required

The TOE is an independent product and does not need any additional non-TOE hardware, software, or firmware required by TOE to meet its claimed security features. The TOE consists of the chip and the complete operating system and application. A module holding the chip as well as an optional antenna, card body or carrier are irrelevant for the secure operation of the TOE and are therefore out of scope of the TOE.

To be powered and able to communicate, the TOE requires a reader and the terminal application that can provide the necessary environment for management and signing (including HID for VAD input).

1.3. Operation of the TOE

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

The preparation environment

- The TOE interacts with a certification service provider through a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with the 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 TOE interacts with a certification service provider (CSP) through a SCD/SVD generation application to import the signature creation data (SCD) and a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding to the SCD the certification service provider has generated. The SCD/SVD generation application transmits the SVD to the CGA.
- The initialization environment interacts further with the TOE to personalize it with the initial value of the reference authentication data (RAD).

The signing environment

- The TOE 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 data to be signed (DTBS), or a unique representation 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 environment

- The TOE 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. 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] if the certificate for the SVD is a qualified certificate (Annex I).
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 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. If the signature creation application handles, is requesting or obtaining a VAD from the user, it is assumed to protect the confidentiality and integrity of this data.
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:

- initialising the RAD,
- generating a key pair,
- storing personal information of the legitimate user,

The TOE is a smart card. A smart-card terminal shall be deployed that provides the required secure environment to handle a request for signatory authorization. A signature can be obtained on a document prepared by a signature creation application component running on personal computer connected to the card terminal. The signature creation application, after presenting the document to the user and after obtaining the authorization PIN initiates the digital signature creation function of the smart card through the terminal.

1.4. The TOE life cycle

The TOE lifecycle distinguishes stages for development production, preparation and operational use.
The development phase comprises the development and production of the TOE. The development phase is subject of the evaluation according to the assurance lifecycle (ALC) class. The development phase ends with the delivery of the TOE to the SSCD-provisioning service.

The operational usage of the TOE comprises the preparation stage and the operational use stage. In the preparation stage the personal information of the legitimate user is written and, optionally, one or more SCD/SVD pairs can be generated on the card or imported to the card together with the corresponding certificates by the SSCD-provisioning service
The TOE operational use stage begins when the signatory has obtained both the VAD and the TOE. Enabling the TOE for signing requires at least one set of SCD stored in its memory.
If an SCD/SVD key pair is not generated beforehand, the lifecycle allows the generation of an SCD/SVD key pair after the supply to the signatory.
The following figure shows an example of the lifecycle where an SCD/SVD pair is generated on the TOE before supply to the signatory. The lifecycle allow generation of SCD or SCD/SVD key pairs after delivery to the signatory as well.

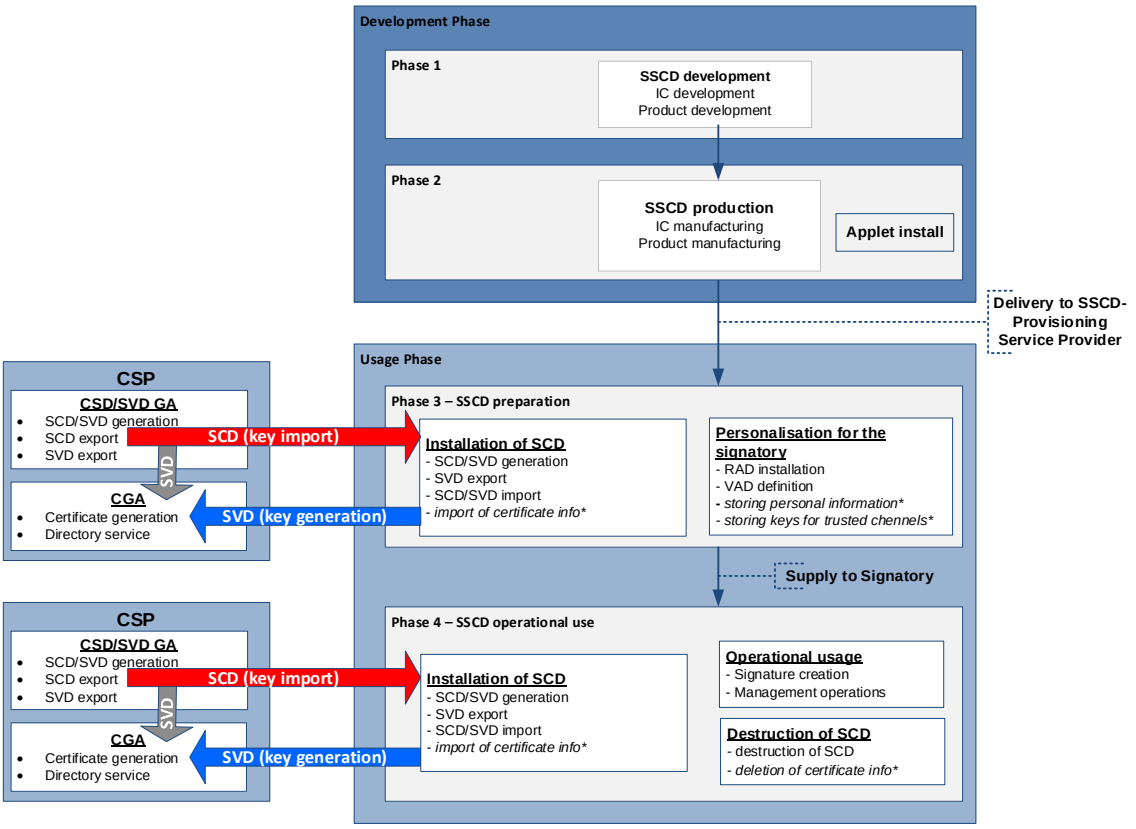

Figure 2 - TOE life cycle

An SSCD-provisioning service provider having accepted the TOE from a manufacturer prepares the TOE for use and delivers it to its legitimate user. The preparation phase ends when the legitimate user has received the TOE from the SSCD-provisioning service and any SCD it might already hold have been enabled for use in signing.
During preparation of the TOE, as specified above, an SSCD-provisioning service provider performs the following tasks:

(1) 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.
(2) Generate a PIN of the legitimate user, store this data as RAD in the TOE and prepare information about the VAD for delivery to the legitimate user.
(3) 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,

(4) Optionally, present certificate info to the SSCD.
(5) Deliver the TOE and the accompanying VAD info to the legitimate user.

The SVD certification task (third item listed above) of an SSCD-provisioning service provider as specified in [PP SSCD-2] supports a centralised, pre-issuing key generation process, with at least one key generated and certified, before supply to the legitimate user. Alternatively, or additionally, that task supports key generation by the signatory after delivery and outside the secure preparation environment. A TOE 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 (cf. [The Directive], 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 can be stored in the SSCD during personalization if key generated centrally before the TOE is delivered to the legitimate user.

Before initiating the actual certificate signature, the certificate generation 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 supports 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. Security requirements to protect the SVD export function and the certification data if the SVD is generated by the signatory and then exported from the SSCD to the CGA are specified in a [PP SSCD-4].

Prior to generating the certificate, the certification service provider asserts the identity of the signatory specified in the certification request as the legitimate user of the TOE.

Regarding the key import, an SSCD-provisioning service provider ensures the following tasks:

The preparation phase of the TOE lifecycle is processing the TOE from the customer's acceptance of the delivered TOE to a state ready for operation by the signatory. The customer receiving the TOE from the manufacturer is the SSCD-provisioning service that prepares and provides the SSCD to subscribers. The preparation includes

(1) The personalization of the TOE for use by the signatory, i.e. the installation of the RAD in the TOE and handover of VAD to the signatory.
(2) The initialization of the TOE, i.e. the CSP generates the SCD/SVD pair by means of a SCD/SVD generation device, loads the SCD to the TOE, and sends the SVD to the CGA. The TOE may import and store the SCD/SVD pair.
(3) The generation of the (qualified) certificate containing among others (cf. [The Directive], 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.

(4) The preparation may include optional loading of the certificate info into the SSCD for signatory convenience.

The CSP generates a SCD/SVD pair and imports SCD, and optionally also SVD, into the SSCD. The CSP ensures

(a) the correspondence between SCD and SVD,
(b) that algorithm and key size for the SVD are appropriate.

Please take note that verifying whether the claimed identity of the signer originates from that given SSCD has to be done by the CSP operating the CGA.

If the TOE is used for creation of advanced electronic signatures, the certificate links the signature verification data to the person (i.e. the signatory) and confirms the identity of that person (cf. [The Directive], article 2, clause 9).

The TOE provides mechanisms for import of SCD, implementation of the SCD and personalization. The environment is assumed to protect all other processes for TOE preparation like SCD transfer between the SCD/SVD generation device and the TOE, and SVD transfer between the SCD/SVD generation device and the CGA. The CSP may export the SVD to the TOE for internal use by the TOE (e.g., self-test).

Before generating a (qualified) certificate, the CSP is expected to first store the SCD in a SSCD. A secure channel with the TOE may be used to support this, by ensuring integrity of the SCD during transmission to the TOE.

Regarding key generation and trusted channel to certificate generation application an SSCD-provisioning service provider ensures the following tasks:

- In the preparation stage of the usage phase, the SSCD-provisioning provider additionally initializes the security functions in the TOE for the identification as SSCD, for the proof of this SSCD identity to external entities, and for the protected export of the SVD.
- In the preparation stage of the usage phase, the SSCD-provisioning provider additionally links the identity of the TOE as SSCD and the identity of the legitimate user as potential applicant for certificates for SVD generated by the TOE.

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

The TOE operational use stage begins when the signatory has obtained both the VAD and the TOE. Enabling the TOE for signing requires at least one set of SCD stored in its memory.

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 supports functions to generate additional signing keys and 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. If the conditions to obtain a qualified certificate are met the new key can also be used to create advanced electronic signatures.

The TOE functions for additional key generation and certification require additional security functions in the TOE and an interaction with the SSCD-provisioning service provider in an environment that is secure. It includes:

- 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.

- In the usage phase, before generating the certificate including the SVD exported from the TOE, the CGA additionally establishes (1) the identity of the TOE as SSCD, (2) that the originating SSCD has been personalized for the applicant for the certificate as legitimate user, and (3) the correspondence between SCD stored in the SSCD and the received SVD.

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

1.5. TOE delivery

The delivery includes the following items:

TOE component	Form of delivery	Delivery method
AKD eID 2.0 SSCD	Application Software loaded onto the contact, contactless or dual interface smart card. TOE identification INS_GET_VERSION 0x020002000072657638 (2.0 rev8)	Trusted courier delivery Note: The TOE is protected by a Transport Key during the transfer between AKD Manufacturing and the SSCD Provisioning Service site.
User Guidance AKD eID 2.0 SSCD v1.12.pdf	Electronic document	PGP encrypted file via AKD cloud platform

2. Conformance claims

2.1. CC conformance claim

This Security Target claims to be conformant to the Common Criteria version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001 [CC P1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002 [CC P2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003 [CC P3]

For the evaluation the following methodology will be used:

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

Conformance to the Common Criteria version 3.1 is claimed as follows:

- Part 1: conformant
- Part 2: extended with
  - FIA_API Authentication proof of identity
  - FPT_EMS TOE emanation
- Part 3: conformant

2.2. PP claim

This ST claims to be strict conformant to the Protection Profiles:

- EN 419211-2:2013 Protection profiles for secure signature creation device - Part 2: Device with Key Generation, Version 2.0.1., 2013, registered and certified under the reference BSI-CC-PP-0059-2009-MA-02, [PP SSCD-2],
- EN 419211-3:2013 Protection profiles for secure signature creation device - Part 3: Device with key import, Version 1.0.2, 2012-07-24, registered and certified under the reference BSI-CC-PP-0075-2012-MA-01, [PP SSCD-3],
- 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, Version 1.0.1, 2013-11-27, registered and certified under the reference BSI-CC-PP-0071-2012-MA-01, [PP SSCD-4],
- EN 419211-5:2013 Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application, Version 1.0.1, 2012-11-14, registered and certified under the reference BSI-CC-PP-0072-2012-MA-01 [PP SSCD-5], and
- EN 419211-6:2013 Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application, Version 1.0.4, registered and certified under the reference BSI-CC-PP-0076-2013-MA-01, [PP SSCD-6] .

The basis of this composite evaluation is:

- NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), BSI-DSZ-CC-1149-V3-2023, [CR IC],
- NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), Security Target lite, Version 1.8, 2023-12-01, [ST IC],
- NXP JCOP 4.5 P71, NSCIB-CC-2300127-01-CR, 16 January 2024 [CR Java] and
- JCOP 4.5 P71 Security Target Lite, Rev. 2.6, 11 December 2023, [ST Java].

2.3. Package claim

This Security Target claims conformance to the assurance package EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

2.4. Conformance rationale

This ST combining the functionalities of the PPs. This implies for this ST:

(1) The parts taken from the PPs are included in this ST exactly in the same wording as the PPs.

(2) The application notes from the PPs are changed or explained in this ST, and the additional note was added by the author of the ST.

(3) All definitions of the security problem definition (SPD), security objectives and security functional requirements in this ST have been taken from the PPs.

(4) The [PP-SSCD-6] does not include any additional security objectives, SFRs and SARs that is not included in the [PP SSCD-3] and the [PP SSCD-5].

(5) The SPD in the [PP SSCD-3], [PP SSCD-4] and [PP_KG_TCSCA include all the SPD of the [PP SSCD-2]. The SPD for the [PP SSCD-3] add the additional assumption A.CSP, which is not present in [PP SSCD-2].

(6) The OT.SCD/SVD_Auth_Gen of the [PP SSCD-2] is correspondent to the OT.SCD/SVD_Gen in [PP SSCD-4] and [PP SSCD-5].

(7) Security objectives for the TOE in the [PP SSCD-2], which are identically stated in the [PP SSCD-3], are OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID and OT.Tamper_Resistance

(these are independent from the fact whether SCD are generated by the TOE itself or imported from the operational environment).

(8) The remaining security objectives for the TOE in the [PP SSCD-2] OT.SCD/SVD_Auth_Gen, OT.SCD_Unique and OT.SCD_SVD_Corresp cover different aspects of the SCD/SVD generation by the TOE and are not present in [PP SSCD-3]. Instead, in [PP SSCD-3] the analogous security objectives for the operational environment OE.SCD/SVD_Auth_Gen, OE.SCD_Unique and OE.SCD_SVD_Corresp are defined, as with key import the operational environment is responsible for the key generation.

(9) The remaining security objective for the TOE OT.SCD_Auth_Imp in the [PP SSCD-3] is related to SCD import only and is therefore not present in [PP SSCD-2].

(10) The TOE type of the [PP SSCD-4] is the same as the TOE type of the core [PP SSCD-2]: the TOE is a combination of hardware and software configured to securely create, use and manage signature creation data.

(11) The security problem definition (SPD) of the [PP SSCD-4] contains the security problem definition of the core [PP SSCD-2]. The SPD for it is described by the same threats, organisational security policies and assumptions as for the TOE in core [PP SSCD-2].

(12) The security objectives for the TOE in the [PP SSCD-4] include all the security objectives for the TOE of the core [PP SSCD-2] and add the security objective OT.TOE_SSCD_Auth (Authentication proof as SSCD) and OT.TOE_TC_SVD_Exp (Trusted channel for SVD).

(13) The security objectives for the operational environment in the [PP SSCD-4] include all security objectives for the operational environment of the core [PP SSCD-2] except OE.SSCD_Prov_Service. It substitutes OE.SSCD_Prov_Service by OE.Dev_Prov_Service and adds OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp in order to address the extended security functionality of the TOE and methods of use.

(14) The SFRs specified in the [PP SSCD-4] includes all security functional requirements (SFRs) specified in the core [PP SSCD-2]. It includes additional SFRs FIA_API.1, FDP_DAU.2/SVD and FTP_ITC.1/SVD.

(15) The [PP SSCD-4] does not provide completion of all operations in the core [PP SSCD-2]. It provides operation of the SFR FIA_UAU.1 of the core PP.

(16) The SARs specified in the [PP_KG_TCGA] includes all SAR specified in the core [PP SSCD-2]. It does not include additional SAR not included in the core [PP SSCD-2].

(17) The security objectives for the TOE in the [PP SSCD-5] and the [PP-SSCD-6] include all the security objectives for the TOE of the core PPs and add the security objective OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import) and OT.TOE_TC_DTBS_Imp (Trusted channel for DTBS).

(18) The security objectives for the operational environment in the [PP SSCD-5] and the [PP SSCD-6] include all security objectives for the operational environment of the core PPs except OE.HID_VAD and OE.DTBS_Protect. It adapts OE.HID_VAD and OE.DTBS_Protect to the support provided by the TOE by new security functionality (cf. OT.TOE_TC_VAD_Imp, OT.TOE_TC_DTBS_Imp) provided by the TOE and changes them into OE.HID_TC_VAD_Exp and OE.SCA_TC_DTBS_Exp.

(19) The SFRs specified in the [PP SSCD-5] and the [PP SSCD-6] includes all security functional requirements (SFRs) specified in the core PPs. Additional SFRs address trusted channel between the TOE and the SCA: FDP_UIT.1/DTBS, FTP_ITC.1/VAD and FTP_ITC.1/DTBS.

(20) The [PP SSCD-5] and the [PP SSCD-6] does not provide completion of all operations in the core PPs. It provides refinements for the SFR FIA_UAU.1 of the core PP.

(21) The SARs specified in the [PP SSCD-5] and the [PP SSCD-6] includes all SAR as specified in the core [PP SSCD-2]. It does not include additional SAR not included in the core PPs.

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 an electronic 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 electronic 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 electronic signature must be maintained.

Users 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 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.
3. 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.

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. Organisational 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. 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.

3.4. Assumptions

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.

Assumption regarding key import:

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

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

4. Security objectives

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organizational security policies and assumptions.

4.1. Security objectives for the TOE

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.

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_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.

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

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

OT.SCD_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_Auth_Imp **Authorized SCD import**

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

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.TOE_TC_VAD_Imp **Trusted channel of TOE for VAD import**

The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed.

Note: This security objective for the TOE is partly covering OE.HID_VAD from the core PPs. While OE.HID_VAD in the core PPs requires only the operational environment to protect VAD, [PP SSCD-5] and [PP SSCD-6] require the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore, [PP SSCD-5] and [PP SSCD-6] re-assign partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

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.

Note: This security objective for the TOE is partly covering OE.DTBS_Protect from the core PPs. While OE.DTBS_Protect in the core PPs requires only the operational environment to protect DTBS, [PP SSCD-5] and [PP SSCD-6] require 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, [PP SSCD-5] and [PP SSCD-6] re-assign 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.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.

Note: 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.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.SCD/SVD_Auth_Gen **Authorized SCD/SVD generation**

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

OE.SCD_Secrecy ***SCD Secrecy***

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

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

The CSP shall ensure the cryptographic quality of the SCD/SVD pair, which is generated in the environment, for the qualified or advanced electronic signature. The SCD used for signature creation shall practically occur only once, i.e. the probability of equal SCDs shall be negligible, and the SCD shall not be reconstructable from the SVD.

OE.SCD_SVD_Corresp **Correspondence between SVD and SCD**

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

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.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.

The developer prepares the TOE by pre-initialisation for the delivery to the customer (i.e. the SSCD provisioning service) in the development phase not addressed by a security objective for the operational environment. The SSCD Provisioning Service performs initialisation and personalisation as TOE for the legitimate user (i.e. the Device holder). If the TOE is delivered to the Device holder with SCD the TOE is a SSCD. This situation is addressed by OE.SSCD_Prov_Service except the additional initialisation of the TOE for proof as SSCD and trusted channel to the CGA. If the TOE is delivered to the Device holder without a SCD the TOE will be a SSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the signatory in the operational use stage the TOE provides additional security functionality addressed by OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp. But this security functionality must be initialised by the SSCD Provisioning Service as described in OE.Dev_Prov_Service. Therefore the [PP SSCD-4] substitutes OE.SSCD_Prov_Service by OE.Dev_Prov_Service allowing generation of the first SCD/SVD pair after delivery of the TOE to the Device holder and requiring initialisation of security functionality of the TOE. Nevertheless the additional security functionality must be used by the operational environment as described in OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp. This approach does not weaken the security objectives of and requirements to the TOE but enforce more security functionality of the TOE for additional method of use. Therefore it does not conflict with the CC conformance claim to the core [PP SSCD-2].

OE.HID_TC_VAD_Exp Trusted channel of HID for VAD export

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.

Note: This security objective for the environment partially covers OE.HID_VAD from the core PPs. While OE.HID_VAD in the core PPs requires only the operational environment to protect VAD, [PP SSCD-5] and [PP SSCD-6] require the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore

[PP SSCD-5] and [PP SSCD-6] re-assign partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

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.

Note: This security objective for the environment partly covers OE.DTBS_Protect from the core PPs. While OE.DTBS_Protect in the core PPs require only the operational environment to protect DTBS, [PP SSCD-5] and [PP SSCD-6] require 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, [PP SSCD-5] and [PP SSCD-6] re-assign 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 coverage

The following tables show how the security objectives for the TOE and the security objectives for the environment cover the threats, organizational security policies and assumptions.

Table 1: Mapping of security problem definition to security objectives for the TOE

	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Auth_Imp	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
T.SCD_Divulg		X										X				
T.SCD_Derive			X						X	X						
T.Hack_Phys		X				X	X	X								
T.SVD_Forgery											X			X		
T.SigF_Misuse	X			X	X										X	X
T.DTBS_Forgery					X											X
T.Sig_Forgery			X							X						
P.CSP_QCert	X										X	X	X			
P.QSign			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

Table 2: Mapping of security problem definition to security objectives for the operational environment

	OE.CGA_QCert	OE.SVD_Auth	OE.DTBS_Intend	OE.Signatory	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.Dev_Prov_Service	OE.CGA_SSCD_Auth	OE.CGA_TC_SVD_Imp	OE.HID_TC_VAD_Exp	OE.SCA_TC_DTBS_Exp
T.SCD_Divulg					X	X							
T.SCD_Derive							X						
T.Hack_Phys													
T.SVD_Forgery		X						X			X		
T.SigF_Misuse			X	X								X	X
T.DTBS_Forgery			X										X
T.Sig_Forgery	X						X						
P.CSP_QCert	X				X			X		X			
P.QSign	X		X										
P.Sigy_SSCD					X	X	X		X	X	X		
P.Sig_Non-Repud	X	X	X	X	X	X	X	X	X	X	X	X	X
A.CGA	X	X											
A.SCA			X										
A.CSP					X	X	X	X					

4.3.2. Threats

T.SCD_Divulg (St*oring, 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 during use by the TOE for signature creation

OE.SCD_Secrecy, which assures the secrecy of the SCD in the CSP environment,

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

- OT.SCD_Auth_Imp, which ensures that only authorised SCD import is possible, (when SCD is generated off-TOE).

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_Unique counters this threat by implementing cryptographically secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographically secure electronic signatures.

(This item is extended with Part 3) OE.SCD_Unique counters this threat by implementing cryptographically secure generation of the SCD/SVD pair.

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 , which 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.SVD_Forgery deals with the forgery of the SVD given to the CGA for certificate generation. T.SVD_Forgery is addressed by

- OE.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD, and
- OE.SVD_Auth, which ensures the authenticity of the SVD given to the CGA of the CSP.

T.SigF_Misuse (*Misuse of the signature creation function of the TOE*) addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create 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 (Security obligation of the 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 (Security obligation of the signatory) ensures also that the signatory keeps their VAD confidential.

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 form 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_TC_VAD_Exp (Trusted channel of HID for VAD) requires the HID to protect the confidentiality and the integrity of the VAD as needed by the authentication method employed. The HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD).

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.

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, OE.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 and OE.SCD_Unique ensure 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.

4.3.3. Organisational security policies

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

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- OE.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.

- OE.SCD/SVD_Auth_Gen, which ensures that the SCD/SVD generation can be invoked by authorized users only,
- OT.SCD_Auth_Imp which ensures that authorised users only may invoke the import of the SCD,
- OE.SCD_SVD_Corresp, which requires the CSP to ensure the correspondence between the SVD and the SCD during their generation, and
- 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.

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]. 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.
- OE.SCD_Unique meets the paragraph 1(a) of the directive [The Directive], Annex III, by the requirements that the SCD used for signature creation can practically occur only once.
- OE.SCD_Unique, OT.SCD_Secrecy and OE.SCD_Secrecy meet the paragraph 1(a) of the directive [The Directive], Annex III, by the requirements to ensure the secrecy of the SCD.
- OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of 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.

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

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

- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialisation, personalisation and operational usage,
- OT.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.
- OT.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only, and
- OE.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only,
- OT.SCD_Auth_Imp, which limits SCD import to authorised users only,
- OE.SCD_Secrecy, which ensures the confidentiality of the SCD during generation and export to the TOE, and deletes the SCD after export to the TOE. The CSP does not use the SCD for signature creation.

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, that ensure the aspects of signatory's sole control over and responsibility for the electronic signatures generated with the TOE.

OE.Dev_Prov_Service ensures that the signatory uses an authentic TOE, initialised and personalised for the signatory.

OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory.

OE.SVD_Auth and OE.CGA_QCert require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory.

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, 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.

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

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.

The confidentiality of VAD is protected during the transmission between the HI device and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD). 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 generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS.

4.3.4. Assumptions

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 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.

(This item is extended with [PP SSCD-3])

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

5. Extended component definition

This Security Target uses the following extended components:

- FPT_EMS and
- FIA_API.

No other components are used.

5.1. Definition of the family FPT_EMS

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

FPT_EMS TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component Leveling:

FPT_EMS TOE Emanation

FPT_EMS.1 TOE Emanation has two constituents:

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

Management: FPT_EMS.1

There are no management activities foressen.

Audit: FPT_EMS.1

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

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit [assignment: *types of emission*] 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*].

5.2. Definition of the family FIA_API

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

FIA_API Authentication proof of identity

Family behaviour

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component Leveling:

FIA_API.1 Authentication Proof of Identity

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication proof of identity

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

6. Security requirements

6.1. Security functional requirements

6.1.1. Cryptographic support (FCS)

FCS_CKM.1 *Cryptographic key generation*

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 *ECDSA* and specified cryptographic key sizes *256 and 384 bits* that meet the following: *[ISO/IEC 14888-3] and [FIPS 186-4].*

Note: Used elliptic curves parameters are NIST P-256 and NIST P-384 according to [FIPS 186-4] and Brainpool P256r1 and Brainpool P384r1 according to [RFC 5639].

FCS_CKM.4 *Cryptographic key destruction*

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 ***physically overwriting the keys in a randomized manner*** that meets the following: ***none.***

Note: The corresponding Module for the ECC cryptographic operation is present in the TOE.

FCS_COP.1/Signature_Creation *Cryptographic operation – Signature Creation*

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/ Signature_Creation	The TSF shall perform *digital signature creation* in accordance with a specified cryptographic algorithm *ECDSA sign with hash in SHA256, SHA384* and cryptographic key sizes *256 and 384 bits* that meet the following: *[ISO/IEC 14888-3] and [FIPS 186-4].*

Note: The certified curves and bit length for ECDSA are listed in note of FCS_CKM.1.1.

FCS_COP.1/SM-ENC *Cryptographic operation – Secure messaging - Encryption*

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/ SM-ENC	The TSF shall perform *data encryption/decryption for secure messaging* in accordance with a specified cryptographic algorithm *AES in CBC mode* and cryptographic key sizes *128, 256 bits* that meet the following: [FIPS 197], [NIST SP800-38A] *and* [EN 419212].

Note: This SFR requires that the TOE implements the cryptographic algorithm the AES in CBC mode for secure messaging with encryption of the transmitted data and the nonce during PACE, as described in [EN 419212]-2, clause 8, during asymmetric device authentication described in [EN 419212]-3, clause 3.6 and during symmetric authentication defined in [EN 419212]-3, clause 3.8.

FCS_COP.1/SM-MAC *Cryptographic operation – Secure messaging - MAC*

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/ SM-MAC	The TSF shall perform *message authentication code for secure messaging* in accordance with a specified cryptographic algorithm *AES in CMAC mode* and cryptographic key sizes *128, 256 bits* that meet the following: [FIPS 197], [NIST SP 800-38B] *and* [EN 419212].

Note: This SFR requires that the TOE implements the cryptographic algorithm AES in CMAC mode for secure messaging with message authentication code over transmitted data during PACE, as described in [EN 419212]-2, clause 8. The message authentication code is also performed during the asymmetric device authentication described in [EN 419212]-3, clause 3.6 and during the symmetric authentication defined in [EN 419212]-3, clause 3.8.

FCS_COP.1/SYM-AUTH *Cryptographic operation – Symmetric authentication*

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/ SYM-AUTH	The TSF shall perform *data encryption/decryption for Symmetric authentication* in accordance with a specified cryptographic algorithm *AES* and cryptographic key sizes *128, 256 bits* that meet the following: [FIPS 197].

Note: This SFR requires the TOE to implement AES for the symmetric authentication scheme as described in [EN 419212]-3, clause 3.8, which requires the TOE to perform mutual authentication of the terminal and the chip by encryption/decryption a challenge and verifying the response.

FCS_COP.1/ASYM-AUTH *Cryptographic operation – Asymmetric authentication*

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/ ASYM-AUTH	The TSF shall perform *Diffie-Hellman key agreement for asymmetric device authentication* in accordance with a specified cryptographic algorithm *ECDH* and cryptographic key sizes *256, 384 bits* that meet the following: [ISO/IEC 11770-3] *and* [NIST SP800-38A].

Note: The certified curves and bit length for ECDH are listed in note of FCS_CKM.1.1.
Note: This SFR assumes that the TOE implements the Diffie-Hellman key agreement for asymmetric device authentication as described in [EN 419212]-3, clause 3.6, which requires the TOE to perform external authentication of the terminal and internal authentication of the chip by signing and verifying a challenge using the cryptographic algorithm ECDSA defined in FCS_COP.1/Signature_Creation.

FCS_COP.1/PACE *Cryptographic operation – PACE*

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/ PACE	The TSF shall perform *Diffie-Hellman Key Agreement for PACE* in accordance with a specified cryptographic algorithm *ECDH* and cryptographic key sizes *256, 384 bits* that meet the following: [ISO/IEC 11770-3] *and* [NIST SP800-38A].

Note: The certified curves and bit length for ECDH are listed in note of FCS_CKM.1.1.
Note: This SFR requires the TOE to perform a Diffie-Hellman key agreement and the generic mapping of the PACE protocol as described in [EN 419212]-2, clause 8.

6.1.2. User data protection (FDP)

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

Table 3: 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, R.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)

FDP_ACC.1/Signature_Creation *Subset access control*

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

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

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

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ Signature_Creation: The TSF shall enforce the Signature Creation SFP to objects based on the following:
(1) the 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_ACC.1/SCD/SVD_Generation *Subset access control*

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ 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*

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

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*

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control

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

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

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ SVD_Transfer	The TSF shall enforce the SVD Transfer SFP to objects based on the following: (1) the S.User is associated with the security attribute Role, (2) the SVD.
FDP_ACF.1.2/ SVD_Transfer	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***R.Admin and R.Sigy*** 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.

Note: The following access control rules has been implemented:

- The Administrator is authorized to generate the SCD/SVD key pair according to FDP_ACF.1/SCD/SVD_Generation and to export the SVD before the signatory role (RAD) is created. This allows identification of a particular instance of the TOE by means of the SVD;
- The Administrator is authorized to generate the SCD/SVD key pair according to FDP_ACF.1/SCD/SVD_Generation and the signatory is allowed to export the SVD to the CGA. This allows determination whether the signatory has control over the TOE instantiation and the certificate may be generated;
- The signatory is authorized to generate the SCD/SVD key pair according to FDP_ACF.1/SCD/SVD_Generation and to export the SVD to the CGA to apply for the certificate.

The TOE protects the integrity and authenticity of the exported SVD public key.

FDP_ACC.1/SCD_Import *Subset access control*

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

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

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

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ SCD_Import	The TSF shall enforce the SCD Import SFP to objects based on the following: the S.User is associated with the security attribute "SCD/SVD Management".

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

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1/SCD	The TSF shall enforce the SCD Import SFP when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2/SCD	The TSF shall ignore any security attributes associated with the SCD when imported from outside the TOE.
FDP_ITC.1.3/SCD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none.

FDP_RIP.1 *Subset residual information protection*

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 the following objects: SCD. 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*

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
Dependencies:	No dependencies.

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

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
Dependencies:	No dependencies.

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

Note: The integrity of TSF data like RAD shall be protected to ensure the effectiveness of the user authentication. This protection is a specific aspect of the security architecture (cf. ADV_ARC.1).

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 to receive user data in a manner protected from modification and insertion errors.
FDP_UIT.1.2/DTBS	The TSF shall be able to determine on receipt of user data, whether modification and insertion has occurred.

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 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.

FDP_UCT.1/SCD *Basic data exchange confidentiality*

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

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

Note: The component FDP_UCT.1/SCD requires the TSF to ensure the confidentiality of the SCD during import. The refinement substituting "user data" by "SCD" highlights that confidentiality of other imported user data like DTBS is not required.

6.1.3. Identification and authentication (FIA)

FIA_AFL.1 *Authentication failure handling*

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 [1 and 127]*** 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.

Note: The RAD is a Password, PIN, PUK, biometric data, MRZ or CAN.

FIA_API.1 *Authentication proof of identity*

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FIA_API.1.1	The TSF shall provide a (1) *PACE authentication* (2) *asymmetric device authentication mechanism* (3) *symmetric authentication mechanism* to prove the identity of the authorized users.

Note: Via the assigned authentication mechanisms, the TOE and the terminal are able to authenticate each other using using TOE specific keys implemented in the TOE during pre-initialisation phase.

FIA_UAU.1 *Timing of authentication*

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) *establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD* 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.

Note: The [PP SSCD-4] performed the operation of the bullet (3) in the element FIA_UAU.1.1 of the [PP SSCD-2] by adding the establishment of a trusted channel to the CGA.

Note: The [PP SSCD-5] as well as the [PP SSCD-6] performed the operation of the bullet (4) in the element FIA_UAU.1.1 of the [PP SSCD-2] and the [PP SSCD-3] by adding the establishment of a trusted channel to HID.

FIA_UID.1 *Timing of identification*

Hierarchical to:	No other components.
Dependencies:	No dependencies.

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) *establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD* 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.

Note: The TOE will perform the operation of the bullets (2) and (3) in the element FIA_UID.1.1 by adding the establishment of a trusted channel to CGA and HID.

6.1.4. Security management (FMT)

FMT_MOF.1 *Management of security functions behaviour*

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 the functions signature creation function to R.Sigy.

FMT_MSA.1/Admin *Management of security attributes*

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

FMT_MSA.1.1/ Admin	The TSF shall enforce the SCD/SVD Generation SFP and SCD Import SFP to restrict the ability to modify the security attributes SCD/SVD management to R.Admin.

FMT_MSA.1/Signatory *Management of security attributes*

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

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

FMT_MSA.2 *Secure security attributes*

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.

Note: The TSF enforce the assignment of the secure value:

- for SCD/SVD Management in the preparation phase in secure environment, the subject S.Admin is assigned “yes” and of S.Sigy to “no”
- for SCD/SVD Management in the operational use stage and a trusted channel for export of the SVD to the CGA, the authenticated subjects S.Sigy and the R.Admin are assigned to “yes”
- for SCD operational in the preparation phase, the subjects S.Sigy and the R.Admin are assigned to “no”
- for SCD operational in the operational use stage, the authenticated subjects S.Sigy is assigned to “yes”

FMT_MSA.3 *Static attribute initialisation*

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 , SCD Import 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*

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.

(3) If S.Admin imports SCD while S.Sigy is not currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "no" after import of the SCD as a single operation.

(4) If S.Admin imports SCD while S.Sigy is currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "yes" after import of the SCD as a single operation.

Note: The TOE supports the generating an SCD/SVD pair by the administrator and by the signatory alone and rule (2) is relevant.

FMT_MTD.1/Admin *Management of TSF data*

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 the RAD to R.Admin.

FMT_MTD.1/Signatory *Management of TSF data*

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 ***and unblock*** the RAD to R.Sigy.

FMT_SMF.1 *Security management functions*

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) ***none***

FMT_SMR.1 *Security roles*

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

6.1.5. Protection of the TSF (FPT)

FPT_EMS.1 *TOE Emanation*

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*** in excess of ***non-useful information*** enabling access to RAD and SCD.
FPT_EMS.1.2	The TSF shall ensure ***any user*** are unable to use the following interface ***physical chip contacts and contactless I/O*** to gain access to RAD and SCD.

FPT_FLS.1 *Failure with preservation of secure state*

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) **none.**

FPT_PHP.1 *Passive detection of physical attack*

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.

FPT_PHP.3 *Resistance to physical attack*

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_PHP.3.1	The TSF shall resist ***physical manipulation and physical probing*** to the ***TSF*** by responding automatically such that the SFRs are always enforced.

FPT_TST.1 *TSF testing*

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*** 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.

6.1.6. Trusted path/channel (FTP)

FTP_ITC.1/SCD *Inter-TSF trusted channel*

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1/SCD	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SCD	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/SCD	The TSF shall initiate communication via the trusted channel for 1) Data exchange integrity according to FDP_UCT.1/SCD. 2) ***none;***

Note: The TSF enforces the establishment of a trusted channel by another trusted IT product generating the SCD/SVD pair for import the SCD.

FTP_ITC.1/SVD *Inter-TSF trusted channel*

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 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) ***none***

Note: The TSF enforces the establishment of a trusted channel by the CGA to export the SVD to the CGA.

FTP_ITC.1/VAD *Inter-TSF trusted channel – TC Human Interface Device*

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1/VAD	The TSF shall provide a communication channel between itself and a remote trusted IT product **HID** 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/VAD	The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/VAD	The TSF **or the HID** shall initiate communication via the trusted channel for (1) User authentication according to FIA_UAU.1.

(2) ***none***

Note: The TSF enforces the establishment of a trusted channel by the HID to send the VAD.

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 a remote 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 to initiate communication via the trusted channel.
FTP_ITC.1.3/DTBS	The TSF **or the SCA** shall initiate communication via the trusted channel for (1) signature-creation (2) ***none***

Note: The TSF enforces the establishment of a trusted channel by the SCA to send the DTBS.

6.2. Security assurance requirements

This ST is conforming to assurance package evaluation assurance level 4 (EAL4) augmented with AVA_VAN.5 and ALC_DVS.2 defined in [CC_P3].
Augmentation AVA_VAN.5 is required by the protection profile.
Augmentation ALC_DVS.2 introduced in this Security Target is a higher hierarchical assurance component to EAL4 (only ALC_DVS.1 is found in EAL4).
For the EAL4 augmented (EAL 4+), the relevant assurance classes and assurance components are listed in the table below.

Table 4: Security assurance requirements: EAL4 augmented with AVA_VAN.5 and ALC_DVS.2

Assurance Class and Components	Description
ADV	**Development**
ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation representation 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

Assurance Class and Components	Description
ALC_DVS.2	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	Focused vulnerability analysis

6.3. Security requirements rationale

6.3.1. Security requirements coverage

Table 5: Mapping of functional requirements to security objectives for the TOE

TOE security objectives / Functional requirements	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Auth_Imp	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FCS_CKM.1	X	X								X	X					
FCS_CKM.4	X	X														
FCS_COP.1/Signature_Creation	X		X													
FCS_COP.1/SM-ENC														X	X	X
FCS_COP.1/SM-MAC														X	X	X
FCS_COP.1/SYM-AUTH	X											X	X	X	X	X
FCS_COP.1/ASYM-AUTH	X											X	X	X	X	X
FCS_COP.1/PACE	X											X	X	X	X	X
FDP_ACC.1/Signature_Creation	X			X												
FDP_ACF.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_ACC.1/SCD_Import	X											X				
FDP_ACF.1/SCD_Import	X											X				
FDP_ITC.1/SCD	X															

TOE security objectives / Functional requirements	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Auth_Imp	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FDP_RIP.1		X		X												
FDP_SDI.2/Persistent		X	X								X					
FDP_SDI.2/DTBS				X	X											
FDP_DAU.2/SVD														X		
FDP_UCT.1/SCD	X	X														
FDP_UIT.1/DTBS																X
FIA_AFL.1				X												
FIA_API.1													X			
FIA_UAU.1				X					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/Signatory	X			X												
FMT_SMF.1	X			X							X					
FMT_SMR.1	X			X												
FPT_EMS.1		X				X										
FPT_FLS.1		X														
FPT_PHP.1							X									
FPT_PHP.3		X						X								
FPT_TST.1	X	X	X													
FTP_ITC.1/SCD	X	X														
FTP_ITC.1/SVD														X		
FTP_ITC.1/VAD															X	
FTP_ITC.1/DTBS																X

6.3.2. TOE security requirements sufficiency

The rationale in the [PP SSCD-2], section 6.1.2, explains how the security functional requirements cover the common security objectives for the TOE OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID and OT.Tamper_Resistance.

It also explains how the security functional requirements cover the security objectives for the OT.SCD/SVD_Auth_Gen, OT.SCD_Unique, OT.SCD_SVD_Corresp, which are present only in [PP SSCD-2].

The rationale for the security objective OT.SCD_Auth_Imp is from [PP SSCD-3] which also complements OT.Lifecycle_Security and OT.SCD_Secrecy.

The rationale for the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp is taken from [PP SSCD-4].

OT.Lifecycle_Security (*Lifecycle security*) is provided by the SFR as follows:

The secure SCD usage is ensured cryptographically according to FCS_COP.1/Signature_Creation and FCS_COP.1/RSACipher.

The SFR FCS_CKM.4 ensures a secure SCD destruction.

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.

(This item is extended with Part 2)

The FCS_CKM.1 ensures a SCD/SVD generation.

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.

(This item is extended with Part 3)

The SCD import is controlled by TSF according to FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import and FDP_ITC.1/SCD. The confidentiality of the SCD is protected during import according to FDP_UCT.1/SCD in the trusted channel FTP_ICT.1/SCD.

Additionally, FCS_COP.1/SYM-AUTH, FCS_COP.1/ASYM-AUTH and FCS_COP.1/PACE provide an authentication of Admin/CGA and trusted channel and the related management functions for administration of the authentication keys needed.

(This item is extended with Part 2)

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 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.

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.

(This item is extended with Part 2)

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.

(This item is extended with Part 3)

FDP_UCT.1/SCD and FTP_ICT.1/SCD ensures the confidentiality for SCD import.

OT.Sig_Secure (*Cryptographic security of the electronic signature*) is provided by the cryptographic algorithms specified by FCS_COP.1/Signature_Creation and FCS_COP.1/RSACipher, 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 provide 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.

(This item is extended with Part 3)

OT.SCD_Auth_Imp (Authorized SCD import) is provided by the security functions specified by the following SFR. FIA_UID.1 and FIA_UAU.1 ensure that the user is identified and authenticated before SCD can be imported. FDP_ACC.1/SCD_Import and FDP_ACF.1/SCD_Import ensure that only authorised users can import SCD.

Additionally, FCS_COP.1/SYM-AUTH, FCS_COP.1/ASYM-AUTH and FCS_COP.1/PACE provide an authentication of Admin/CGA.

(This item is extended with Part 4)

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 SSCD-2]) establishment of the trusted channel before (human) user is authenticated.

Additionally, FCS_COP.1/SYM-AUTH, FCS_COP.1/ASYM-AUTH and FCS_COP.1/PACE provide an authentication of Admin/CGA and TOE which is a mutual authentication with TOE individual keys and therefore allows authentication of the TOE as SSCD.

(This item is extended with Part 4)

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.

Additionally, FCS_COP.1/SM-ENC, FCS_COP.1/SM-MAC, FCS_COP.1/SYM-AUTH, FCS_COP.1/ASYM-AUTH and FCS_COP.1/PACE provide an authentication of Admin/CGA and trusted channel for SVD export.

(This item is extended with Part 5 and Part 6)

- **OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import)** is provided by FTP_ITC.1/VAD to provide a trusted channel to protect the VAD provided by the HID to the TOE.

Additionally, FCS_COP.1/SM-ENC, FCS_COP.1/SM-MAC, FCS_COP.1/SYM-AUTH, FCS_COP.1/ASYM-AUTH and FCS_COP.1/PACE provide an authentication of HID and trusted channel for VAD import to protect the VAD.

- **OT.TOE_TC_DTBS_Imp (Trusted channel 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.

Additionally, FCS_COP.1/SM-ENC, FCS_COP.1/SM-MAC, FCS_COP.1/SYM-AUTH, FCS_COP.1/ASYM-AUTH and FCS_COP.1/PACE provide an authentication of SCA and trusted channel for DTBS import to protect the DTBS.

6.3.3. Satisfaction of dependencies of security functional requirements

Table 6: Satisfaction of dependencies of security functional requirements

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 FDP_ITC.1/SCD
FCS_COP.1/Signature_Creation FCS_COP.1/SM-ENC FCS_COP.1/SM-MAC FCS_COP.1/SYM-AUTH FCS_COP.1/ASYM-AUTH FCS_COP.1/PACE	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4 FDP_ITC.1/SCD
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
FDP_ACF.1/SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDR_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_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, FDP_ACC.1/SCD_Import, 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, FDP_ACC.1/SCD_Import, 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/SCD_Import, 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

Functional requirement	Dependencies	Satisfied by
FMT_SMF.1	No dependencies	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
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
FDP_ACC.1/SCD_Import	FDP_ACF.1	FDP_ACF.1/SCD_Import
FDP_ACF.1/SCD_Import	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_ITC.1/SCD	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_UCT.1/SCD	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1/SCD, FDP_ACC.1/SCD_Import
FTP_ITC.1/SCD	No dependencies	n/a
FDP_DAU.2/SVD	FIA_UID1.	FIA_UID.1
FIA_API.1	No dependencies	n/a
FTP_ITC.1/SVD	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
FTP_ITC.1/VAD	No dependencies	n/a
FTP_ITC.1/DTBS	No dependencies	n/a

Table 7: Satisfaction of dependencies of security assurance requirements

Assurance requirement(s)	Dependencies	Satisfied by
EAL4 package	dependencies of EAL4 package are not reproduced here)	Fulfilled 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)
ALC_DVS.2	no dependencies	n/a

6.3.4. Security relevant functionality requirements

The assurance level for this ST is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialised processes and practices. It is considered to be the highest level that could be applied to an existing product line without 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 ST 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.

- ALC_DVS.2 Sufficiency of security measures
  The selection of the component ALC_DVS.2 provides a higher assurance of the security of the TOE's development and manufacturing especially for the secure handling of the TOE's material.

7. TOE summary specification

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1. Security functionality

Security functionalities provided by the TOE are listed in the table below.

Table 8: Security functionalities

Security function	Description
SF.AUTHENTICATION	User authentication
SF.ROLE	Operation management and access control
SF.TRUSTED_CHANNEL	Secure Communication
SF.CRYPTO	Cryptographic functions
SF.SELF_PROTECTION	Self-protection management

SF.AUTHENTICATION provides the authentication management on the TOE which realizes the authentication mechanisms:

- The user authentication with PIN, PUK, MRZ, CAN, biometric data, or a combination of these.
- The mutual device authentication of the reading device and of the TOE on asymmetric scheme with Diffie-Hellman or with symmetric scheme.

This security functionality provided by the TOE uses cryptographic operations of the platform from SF.Crypto which includes:

- The Password Based authentication (PACE) with generic mapping based on ECDH key agreement.
- The asymmetric device authentication using ECDH.
- The symmetric authentication using AES.

It covers the following SFRs:

- The authentication failure handling as defined in FIA_AFL.1.
- The authentication of proof of identity and data authentication with identity of guarantor as defined in FIA_API.1 and FDP_DAU.2/SVD.
- The timing of identification and authentication as defined in FIA_UID.1 and FIA_UAU.1.

SF.ROLE provides operation management for the roles Administrator and Signatory and its access rights to objects (files, directories, data and secrets) stored in the applet's file system.
This security functionality provided by the TOE is integral part of asymmetric device authentication and symmetric authentication from SF.Authentication.
It covers the following SFRs:

- The access control management for the Signature creation, SVD Generation, SVD_Transfer, SVD_Import as defined in FDP_ACC.1 and FDP_ACF.1.
- The input and output of user data as defined in FDP_ITC.1/SCD.
- The management of security functions behaviour and functions as defined in FMT_MOF.1 and FMT_SMF.1.
- The management of security attributes for the Administrator and Signatory as defined in FMT_MSA.1, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4.
- The management of TSF data as defined in FMT_MTD.1/Admin and FMT_MTD.1/Signatory.
- The management of security roles the Administrator and Signatory as defined in FMT_SMR.1.

SF.TRUSTED_CHANNEL provides the secure messaging.
Session keys required for the secure messaging protocol are derived during the PACE authentication, the asymmetric device authentication and the symmetric authentication from SF.Authentication.
This security functionality provided by the TOE uses cryptographic operations of the platform from SF.Crypto which includes:

- The data encryption/decryption AES in CBC mode.
- The message authentication code AES in CMAC mode.

It covers the following SFRs:

- The data exchange integrity and confidentiality as defined in FDP_UCT.1/SCD.
- The secure trusted path/channel assured identification of its end points and protection of the of the SCD, DVD, VAD and DTBS from modification or disclosure as defined in FTP_ITC.1.

SF.CRYPTO provides the cryptographic support to the other security functions.
The TOE uses the security functionalities of the platform to implement the application interfaces to the TOE as is specified in [EN 419212].
It covers the following SFRs:

- The cryptographic key generation NIST or Brainpool as defined in FCS_CKM.1.
- The cryptographic key destruction as defined in FCS_CKM.4.
- The digital signature creation ECDSA as defined in FCS_COP.1/Signature_Creation.
- The data encryption/decryption AES in CBC mode for secure messaging as defined in FCS_COP.1.1/SM-ENC.
- The message authentication code AES in CMAC mode for secure messaging as defined in FCS_COP.1/SM-MAC.
- The data encryption/decryption AES for symmetric authentication as defined in FCS_COP.1/SYM-AUTH.
- The Diffie-Hellman key agreement ECDH for asymmetric device authentication as defined in FCS_COP.1/ASYM-AUTH.
- The Diffie-Hellman Key Agreement for PACE as defined in FCS_COP.1/PACE.

SF.SELF_PROTECTION provides protecting of the integrity of internal applet data and the integrity monitoring on the TOE and DTBS and protection against physical attacks.
This security functionality is provided by the certified platform.

It covers the following SFRs:

- The stored data integrity monitoring and action as defined in FDP_SDI.2/Persistent and FDP_SDI.2/DTBS.
- The integrity of sensitive data as defined in FDP_SDI.2/Persistent and FDP_SDI.2/DTBS and FDP_UIT.1/DTBS.
- The protection against physical attacks as defined in FPT_EMS.1, FPT_FLS.1, FPT_PHP.1, and FPT_PHP.3.
- The testing of the card as defined in FPT_TST.1.
- The secure unavailability of sensitive data as defined in FDP_RIP.1.

7.2. Security functionality rational

Table 9: Security functionality rational

TOE security objectives / Functional requirements	SF. AUTHENTICATION	SF.ROLE	SF.TRUSTED_CHANNEL	SF.CRYPTO	SF.SELF_PROTECTION
FCS_CKM.1				X	
FCS_CKM.4				X	
FCS_COP.1/Signature_Creation				X	
FCS_COP.1/SM-ENC				X	
FCS_COP.1/SM-MAC				X	
FCS_COP.1/SYM-AUTH				X	
FCS_COP.1/ASYM-AUTH				X	
FCS_COP.1/PACE				X	
FDP_ACC.1/Signature_Creation		X			
FDP_ACF.1/Signature_Creation		X			
FDP_ACC.1/SCD/SVD_Generation		X			
FDP_ACF.1/SCD/SVD_Generation		X			
FDP_ACC.1/SVD_Transfer		X			
FDP_ACF.1/SVD_Transfer		X			
FDP_ACC.1/SCD_Import		X			
FDP_ACF.1/SCD_Import		X			
FDP_ITC.1/SCD		X			
FDP_RIP.1					X
FDP_SDI.2/Persistent					X
FDP_SDI.2/DTBS					X
FDP_DAU.2/SVD	X				
FDP_UCT.1/SCD			X		
FDP_UIT.1/DTBS					X
FIA_AFL.1	X				
FIA_API.1	X				
FIA_UAU.1	X				
FIA_UID.1	X				
FMT_MOF.1		X			
FMT_MSA.1/Admin		X			
FMT_MSA.1/Signatory		X			
FMT_MSA.2		X			
FMT_MSA.3		X			

TOE security objectives / Functional requirements	SF. AUTHENTICATION	SF.ROLE	SF.TRUSTED_CHANNEL	SF.CRYPTO	SF.SELF_PROTECTION
FMT_MSA.4		X			
FMT_MTD.1/Admin		X			
FMT_MTD.1/Signatory		X			
FMT_SMF.1		X			
FMT_SMR.1		X			
FPT_EMS.1					X
FPT_FLS.1					X
FPT_PHP.1					X
FPT_PHP.3					X
FPT_TST.1					X
FTP_ITC.1/SCD			X		
FTP_ITC.1/SVD			X		
FTP_ITC.1/VAD			X		
FTP_ITC.1/DTBS			X		

8. References

Short Reference	Common Criteria References
[1] [CC P1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017, CCMB-2017-04-001
[2] [CC P2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002
[3] [CC P3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003
[4] [CC M]	Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004
Short Reference	Protection Profiles References
[5] [PP O]	EN 419211-1:2011 Protection profiles for Secure signature creation device - Part 1: Overview
[6] [PP SSCD-2]	EN 419211-2:2013 Protection profiles for secure signature creation device - Part 2: Device with Key Generation, registered and certified under the reference BSI-CC-PP-0059-2009-MA-02
[7] [PP SSCD-3]	EN 419211-3:2013 Protection profiles for secure signature creation device - Part 3: Device with key import, registered and certified under the reference BSI-CC-PP-0075-2012-MA-01
[8] [PP SSCD-4]	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, registered and certified under the reference BSI-CC-PP-0071-2012-MA-01
[9] [PP SSCD-5]	EN 419211-5:2013 Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application, registered and certified under the reference BSI-CC-PP-0072-2012-MA-01
[10] [PP SSCD-6]	EN 419211-6:2014 Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application, registered and certified under the reference BSI-CC-PP-0076-2013-MA-01
[11] [PP Java]	Java Card™ System Protection Profile Open Configuration Version 2.6
[12] [PP IC]	Security IC Platform Protection Profile; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007, Version 1.0, June 2007
Short Reference	TOE and platform references
[13] [ST_AKDeID]	Security Target AKD eID 2.0 SSCD v2.4
[14] [USR_AKDeID]	User Guidance AKD eID 2.0 SSCD v1.12
[15] [ST Java]	JCOP 4.5 P71 Security Target Lite, Rev. 2.6, 11 December 2023
[16] [CR Java]	JCOP 4.5 P71 Certification Report, 16 January 2024, NSCIB-CC-2300127-01-CR
[17] [ST IC]	NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), Security Target lite, Version 1.8, 2023-12-01

[18] [CR IC]	NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), BSI-DSZ-CC-1149-V3-2023
Short Reference	Other references
[19] [eIDAS Regulation]	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[20] [eIDAS Dis]	Commission implementing decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[21] [The Directive]	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
[22] [ID Regulation]	Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement
[23] [C2018 7767 final]	Commission Implementing Decision of 30.11.2018 laying down the technical specifications for the uniform format for residence permits for third country nationals and repealing Decision C(2002)30691, C(2018) 7767 final
[24] [CEN15480-2]	Identification card systems –European Citizen Card –Part 2: Logical data structures and card services
[25] [PKCS#15]	ISO/IEC 7816-15:2016 Identification cards — Integrated circuit cards — Part 15: Cryptographic information application
Short Reference	Crypto Standards References
[26] [EN 419212]	Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services, Parts 1-5, 2017/2018.
[27] [ISO/IEC 14888-3]	ISO/IEC 14888-3:2015 – Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, 2016
[28] [FIPS 186-4]	NIST FIPS PUB 186-4: Digital Signature Standard (DSS), 2013.
[29] [RFC 5639]	RFC 5639: J. Merkle, ECC Brainpool Standard Curves and Curve Generation, BSI, March 2010
[30] [FIPS 197]	FIPS 197 Advanced Encryption Standard (AES), 2001
[31] [NIST SP800-38A]	National Institute of Standards and Technology SP800-38A: Recommendation for Block Cipher Modes of Operation, 2001
[32] [NIST SP 800-38B]	National Institute of Standards and Technology SP800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
[33] [NIST SP800-56A]	NIST Special Publication 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, 2013

[34] [ISO/IEC 11770-3]	ISO/IEC 11770-3:2015: Information technology – Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques, 2015, ISO/IEC
[35] [SOG-IS]	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, v1.3, February 2023
[36] [ETSI TS 119 312]	ETSI TS 119 312 V1.4.2 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites, 2022-02

9. Glossary and Acronyms

Term	Definition pertaining to the PPs
Administrator	User who performs TOE initialisation, TOE personalisation, or other TOE administrative functions
Advanced electronic signature	Digital signature which meets specific requirements in [The Directive: 2.2] NOTE According to [The Directive] a digital signature qualifies as an advanced electronic signature if it: - is uniquely linked to the signatory; - is capable of identifying the signatory; - is created using means that the signatory can maintain under his sole control, and - is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Authentication data	Information used to verify the claimed identity of a user
Certificate	Digital signature used as electronic attestation binding signature-verification data to a person confirming the identity of that person as legitimate signer [The Directive: 2.9]
Certificate info	Information associated with a SCD/SVD pair that may be stored in a secure signature creation device NOTE 1 Certificate info is either: - a signer's public key certificate or, - one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values. NOTE 2 Certificate info may contain information to allow the user to distinguish between several certificates.
CGA Certificate-generation application	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
CSP Certification service provider	Entity that issues certificates or provides other services related to electronic signatures [The Directive: 2.11]
DTBS Data to be signed	Data to be signed DTBS - all of the electronic data to be signed including a user message and signature attributes
DTBS/R Data to be signed or its unique representation	Data received by a secure signature creation device as input in a single signature-creation operation NOTE DTBS/R is either: - a hash-value of the data to be signed (DTBS), or - an intermediate hash-value of a first part of the DTBS complemented with a remaining part of the DTBS, or

	- the DTBS.
HID Human Interface Device	Human interface provided by the SCA for user authentication
Legitimate user	User of a secure signature creation device who gains possession of it from an SSCD-provisioning service provider and who can be authenticated by the SSCD as its signatory
Middleware	Set of software applications, particularly comprising the CGA and the SCA, meant for being used by the Administrator and/or the Signatory to interact with a QSCD during the operational use phase
Qualified certificate	Public key certificate that meets the requirements laid down in Annex I and that is provided by a CSP that fulfils the requirements laid down in Annex II [The Directive: 2.10]
Qualified electronic signature	Advanced electronic signature that has been created with an SSCD with a key with a qualified certificate NOTE See [The Directive: 5.1].
RAD Reference authentication data	Data persistently stored by the TOE for to authenticate a user as authorized for a particular role
SSCD Secure signature-creation device	Personalized device that meets the requirements laid down in Annex III by being evaluated according to a security target conforming to a PP in this series of European Standards [The Directive: 2.5 and 2.6]
Signatory	Legitimate user of an SSCD associated with it in the certificate of the signature-verification data and who is authorized by the SSCD to operate the signature-creation function [The Directive: 2.3]
Signature attributes	Additional information that is signed together with a user message
SCA Signature-creation application	Application complementing an SSCD with a user interface with the purpose to create an electronic signature NOTE A signature creation application is software consisting of a collection of application components configured to: - present the data to be signed (DTBS) for review by the signatory, - obtain prior to the signature process a decision by the signatory, - if the signatory indicates by specific unambiguous input or action its intent to sign send a DTBS/R to the TOE - process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.
SCD Signature-creation data	Private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature [The Directive: 2.4]
SCS Signature-creation system	Complete system that creates an electronic signature consisting of an SCA and an SSCD
SVD Signature-verification data	Public cryptographic key that can be used to verify an electronic signature [The Directive: 2.7]
SDO	Signed Data Object

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
VAD Verification authentication data	Data provided as input to a secure signature creation device for authentication by cognition or by data derived from a user's biometric characteristics
Term	Definition pertaining to the ST
IC Integrated circuit	Electronic component(s) designed to perform processing and/or memory functions. The smart card chip is an integrated circuit.
QSCD Qualified Signature Creation Device	Configured software or hardware which is used to implement signature creation and encrypted data decipherment, and which meets the requirements laid down in [eIDAS Regulation], Annex II.
PIN	The Personal Identification Number (PIN) is a short secret password that SHALL be only known to the legitimate holder of the document.
PUK	The PIN Unblock Key (PUK) is a long secret password that SHALL be only known to the legitimate holder of the document.
Acronym	Term
CC	Common Criteria
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read-Only Memory
ICAO	International Civil Aviation Organization
PACE	Password Authenticated Connection Establishment
IT	Information Technology