AKD ELECTRONIC IDENTITY CARD

SECURITY TARGET LITE

Version 1.3

Status: 26. September 2014.

1. Scope

The aim of this document is to describe the Security Target (ST) for the AKD eID Card 1.0, which is a smart card, intended to be used as Secure Signature Creation Device (SSCD).

2. References

Short Reference	Document Title – Reference
[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
[CEN/TS 15480-2]	PD CEN/TS 15480-2:2012 Identification card systems - European Citizen Card Part 2: Logical data structures and security services
[EN 14890-1]	BS EN 14890-1:2008 Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements, 31 January 2009
[TR 03116-2]	Technische Richtlinie TR-03116-2, eCard-Projekte der Bundesregierung, Teil 2 – Hoheitliche Ausweisdokumente, BSI, 21.03.2013
[CC_P1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, Version 3.1, Revision 4, CCMB-2012-09-001
[CC_P2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002
[CC_P3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003
[PP_SSCD_O]	EN 419211-1:2011[1] Protection profiles for Secure signature creation device - Part 1: Overview
[PP_SSCD_KG]	EN 419211-2:2013[2] 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-01
[PP_SSCD_KI]	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
[PP_SSCD_KG_TCCGA]	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
[PP_SSCD_KG_TCSCA]	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
[PP_SSCD_KI_TCSCA]	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
[CAdES]	ETSI TS 101 733 Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)

1 To be published.
2 This document was submitted to the enquiry procedure under the reference prEN 14169-2, Protection profiles for secure signature creation device — Part 2: Device with key generation, Version: 2, 2012-01.

[XAdES]	ETSI TS 101 903 Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)
[PAdES]	ETSI TS 102 778 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles (PAdES)
[JCOP_ST]	NXP J3E081_M64, J3E081_M66, J2E081_M64, J3E041_M66, J3E016_M66, J3E016_M64, J3E041_M64 Secure Smart Card Controller Revision 3, Rev. 01.03 2014-08-07
[JCOP 2.4.2 R3]	NXP J3E081_M64, J3E081_M66, J2E081_M64, J3E041_M66, J3E016_M66, J3E016_M64, and J3E041_M64 Secure Smart Card Controller Revision 3, NSCIB-CC-13-37761-CR2, August 2014
[CL v2.7/v2.9]	Crypto Library V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s), BSI-DSZ-CC-0633-V2-2014, 16 July 2014
[NXP_HW]	NXP Secure Smart Card Controllers P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s), BSI-DSZ-CC-0857-2013, 2013
[FIPS 180-3]	FIPS PUB 180-3, Secure Hash Standard, Federal Information Processing Standards Publication, October 2008, US Department of Commerce/National Institute of Standards and Technology
[FIPS 46-3]	FIPS PUB 46-3: Federal Information Processing Standards Publication, Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. Department of Commerce/National Institute of Standards and Technology
[ISO 9797-1]	ISO/IEC 9797-1:1999: Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher
[PKCS#1 v2.1]	PKCS1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 2002
[PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, RSA Laboratories Technical Note Version 1.4, Revised November 1, 1993
[SP 800-38B]	NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, May 2005
[NXP SSCC]	NXP Secure Smart Card Controllers P5CD016/021/041/051 and P5Cx081V1A/V1A(s) Security Target Lite, Rev. 1.9, 03.06.2013, registered and certified under the reference BSI-DSZ-CC-0857-2013

3. Conventions and terminology

3.1. Terms and definitions

For the purposes of this document, terms and definitions given in [PP_SSCD_O] apply.

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” [The Directive]

NOTE References in this document to a specific article and paragraph of Directive 1999/93/EC are of the form “[The Directive: n.m]”.

Annex - one of the annexes, Annex I, Annex II or Annex III of [The Directive]

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.

Certificate-generation application CGA - collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate

Certification service provider CSP - entity that issues certificates or provides other services related to electronic signatures [The Directive: 2.11]

Data to be signed DTBS - all of the electronic data to be signed including a user message and signature attributes

Data to be signed or its unique representation DTBS/R - data received by a 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.

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

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].

Reference authentication data RAD - data persistently stored by the TOE for to authenticate a user as authorised for a particular role

Secure signature-creation device SSCD - 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

Signature-creation application SCA - 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.

Signature-creation data SCD - private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature [The Directive: 2.4]

Signature-creation system SCS - complete system that creates an electronic signature consisting of an SCA and an SSCD

Signature-verification data SVD - public cryptographic key that can be used to verify an electronic signature [The Directive: 2.7]

SSCD-provisioning service - service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD

User - entity (human user or external IT entity) outside the TOE that interacts with the TOE

User Message - data determined by the signatory as the correct input for signing

Verification authentication data VAD - data provided as input to a secure signature creation device for authentication by cognition or by data derived from a user's biometric characteristics

3.2. Abbreviated terms

The used abbreviated terms are:

API	Application Programming Interface
CC	Common Criteria
CA	Certificate Authority
CGA	Certification generation application
CSP	Certification-service-provider
DES	Data Encryption Standard
DTBS	Data to be signed
DTBS/R	Data to be signed or its unique representation
EAL	Evaluation Assurance Level
HID	Human Interface Device
EEPROM	Electrically Erasable Programmable Read-Only Memory
IC	Integrated Chip
ICC	Integrated Chip Card
IFD	Interface Device
IT	Information Technology
MAC	Message Authentication Code
PKI	Public key infrastructure
PIN	Personal Identification Number
PUK	Personal Unblocking Key
PP	Protection Profile
PAN	Primary Account Number
RAD	Reference authentication data
ROM	Read-only memory
RSA	Rivest, Shamir and Adleman
RSA CRT	Rivest, Shamir and Adleman - Chinese Remainder Theorem
SHA	Secure Hash Algorithm
SSPS	SSCD Provisioning Service Provide
SSCD	Secure signature-creation device
SSMA	Signatory SSCD Management Application
SCA	Signature-creation application
SCD	Signature-creation data
SCS	Signature-creation system
SDO	Signed data object
SFP	Security Function Policy
SPS	SSCD Provisioning Service
ST	Security Target
TSF	TOE Security Functionality
TOE	Target of evaluation
VAD	Verification authentication data

4. ST Introduction

4.1. ST and TOE reference

Document Id	DP-I-101
Document Title	AKD Electronic Identity Card Security Target Lite
Document Reference	ST_AKDeID
Document Version	1.3
Document Date	2014-09-26
Document Author	AKD, Agencija za komercijalnu djelatnost d.o.o
TOE reference	AKD eID Card 1.0
TOE Product Type	Secure Signature Creation Device (SSCD)
TOE Developer	AKD, Agencija za komercijalnu djelatnost d.o.o
TOE Platform	NXP J2E081_M64 Secure Smart Card Controller Revision 3 [JCOP 2.4.2 R3]
Certification Id	BSI-DSZ-CC-0821-2014
Evaluation assurance level	EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 (EAL 4+)

4.2. TOE Overview

The target of evaluation (TOE) is the AKD eID Card 1.0, which is multifunctional smartcard product, intended for use as a secure signature creation device (SSCD) in accordance with the European Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a community framework for electronic signatures [The Directive] and its possible revision.

For an electronic signature product that has been evaluated according to Common Criteria (version 3.1) as conforming to a Security Target (ST) that is compliant with one or more of EN 419 211 Protection Profiles (PP) this European Standard implies that European Union Member States shall presume compliance with the requirements in Annex III of [The Directive] for that product. This Security Target (ST) is strictly 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, submitted to the enquiry procedure under the reference prEN 14169-2, registered and certified under the reference BSI-CC-PP-0059-2009-MA-01 [PP_SSCD_KG],
- 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 [PP_SSCD_KI] and
- 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 [PP_SSCD_KG_TCCGA],

The product can be operated in other environments providing functionalities based on the following two Protection Profiles, but these functionalities are out of the certified scope of this evaluation:

- 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 [PP_SSCD_KG_TCSCA] 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 [PP_SSCD_KI_TCSCA], registered and certified under the reference BSI-CC-PP-0076-2013

The basis of this composite evaluation is the composite evaluation of the platform:

- NXP J3E081_M64, J3E081_M66, J2E081_M64, J3E041_M66, J3E016_M66, J3E016_M64, J3E041_M64 Secure Smart Card Controller Revision 3 [JCOP_ST], NSCIB-CC-13-37761-CR2, August 2014

which consist of the hardware and the cryptographic library:

- NXP Secure Smart Card Controllers P5CD016/021/041/051 and P5Cx081V1A/V1A(s) [NXP_HW], BSI-DSZ-CC-0857-2013, 2013 and
- Crypto Library V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s) [CL v2.7/v2.9], BSI-DSZ-CC-0633-V2-2014, 16 July 2014

The TOE specifies a SSCD that may generate signing keys internally or externally, export the public key in protected manner and communicate with the signature creation application in protected manner. When operated in a secure environment a signatory may use the TOE to create an advanced electronic signature or a qualified electronic signature to conform to the specifications in ETSI TS 101 733 [CAdES], ETSI TS 101 903 [XAdES] and ETSI 102 778 [PAdES].

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 TOE comprises the all mandatory features for the European Citizen Card according to [CEN/TS 15480-2], which makes it suitable for implementing national e-ID card combining e-services and national e-ID applications. In order to enable interoperability and usage of the TOE on a national or European level, the application interfaces to the TOE are implemented as is specified in [EN 14890-1].

The AKD eID Card 1.0 may be used for various applications (electronic identification card, electronic health card, electronic signature application requiring qualified signature, electronic service card…) and purpose (digital signature, client server authentication, data encryption and certificate verification...).

The assurance level for the TOE is CC EAL4+.

4.3. TOE Description

4.3.1. Overview for this section

The term "PPs" is used instead of listing [PP_SSCD_KG], [PP_SSCD_KI] and [PP_SSCD_KG_TCCGA], and the term "core PPs" is used instead of listing [PP_SSCD_KG] and [PP_SSCD_KI].

This section is based on the TOE overview of PPs and has only been extended by the product specific details.

4.3.2. Operation of the TOE

Figure 1 shows this TOE, its operational environments and the interaction with the environment.

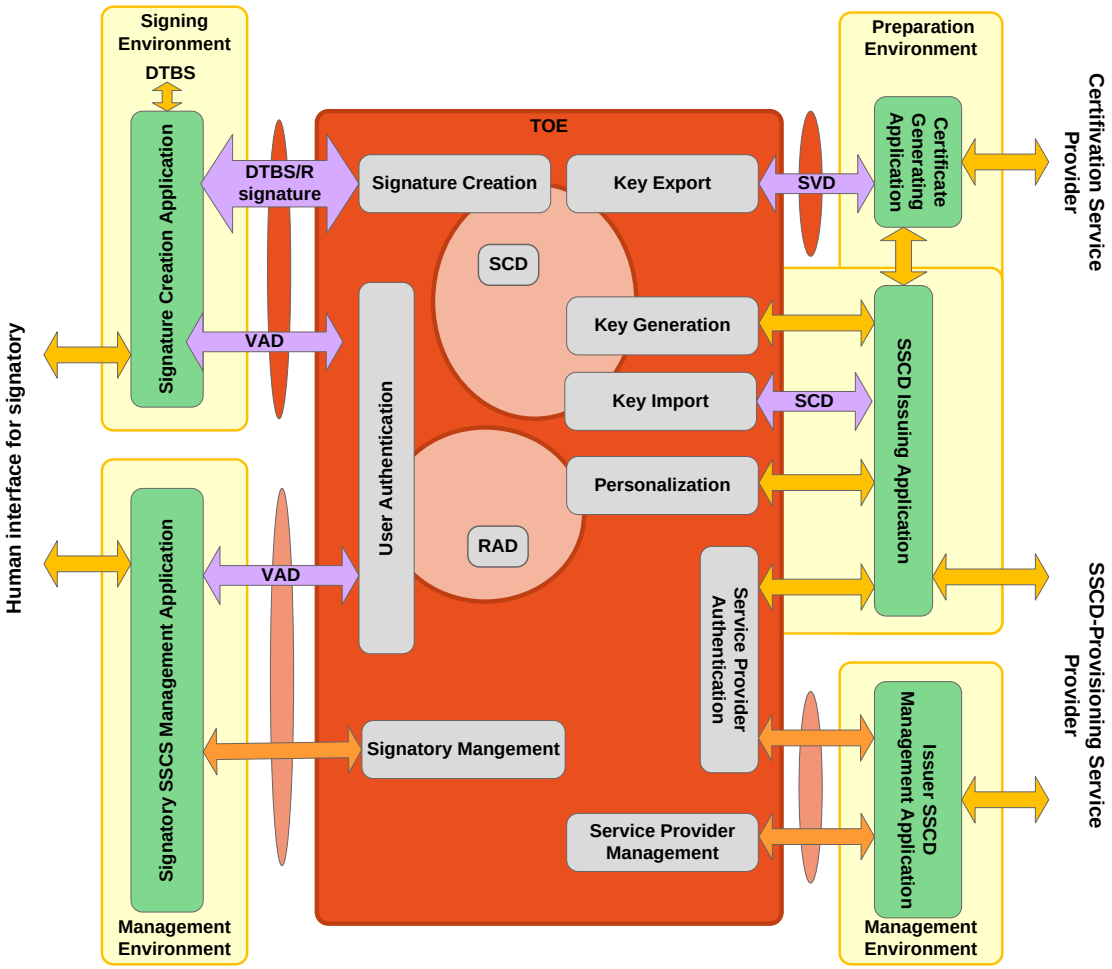


Figure 1: The TOE and operational environments

The key generation and key import functions of the TOE can be performed in the preparation environment as well as in signing or management environment.

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

- **The preparation environment**,

- where it interacts with a certification service provider through a certificate generation application (CGA) to obtain a certificate for the signature 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.
- where 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**
  - where it interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation application provides the 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 environments**
  - where it interacts with the user or an SSCD-provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

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

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. 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 electro*nic signature* as defined in Article 5.1 of **[The Directive]** if the certificate for the SVD is a qualified certificate (Annex I). Determining the state of the certificate as qualified is beyond the scope of this standard.

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.

4.3.3. Security features

Security functionalities provided by the TOE map the general requirements of the EU directive to asymmetric techniques [The Directive] as required by the EN419211 Protection Profiles for Secure Signature Creation Device (SSCD) and cover additional services, useful in its operational-use stage.

To accomplish the required security as claimed in the PPs, the TOE security functionalities cover the signing function, key generation and key import, storage of certificates, the related user verification, establishment and use of trusted path and channel as well as the allocation and format of resources required for the execution of those functions and related cryptographic token information.

The self protect function and all cryptographic functions including those based on the same technology as key decipherment, client server authentication and signature verification are provided by the NXP JCOP platform.

4.3.3.1. Main functions

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 may implement its function for digital signature creation to conform to the specifications in ETSI TS 101 733 (CAdES), ETSI TS 101 903 (XAdES) and ETSI TS 101 903 (PAdES).

The TOE may properly 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 shall be in a non-operational state. Upon receiving the TOE the signatory shall verify that its non-operational state and change the SCD state to operational.
After preparation the intended, legitimate user should be informed of the signatory's verification authentication data (VAD) required for use of the TOE in signing. If the VAD is a password or PIN, 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.

4.3.3.2. Identification and user authentication

The TOE contains a Primary Account Number (PAN) in accordance with ISO/IEC 7812-1, which enables identification of the card issuer and the cardholder.
The user authentication is knowledge based, i.e. submission of a PIN/password. This authentication scheme enables to authenticate the user role Signatory.
The TOE provides functions to enable the user to:

a) Verify PIN
b) Change the value of a PIN and
c) Unblock all PINs using the PUK value.

The TOE has two PINs and one PUK value. One PIN is intended for digital signature authentication exclusively. Another PIN is used for authentication in all other sensitive operations as well as for privacy protection of the certain data in the card. The same PUK value is used to unblock both PINs.

4.3.3.3. Device authentication

Device authentication aims at authenticating both entities willing to communicate and securing the communication between the card and a remote entity. Remote entity might be SCA and CGA in the signing environment or Signatory SSCD Management Application and Issuer SSCD Management Application in the management environment.
The TOE implements the following device authentication protocols:

a) symmetric authentication using 3DES keys,
b) asymmetric authentication using Card Verifiable (CV) certificates and device authentication with privacy protection protocol

The terminal shall implement listed protocols and adapt authentication according to the security level required by the resource it wishes to access.

4.3.3.4. Secure messaging

Secure messaging session establishment begins with device authentication when secure messaging session keys are computed.
Secure messaging should ensure that communication between the TOE and the IFD is protected. The secure messaging constantly performs checks and the session is aborted in case of any errors.

The secure message provides functions to establish a trusted, cryptographically protected communication to remote IT entities, such as:

a) A certificate-generation application (CGA)
b) An SVD-generating application, if it is not part of CGA application
c) A signature-creation application (SCA)
d) Human interface device (HID)
e) Management application

4.3.3.5. Role authentication

The Role authentication is used by the external entity to present a specific authorization to the TOE. The TOE establishes the security context by setting a respective value in its security environment and enforces usage of the correct security policy. The TOE requires authentication for a specific operation and for privacy protection because certain data in the card (or data secured by the card) can only be accessed after authentication. Prior to any operation the application checks the requested access rights to resources and to operations performed on those resources. If security conditions are fulfilled, access is granted.

The TOE maintains the roles for Signatory and Administrator to grant different access rights.

Signatory and Administrator may:

a) Generate an SCD or install an SCD, generated outside the device in a trusted environment and communicated over a secure communication link),
b) Disabling an SCD it holds, e.g. by erasing it from memory,
c) Create, extend or modify certificate info stored in the device,
d) Create SVD for an SCD stored and export it for certification by a certificate generating application protected by trusted communication,

Only Signatory may:

a) Switch the TOE from a non-operational state to an operational state, and thereby change initial PIN and set the PUK value,
b) Change value of the PIN/PUK,
c) Unblock the PIN using PUK value while the SSCD is in operational state,
d) Only the Signatory is allowed to create digital signatures and only if the TOE is in operational state.

Only Administrator may:

a) Define minimum length of an alphanumeric value of PIN/PUK
b) Initialize the PIN for the signatory while card is in non-operational state,
c) Import personal user data
d) Change symmetric or asymmetric keys for device authentication
e) Change personal information of the legitimate user
f) Switch blocked SSCD to a non-operational state and unblock the PIN and PUK resetting the remaining tries counter to the predefined maximum error counter

The Administrator is not allowed to create digital signatures in any environment. Generally, it is not allowed to create digital signature in the card preparation phase nor is digital signature creation allowed in operational use stage if the TOE is not in operational state.

4.3.3.6. Cryptographic functions

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

The TOE uses the JCOP platform functions and allows the card to be used as a crypto token, which provides the following cryptographic operation:

(1) Digital Signature
The TOE enables the Signatory to digital sign documents. The signature may be advanced or qualified.

(2) Client/server authentication
The TOE computes a signature for the computer the cardholder uses to access remote services. The computer is authenticated with the signature computed by the card using an asymmetric cryptographic scheme.

(3) Encryption key decipherment

Encryption key decipherment enables the cardholder to store secret data on an electronic vault. The RSA private key needed to decipher the symmetric key encrypting these data is securely stored in the TOE. The remote entity sends by the RSA public key encrypted symmetric encryption key to the TOE to get the plain symmetric encryption key.

Encryption key decipherment is also used in SSL session establishment when connecting to web services. The purpose is to send data enciphered by a remote server to a computer a person uses to access web services in a secure manner. The TOE receives the symmetric key to use (for decipherment) within a cryptogram.

(4) Certificate verification
This feature enables the TOE to verify a certificate issued by a certificate authority the TOE trust. The trust is established by the transfer to the TOE of a public RSA key of an authority certified by an authority whose public key is present in the TOE.

4.3.3.7. Self protection

The JCOP platform provides functionality such as a monitoring the auditable events and indicate a potential violation, a secure management of TOE resources, control of operating conditions, protection against physical manipulation, logical protection, protection of mode control, memory access control and register access control.

4.3.4. TOE platform

The TOE comprises of:

(1) The TOE platform NXP J3E081_M64, J3E081_M66, J2E081_M64, J3E041_M66, J3E016_M66, J3E016_M64, and J3E041_M64 Secure Smart Card Controller Revision 3, NSCIB-CC-13-37761-CR2, August 2014 [JCOP 2.4.2 R3], according to the Common Criteria for evaluation assurance level 5+.

(2) The Java Card applet the AKD eID Card 1.0 on the application layer containing the SSCD functionality

(3) The associated guidance documentation, which is subject of the evaluation according to the assurance guidance documents (AGD) class. The exact version of the guidance document is given in the certification report.
(4) The personalization key

The evaluated NXP platform includes the cryptographic library and the hardware:

- Crypto Library V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s), BSI-DSZ-CC-0633-V2-2014, 16 July 2014 [CL v2.7/v2.9]
- NXP Secure Smart Card Controllers P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s), BSI-DSZ-CC-0857-2013, 2013 [NXP_HW]

The NXP platform consists of:

- Smart card platform (SCP) (parts of the hardware platform and hardware abstraction layer)
- Embedded software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager)
- Native MIFARE application (physically always present but logical availability depends on configuration)

The Smart Card Platform (SCP) consists of the Hardware Abstraction Layer (HAL) and the Hardware Platform. The cryptographic library (Crypto Library) is part of the Hardware Abstraction Layer (HAL).

The TOE limits are shown schematically in Figure 2. The Platform is bordered with green dashed line and the TOE is bordered with red dashed line.

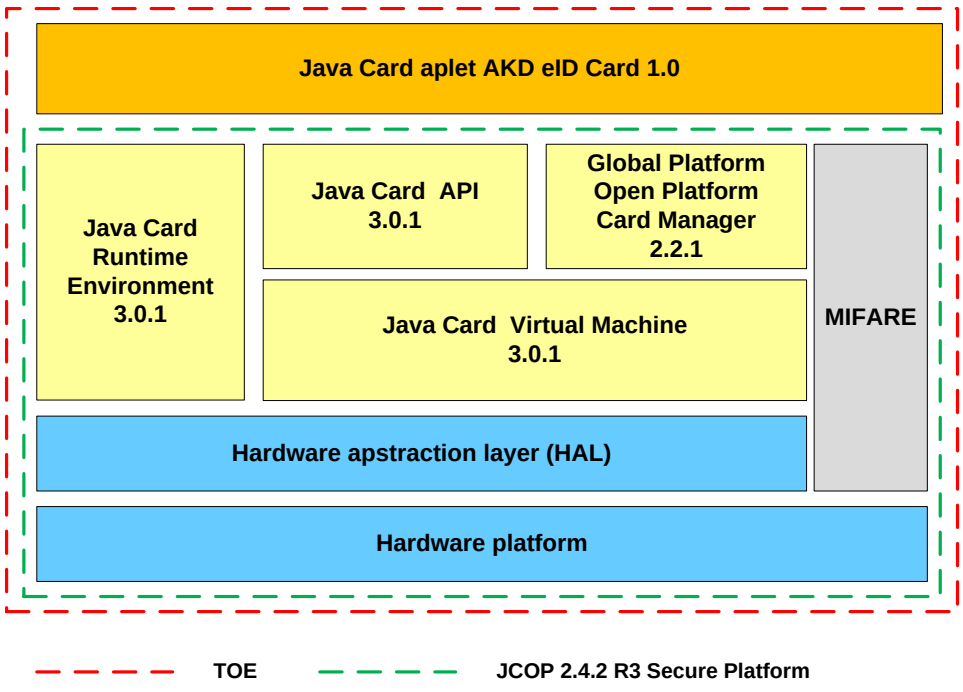


Figure 2: The TOE limits

The TOE is available on the P5CC081V1A hardware in which MIFARE interface is disabled.

For the TOE relevant is only NXP J2E081_M64 Secure Smart Card Controller Revision 3, which is based on Java Card 3.0.1 and Global Platform 2.2.1 industry standards. It implements high security mechanisms and supports various protocols, cryptographic algorithms.

4.3.5. The TOE life cycle

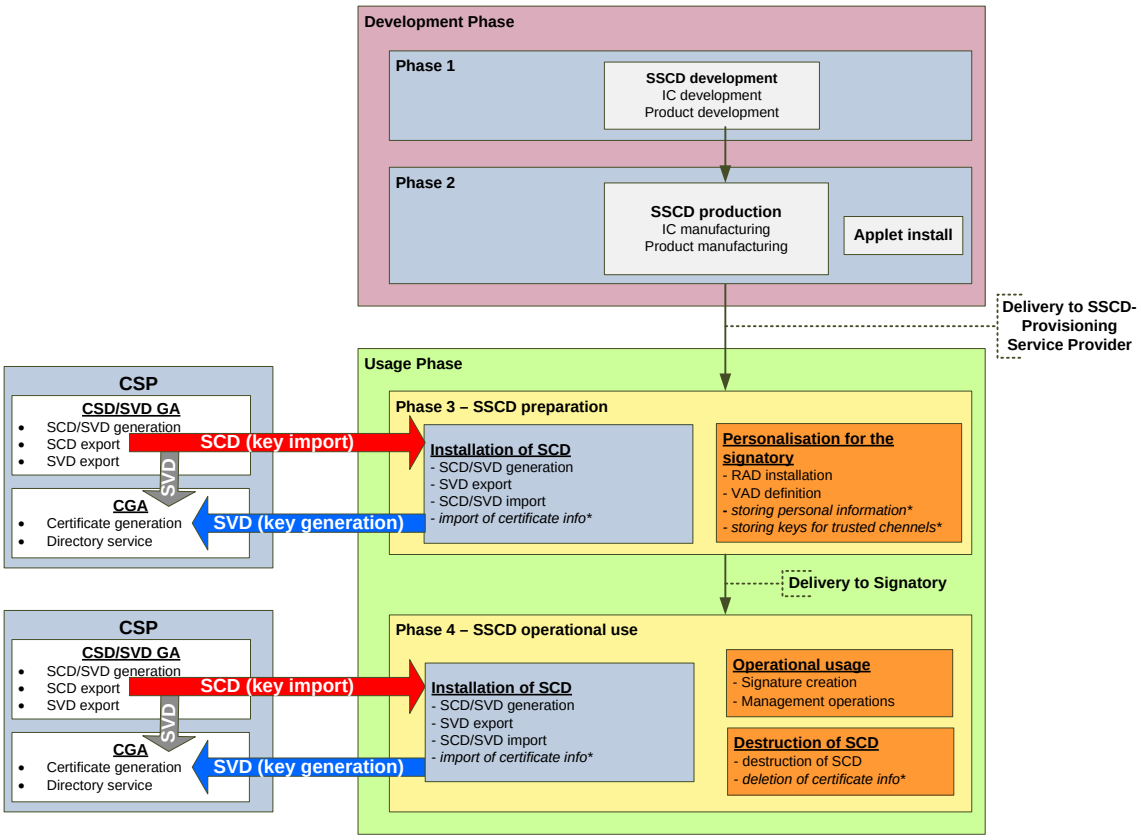
4.3.5.1. General

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. The TOE operational use stage begins when the signatory has obtained both the VAD and the TOE.

Figure 3 shows an example of the lifecycle where an SCD/SVD pair is generated on the TOE before delivery to the signatory. The lifecycle allow generation of SCD or SCD/SVD key pairs after delivery to the signatory as well.



*The asterisks * marks the optional import of the SVD and certificate info during TOE preparation and certificate info deletion when SCD is destroyed.*

Figure 3: TOE life cycle

4.3.5.2. Development stage

The subject manufacturer acts in the development phase. They are the IC Manufacturer and the Product Manufacturer.

IC Manufacturer provides the following activities:

(1) during phase 1 designs and develop IC and the embedded software
(2) during phase 2
    a) manufactures the IC and the embedded software,
    b) optionally, loads the applet if applet shall be present in the ROM and provides card pre personalization and initialization
    c) performs IC testing and packaging

Product Manufacturer provides following activities:

(1) during phase 1 designs and develops the product and the applet software,
(2) during phase 2
    a) manufactures the product performing card printing and IC embedding activities,
    b) optional, loads applet if applet shall be present in the EEPROM and provides card pre personalization and initialization
    c) performs product testing and packaging

For this product, the AKD eID Card 1.0, the IC Manufacturer is NXP and the Product Manufacturer is AKD.

Applet of the AKD eID Card 1.0 can be loaded into the ROM or the EEPROM. This is the only applet present on the card. There are no other applets on the card and post-issuance loading of applets cannot be done.

4.3.5.3. Preparation stage

Regarding [PP_SSCD_KG] an SSCD-provisioning service provider may ensure the following tasks:

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 this ST supports a centralised, pre-issuing key generation process, with at least one key generated and certified, before delivery 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 may support both key generation processes, for

example with a first key generated centrally and additional keys generated by the signatory in the operational use stage.

Data required for inclusion in the SVD certificate at least includes (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 may have been stored in the SSCD during personalization.

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 may support a function to provide an explicit proof of correspondence between an SCD it stores and an SVD realized by self-certification. Such a function may be performed implicitly in the SVD export function and may be invoked in the preparation environment without explicit consent of the signatory. 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_KG_TCCGA].

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 [PP_SSCD_KI] an SSCD-provisioning service provider may ensure 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 [PP_SSCD_KG_TCCGA] an SSCD-provisioning service provider may ensure 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.

4.3.5.4. Operational use stage

Regarding [PP_SSCD_KG] and [PP_SSCD_KI]:

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

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

Regarding [PP_SSCD_KG_TCCGA]:

- 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.

5. Conformance Claims

5.1. Common Criteria Conformance Claim

This ST claims to be conformant to the Common Criteria Version 3.1, Revision 4, which is comprised of:

- [CC_P1] - Common Criteria for Information Technology Security Evaluation (CC), Part 1: Introduction and general model; September 2012, Version 3.1, Revision 4
- [CC_P2] - Common Criteria for Information Technology Security Evaluation (CC), Part 2: Security functional components; September 2012, Version 3.1, Revision 4
- [CC_P3] - Common Criteria for Information Technology Security Evaluation (CC),Part 3: Security assurance components; September 2012, Version 3.1, Revision 4

as follows:

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

Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; September 2012, Version 3.1, Revision 4 has been taken into account.

5.2. Protection Profile 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, submitted to the enquiry procedure under the reference prEN 14169-2, registered and certified under the reference BSI-CC-PP-0059-2009-MA-01 [PP_SSCD_KG],
- 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 [PP_SSCD_KI] and
- 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 [PP_SSCD_KG_TCCGA].

5.3. Package Claim

This security target is package conformant to EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

5.4. Conformance Rationale

5.4.1. Main aspects

(1) The TOE Description (sec 4.3) is based on PPs and has been extended by product specific details.

(2) All definition in the Security problem definition (sec 6), Security objectives (sec 7) and Security requirements (sec 9) have been included in the ST exactly in the same wording of the PPs.

(3) The all application notes from the PPs are kept in this ST. The following comment has been added:

- "PP - Information" - if the application note from the PP is repeated in the same wording as the PP
- "PP - Applied" - if the application note from the PP is changed or explained
- "ST - Added" - if the additional application note is added by the ST author

5.4.2. Differences between ST and PP

This ST uses possibility of combining the functionalities of the PPs, which is allowed by the [PP_SSCD_O]. This implies for this ST:

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

(2) The SPD in the [PP_SSCD_KI] and [PP_SSCD_KG_TCCGA] include all the SPD of the [PP_SSCD_KG]. The SPD for the [PP_SSCD_KI] add the additional assumption A.CSP, which is not present in [PP_SSCD_KG].

(3) The OT.SVD_Auth_Gen of the [PP_SSCD_KG] is correspondent to the OT.SCD/SVD_Gen in all other PPs.

(4) Security objectives for the TOE in the [PP_SSCD_KG], which are identically stated in the [PP_SSCD_KI], 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).

(5) The remaining security objectives for the TOE in the [PP_SSCD_KG] 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_KI]. Instead, in [PP_SSCD_KI] 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.

(6) The remaining security objective for the TOE OT.SCD_Auth_Imp in the [PP_SSCD_KI] is related to SCD import only and is therefore not present in [PP_SSCD_KG].

(7) The TOE type of the [PP_SSCD_KG_TCCGA] is the same as the TOE type of the core [PP_SSCD_KG]: the TOE is a combination of hardware and software configured to securely create, use and manage signature creation data.

(8) The security problem definition (SPD) of the [PP_SSCD_KG_TCCGA] contains the security problem definition of the core [PP_SSCD_KG]. The SPD for it is described by the same threats, organisational security policies and assumptions as for the TOE in core [PP_SSCD_KG].

(9) The security objectives for the TOE in the [PP_SSCD_KG_TCCGA] include all the security objectives for the TOE of the core [PP_SSCD_KG] and add the security objective OT.TOE_SSCD_Auth (Authentication proof as SSCD) and OT.TOE_TC_SVD_Exp (Trusted channel for SVD).

(10) The security objectives for the operational environment in the [PP_SSCD_KG_TCCGA] include all security objectives for the operational environment of the core [PP_SSCD_KG] 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.

(11) The SFRs specified in the [PP_SSCD_KG_TCCGA] includes all security functional requirements (SFRs) specified in the core [PP_SSCD_KG]. It includes additional SFRs FIA_API.1, FDP_DAU.2/SVD and FTP_ITC.1/SVD.

(12) The [PP_SSCD_KG_TCCGA] does not provide completion of all operations left to the ST writer in the core [PP_SSCD_KG]. It provides operation of the SFR FIA_UAU.1 of the core PP.

(13) The SARs specified in the [PP_SSCD_KG_TCGA] includes all SAR specified in the core [PP_SSCD_KG]. It does not include additional SAR not included in the core [PP_SSCD_KG].

6. Security problem definition

6.1. 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.

6.2. Threats

6.2.1. 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.

6.2.2. 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.

6.2.3. 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.

6.2.4. 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.

6.2.5. 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.

6.2.6. 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.

6.2.7. 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.

6.3. Organisational security policies

6.3.1. 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.

6.3.2. 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.

6.3.3. 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.

6.3.4. 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.

6.4. Assumptions

6.4.1. 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.

6.4.2. 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.

6.5. Further assumption regarding key import

6.5.1. 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.

7. 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.

7.1. Security objectives for the TOE

7.1.1. Security objectives regarding all PPs

7.1.1.1. OT.Lifecycle_Security *Lifecycle security*

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

Application note 1: [PP_SSCD_KG] (app. note 1) and [PP_SSCD_KI] (app. note 1) - Information
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.

7.1.1.2. OT.SCD_Secrecy *Secrecy of the signature creation data*

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

Application note 2: [PP_SSCD_KG] (app. note 2) and [PP_SSCD_KI] (app. note 2) - Information
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.

7.1.1.3. 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.

7.1.1.4. 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.

7.1.1.5. 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.

7.1.1.6. 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.

7.1.1.7. 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.

7.1.1.8. OT.Tamper_Resistance *Tamper resistance*

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

7.1.2. Security objectives regarding the key generation

7.1.2.1. 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.

7.1.2.2. 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.

7.1.2.3. 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.

7.1.3. Security objectives regarding the key import

7.1.3.1. 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

7.1.4. Security objectives regarding the trusted communication with CGA

7.1.4.1. 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.

7.1.4.2. 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.

7.2. Security objectives for the operational environment

7.2.1. Security objectives for the operational environment regarding all PPs

7.2.1.1. 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.

7.2.1.2. 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.

7.2.1.3. 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.

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

The signatory shall use a trustworthy SCA that

- generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,
- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
- attaches the signature produced by the TOE to the data or provides it separately.

Application note 3: [PP_SSCD_KG] (app. note 3) and [PP_SSCD_KI] (app. note 3) - Information

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.

7.2.1.5. 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.

7.2.1.6. 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.

7.2.2. Security objectives for the operational environment regarding key import

7.2.2.1. 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.

7.2.2.2. 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.

7.2.2.3. 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.

7.2.2.4. 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.

7.2.3. Security objectives for the operational environment regarding the trusted communication with CGA

7.2.3.1. 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).

7.2.3.2. 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.

7.2.3.3. 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_KG_TCCGA] 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_KG].

7.3. Security Objectives Rationale

7.3.1. 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
T.SCD_Divulg		X										X		
T.SCD_Derive			X							X				
T.Hack_Phys		X				X	X	X						
T.SVD_Forgery											X			X
T.SigF_Misuse	X			X	X									
T.DTBS_Forgery					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

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

	OE.CGA_QCert	OE.SVD_Auth	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	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
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	

	OE.CGA_QCert	OE.SVD_Auth	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	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
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
A.CGA	X	X											
A.SCA			X	X									
A.CSP							X	X	X	X			

7.3.2. Security objectives sufficiency

Countering of threats by security objectives:

T.SCD_Divulg (*Storing, copying and releasing of the signature creation data***)** addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in recital (18) of [The Directive]. This threat is countered by

- OT.SCD_Secrecy, which assures the secrecy of the SCD 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.

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

T.Hack_Phys (*Exploitation of physical vulnerabilities***)** deals with physical attacks exploiting physical vulnerabilities of the TOE.

OT.SCD_Secrecy preserves the secrecy of the SCD.

OT.EMSEC_Design counters physical attacks through the TOE interfaces and observation of TOE emanations.

OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tampering attacks.

T.SVD_Forgery (*Forgery of the signature verification data*) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by

- OT.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and
- OE.SVD_Auth , 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.

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

T.Sig_Forgery (*Forgery of the electronic signature***)** deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique, 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.

Enforcement of OSPs by security objectives:

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

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the 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.

Upkeep of assumptions by security objectives:

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

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

A.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).

8. Extended Component Definition

8.1. 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.
The definition of the family FPT_EMS is taken from the [PP_SSCD_KG].

8.2. 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.

The definition of the FIA_API family is taken from [PP_SSCD_KG_TCCGA].

9. Security requirements

9.1. Security Functional Requirements

9.1.1. Use of requirement specifications

The perform operations (assignment, iteration, selection and refinement) of the SFR are printed in ***italicized bold***.

Parts copied from the PPs are printed in **bold** and underline as when operation is already performed in the PP.

9.1.2. Cryptographic support (FCS)

Application note 4: [PP_SSCD_KG] (app. note 4)- Information

Member states of the European Union have specified entities as responsible for accreditation and supervision of the evaluation process for products conforming to this standard and for determining admissible algorithms and algorithm parameters (the directive: 1.1b and 3.4). The ST writer shall consult with these entities to learn of admissible algorithms and cryptographic key sizes and other parameters or applicable standards.

9.1.2.1. 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 with zeros by method (e.g. clearKey) , according to sec. 6.1.2.4 of [JCOP_ST]*** that meets the following: ***none***.

Application note 5: [PP_SSCD_KG] (app. note 6) - Information

The specified cryptographic key destruction methods include but are not limited to overwriting the cryptographic key with any fixed or random data e.g. by generation of a new key.

Application note 6: [PP_SSCD_KI] (app. note 4) - Information

The cryptographic key SCD will be destroyed on demand of the signatory. The signatory may want to destruct the SCD stored in the SSCD e.g. after the qualified certificate for the corresponding SVD is not valid any more.

9.1.2.2. FCS_COP.1/Signature_Creation *Cryptographic operation*

Hierarchical to: No other components.

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

FCS_COP.1.1/ Signature_Creation: The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm ***RSA signature algorithm with EMSA-PKCS1-v1_5 encoding and SHA-1 and SHA-256*** and cryptographic key sizes ***2048 Bit*** that meet the following: ***RSASSA-PKCS1-v1.5 of [PKCS#1 v2.1], according to FCS_COP.1.1/ RSASignaturePKCS#1 in sec. 6.1.2.5 of [JCOP_ST] .***

Application note 7: [PP_SSCD_KG] (app. note 7) - Information
The operations in the element FCS_COP.1.1/Signature_Creation shall be appropriate for the SCD/SVD pairs generated according to FCS_CKM.1. Note that for some cryptographic algorithm like RSA padding is important part of the signature creation algorithm.
Application note 8: [PP_SSCD_KI] (app. note 5) - Information
The operations in the element FCS_COP.1.1/Signature_Creation shall be appropriate for the SCD imported according to FTP_ICT.1/SCD.
Application note 9: ST – Added
The mandatory hash algorithm for digital signature is SHA-256. It is recommended to use SHA-256 for all applications, but for compatibility reasons, the TOE also supports SHA-1.

9.1.2.3. FCS_COP.1/RSACipher *Cryptographic operation*

Hierarchical to: No other components.

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

FCS_COP.1.1/ RSAChiper: The TSF shall perform ***encryption and decryption*** in accordance with a specified cryptographic algorithm ***RSA encryption/decryption algorithm with EME-PKCS1-v1_5 encoding*** and cryptographic key sizes ***2048 Bit*** that meet the following: ***[PKCS#1 v2.1], according to FCS_COP.1.1/RSACipher, sec. 6.1.2.5 of [JCOP_ST]***

9.1.3. 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	(The PP does not define security attributes for SVD)	(The PP does not define security attributes for SVD)

9.1.3.1. 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.

9.1.3.2. 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”.

9.1.3.3. 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":

9.1.3.4. 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.

9.1.3.5. 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.

Application note 10: [PP_SSCD_KG] (app. note 10) and [PP_SSCD_KI] (app. note 8) - Information
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).

9.1.4. Identification and authentication (FIA)

9.1.4.1. 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*
on behalf of the user to be performed before the user is identified.

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

Application note 11: [PP_SSCD_KG] (app. note 11) and [PP_SSCD_KI] (app. note 9) - Applied
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.
The TOE may identify the user by default or by selection of the role, and RAD against the authentication will be performed.
Identification by default is normally linked to the TOE lifecycle, e.g. the TOE will identify by default the Administrator before the signatory's RAD is created and the signatory if signatory's RAD exists. The users may identify themselves as Administrator by selection of an authentication key as Administrator and therefore authentication will be performed by mutual device authentication.

9.1.4.2. 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*
on behalf of the user to be performed before the user is authenticated.

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

Application note 12: [PP_SSCD_KG_TCCGA] (app. note 1) - Information
The [PP_SSCD_KG_TCCGA] performed the operation of the bullet (3) in the element FIA_UAU.1.1 of the [PP_SSCD_KG] by adding the establishment of a trusted channel to the CGA.

9.1.4.3. FIA_AFL.1/PIN *Authentication failure handling*

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PIN 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/PIN When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD.

Application note 13: [PP_SSCD_KG] (app. note 13) and [PP_SSCD_KI] (app. note 11) - information
The assignment is consistent with the implemented knowledge based authentication mechanism.
Application note 14: ST – Added
When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD of the PIN. The minimal length of the PIN value is configurable and shall be defined during the card preparation.

9.1.4.4. FIA_AFL.1/PUK *Authentication failure handling*

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PUK 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/PUK When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD.

Application note 15: ST – Added
When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD of the PUK.
The minimal length of the PUK value is configurable and shall be defined during the card preparation.

9.1.5. Security management (FMT)

9.1.5.1. 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.

9.1.5.2. 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***

9.1.5.3. 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.

9.1.5.4. 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.

Application note 16: ST - Added
This ST combines the assignments SCD/SVD_Generation_SFP from the [PP_SSCD_KG] and the SCD Import SFP from the [PP_SSCD_KI].

9.1.5.5. 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.

9.1.5.6. 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.

Application note 17: [PP_SSCD_KG] (app. note 15) and [PP_SSCD_KI] (app. note 13) – Applied
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"

9.1.5.7. 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.

Application note 18: ST - Added
This ST combines the assignments CD/SVD Generation SFP, SVD Transfer SFP and Signature Creation SFP from the [PP_SSCD_KG] and the SCD Import SFP from the [PP_SSCD_KI].

9.1.5.8. 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.

Application note 19: [PP_SSCD_KG] (app. note 16) – Applied

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

Application note 20: ST – Added

The bullet (3) and (4) are added according to [PP_SSCD_KI].

9.1.5.9. 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.

9.1.5.10. 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.

9.1.6. Protection of the TSF (FPT)

9.1.6.1. 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 ***attackers*** are unable to use the following interface ***electrical contacts*** to gain access to RAD and SCD.

Application note 21: [PP_SSCD_KG] (app. note 18) and [PP_SSCD_KI] (app. note 15) - Information
The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE, or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.
Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

9.1.6.2. 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) ***those associated to the potential security violations described in FAU_ARP.1 of the underlying java card open platform [JCOP_ST]***
(3) ***inconsistencies in the calculation of the signature.***

Application note 22: [PP_SSCD_KG] (app. note 19) and [PP_SSCD_KI] (app. note 16) - Information
The assignment (1) addresses failures detected by a failed self-test and requiring appropriate action to prevent security violation. When the TOE is in a secure state, the TSF shall not perform any cryptographic operations and all data output interfaces shall be inhibited by the TSF.

9.1.6.3. 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.

9.1.6.4. 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.

Application note 23: [PP_SSCD_KG] (app. note 20) and [PP_SSCD_KI] (app. note 17) - Information
The TOE will implement appropriate measures to continuously counter physical tampering which may compromise the SCD. The "automatic response" in the element FPT_PHP.3.1 means (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time. Due to the nature of these attacks the TOE can by no means detect attacks on all of its elements (e.g. the TOE is destroyed). But physical tampering must not reveal information of the SCD. E.g. the TOE may be physically tampered in power-off state of the TOE (e.g. a smart card), which does not allow TSF for overwriting the SCD but leads to physical destruction of the memory and all information therein about the SCD. In case of physical tampering the TFS may not provide the intended functions for SCD/SVD pair generation or signature creation but ensures the confidentiality of the SCD by blocking these functions. The SFR FPT_PHP.1 requires the TSF to react on physical tampering in a way that the signatory is able to determine whether the TOE was physical tampered or not. E.g. the TSF may provide an appropriate message during start-up or the guidance documentation may describe a failure of TOE start-up as indication of physical tampering.

9.1.6.5. 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 ***on start-up, upon detection of a potential security violation and in fulfillment of FPT_FLS.1*** 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.

Application note 24: [PP_SSCD_KG] (app. note 21) and [PP_SSCD_KI] (app. note 17)- Information
The component FPT_TST.1 addresses only the self-test of the TSF. If the TSF relays on security feature of the hardware platform of part of the TOE, the ST should consider inclusion FPT_TEE.1 to require the TSF to test these features for correct work of the dependent TSF.

9.1.7. Security functional requirements regarding key generation

9.1.7.1. 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 ***JCOP RNG*** and specified cryptographic key sizes ***of RSA 2048 Bit*** that meet the following: ***ISO 15946-1-2008, according to sec. 6.1.2.1 of [JCOP_ST]*** .

Application note 25: [PP_SSCD_KG] (app. note 5)- Information
The refinement in the element FCS_CKM.1.1 substitutes "cryptographic keys" by "SCD/SVD pairs" because it clearly addresses the SCD/SVD key generation.

9.1.7.2. 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.

9.1.7.3. 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.

9.1.7.4. 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.

9.1.7.5. 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.

Application note 26: [PP_SSCD_KG] (app. note 9) - Applied
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.

According to the [PP_SSCD_KG_TCCGA], the TOE implements additional security functions to support the export of public keys with integrity and data origin authentication.

9.1.8. Security functional requirements regarding key import

9.1.8.1. 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.

9.1.8.2. 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.

9.1.8.3. 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: ***SCD shall be sent by an authorized CSP***.

9.1.8.4. 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.

Application note 27: [PP_SSCD_KI] (app. note 7) - Information
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.
Application note 28: ST – Added
The TOE supports the establishment of a trusted channel with secure messaging and negotiation of cryptographic keys used for the adequate protection of the communication data. The secure messaging provided by the TOE is using encryption and decryption with Triple-DES in CBC mode and cryptographic key size of 112 bit, as well as message authentication code with Retail MAC and cryptographic key size of 112 bit according to [ISO 9797-1]. For implementation secure messaging, refer to sec. 9 of [EN 14890-1].

9.1.8.5. 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;***

Application note 29: [PP_SSCD_KI] (app. note 19) - Information
The component FTP_ITC.1 requires the TSF to support a trusted channel established to another trusted IT product generating the SCD/SVD pair for import the SCD as described by FDP_UCT.1/SCD.

9.1.9. Security functional requirements regarding trusted communication with CGA

9.1.9.1. FIA_API.1 *Authentication Proof of Identity*

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

FIA_API.1.1 The TSF shall provide a ***symmetric or asymmetric device authentication mechanism*** to prove the identity of the SSCD.

Application note 30: [PP_SSCD_KG_TCCGA] (app.note 2) - Information
Via the authentication mechanism to be assigned here the TOE has to be able to authenticate itself as SSCD to the CGA, using authentication data implemented in the TOE during pre-initialisation phase.
Application note 31: ST – Added
The TOE supports device authentication mechanisms, which allows mutual authentication of the TOE as SSCD and remote entity.
The TOE implements the symmetric authentication scheme based on Triple-DES keys as defined in sec. 8.8. of [EN 14890-1]. A successfully authentication mandates the both parts (TOE & IFD) share the same Triple-DES keys.
The TOE also implements the device authentication with privacy protection based on Diffie-Hellman key exchange and RSA signature generation and verification (RSASSA-PKCS1-v1_5) using SHA-1 or SHA-256 as defined in sec. 8.5 of [EN 14890-1].

9.1.9.2. 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.

Application note 32: ST – Added
This SFR is implemented by the device authentication mechanisms, which allows external authentication of the CGA and internal authentication of the TOE as SSCD. Via the trusted

channel, the user can authentically export the public signature key for certification and import the certificate or certificate information for the public signature key.
In the context of asymmetric device authentication schemes the TOE implements Card verifiable (CV) certificates to import a public key and related attributes into the TOE. The TOE support the RSA signature verification of CV certificates using SHA-1 and SHA-256 and cryptographic key size 2048 Bit that meet the RSASSA-PKCS1-v1.5.
The structure of the supported CV certificates and the card internal verification process as well as details about possible certification hierarchies can be found in sec. 14.3. of [EN 14890-1].

9.1.9.3. 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***

Application note 33: [PP_SSCD_KG_TCCGA] (app. note 4) - Information
The component FTP_ITC.1/SVD requires the TSF to enforce a trusted channel established by the CGA to export the SVD to the CGA.
Application note 34: [PP_SSCD_KG_TCCGA] (app. note 5) – Applied
The TSF enforces a trusted channel established by the CGA to export the SVD to the CGA.
Application note 35: ST – Added
The TOE supports the establishment of a trusted channel with secure messaging and negotiation of cryptographic keys used for the adequate protection of the communication data. The secure messaging provided by the TOE is using encryption and decryption with Triple-DES in CBC mode and cryptographic key size of 112 bit, as well as message authentication code with Retail MAC and cryptographic key size of 112 bit according to [ISO 9797-1]. For implementation secure messaging, refer to sec. 9 of [EN 14890-1].

9.2. 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 4: Security assurance requirements.

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
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

9.3. Security Requirements Rationale

9.3.1. Security Requirements Coverage

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

Functional requirements \ TOE security objectives	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
FCS_CKM.4	X	X												
FCS_COP.1/Signature_Creation	X		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
FCS_COP.1/RSACipher	X		X											
FDP_ACC.1/Signature_Creation	X			X										
FDP_ACF.1/Signature_Creation	X			X										
FDP_RIP.1		X		X										
FDP_SDI.2/Persistent		X	X								X			
FDP_SDI.2/DTBS				X	X									
FIA_AFL.1/PIN				X										
FIA_AFL.1/PUK				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_SMR.1	X			X										
FMT_SMF.1	X			X							X			
FPT_EMS.1		X				X								
FPT_FLS.1		X												
FPT_PHP.1							X							
FPT_PHP.3		X						X						
FPT_TST.1	X	X	X											
FCS_CKM.1	X	X								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													
FDP_UCT.1/SCD	X	X												
FTP_ITC.1/SCD	X	X												
FDP_DAU.2/SVD														X
FIA_API.1													X	
FTP_ITC.1/SVD														X

9.3.2. TOE Security Requirements Sufficiency

The rationale in the [PP_SSCD_KG], 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_KG].

The rationale for the security objective OT.SCD_Auth_Imp is from [PP_SSCD_KI] 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_KG_TCCGA].

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.

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.

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.

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.

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.

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/PIN and FIA_AFL.1/PUK provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.

The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process).

The security functions specified by FDP_ACC.1/Signature_Creation and FDP_ACF.1/Signature_Creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4.

The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory.

FMT_MOF.1 restricts the ability to enable the signature creation function to the signatory.

FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

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

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

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

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

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

OT.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_KG]) establishment of the trusted channel before (human) user is authenticated.

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

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

9.3.3. 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	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4 FDP_ITC.1/SCD
FCS_COP.1/RSAChiper	[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

Functional requirement	Dependencies	Satisfied by
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/PIN	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/PUK	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
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

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)	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

9.3.4. Rationale for chosen security assurance 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 specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in ST is just such a product.
Augmentation results from the selection of additional assurance requirements are:

- 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

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.
The EAL4 requires for the development security the assurance component ALC_DVS.1. This dictates a documentation and check of the security measures in the development environment. The component ALC_DVS.2 requires additionally a justification, that the measures provide the necessary level of protection.

10. TOE Summary Specification

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

10.1. Security Functionality

Security functionalities provided by the composite TOE are listed the table 8.

Table 8: Security functionalities

Security function	Description
SF.USER	User authentication
SF.DEV	Device authentication
SF.SM	Trusted channel
SF.ACCESS	Role authentication
SF.CRYPTO	Cryptographic functions
SF.PROTECT	Self protection

10.1.1. SF.USER *User authentication*

This TOE security functionality (SF) implements the user authentication mechanism used for the user role Signatory. It is based on the knowledge of a PIN or a password. The PIN is an alphanumeric value with a specified minimal length. This minimal length is configurable and is defined during the card preparation.
The TOE has two PIN values and one PUK value. One PIN is used for digital signature authentication exclusively. Another PIN is used to authentication the all other operations. The same PUK value is used for unblock both PINs.
The TOE support:

- The VERIFY command: The Signatory is authenticated by the verification process. After the PIN is successfully verified, the Signatory is allowed to execute selected crypto operation.
- The CHANGE REFERENCE DATA command: Upon successful command execution, the reference data inside the card is replaced by the new reference data provided in the command data field. The initial PIN has to be changed before the TOE is used for the first time.
- The RESET RETRY COUNTER command: A retry counter and an initial value of the retry counter are represented by a configurable number from 1 to 127 for each RAD separately. These values are defined during card preparation. If the verification fails, the retry counter is decremented by one and an error status that contains the remaining attempts is returned by the application. When the retry counter equals zero, the RAD is blocked and can no longer be used. A successful verification of the RAD resets its retry counter to the initial value. The TOE used the same rules, but separated RAD values for the PIN and for the PUK value.
  Once a PIN is blocked, the Signatory can use a PUK (resetting code) to unblock RAD, i.e. to reset the corresponding retry counter to its initial value and optionally to set new RAD.
  If the PUK verification fails, its tries counter is decremented by one. When all available tries have failed, the PUK is blocked. The only role Administrator can reset the blocked PUK.

This SF provides the user authentication for the operation depending on the subject and life cycle state and according the access control (see SF.ACCESS).

10.1.2. SF.DEV *Device authentication*

This TOE security functionality (SF) implements device authentication mechanisms, which allows mutual authentication of the TOE as SSCD and remote entity.
The TOE implements:

(1) Symmetric authentication scheme

The TOE implements the mutual authentication scheme using symmetric keys as defined in sec. 8.8. of [EN 14890-1].
The MUTUAL AUTHENTICATE command is used to:

1. Authenticate the terminal and the card.
2. Generate two temporary session keys that will be further used to compute session keys for the secure messaging in the subsequent commands.
3. Initialize the Send Sequence Counter (SSC), which is a counter used at each checksum computation.

The authentication procedure is based on a Symmetric Key Set (KS) that is composed of two Triple-DES Keys. A successfully authentication mandates the both parts (TOE & IFD) share the same Triple-DES keys.

(2) **Asymmetric authentication scheme**

a) Card verifiable certificate verification commands

The TOE implements Card verifiable (CV) certificates in the context of asymmetric device authentication schemes to import a public key and related attributes into the TOE. These certificates are non-self descriptive certificates.
The structure of the supported CV certificates and the card internal verification process as well as details about possible certification hierarchies can be found in sec. 14.3. of [EN 14890-1].

b) Device authentication with privacy protection

The device authentication with privacy protection scheme is based on sec. 8.5 of [EN 14890-1].
To avoid the card disclosing private information, such as identity, a secure channel session is established before any other operation. To do so, the protocol starts with an unauthenticated Diffie-Hellman key exchange and then authenticates the IFD before the ICC.
Five main phases may be distinguished:

1. agreement of session keys and establishment of a secure channel for privacy protection;
2. transport of the IFD public key to the TOE;
3. external authentication of the IFD;
4. transport of the TOE public key to the IFD;
5. internal authentication of the TOE.

During card preparation, the issuer chooses the authentication scheme and set the keys for device authentication.
Two kinds of environments shall be distinguished, by considering the device authentication of the remote entity: the signing and the management environment. Remote entity might be SCA, CGA or HID in the signing environment or Signatory SSCD Management Application and Issuer SSCD Management Application in the management environment. During personalisation phase, the issuer will define the access rules to the application resources for both environments. The IFD shall adapt the authentication to the environment required by the resource it wishes to access (see SF.ACCESS).
A successful TOE-IFD mutual authentication with session keys establishment is combined with secure messaging for all subsequent commands (see SF.SM).

The device authentication security functionality provided by the TOE using cryptographic operations of the platform (see d), e) and h) of sec. 10.1.5 SF.CRYPTO).

10.1.3. SF.SM *Secure messaging*

This TOE security functionality (SF) implements secure messaging protocol, which aims at ensuring communication between the IFD and the TOE when the TOE is used within an untrusted environment.
The secure channel is established through a device authentication (see SF.DEV). Session keys required for the secure messaging protocol are derived during the device authentication protocol. These keys are derived according to sec. 8.9. of [EN 14890-1].
After successful device authentication, the Send Sequence Counter (SSC) number is initialized.
The secure channel remains open as long as the incoming commands are correctly wrapped with the secure messaging session keys and the SSC. The SSC is defined, initialised and handled as specified in sec. 8.10. of [EN 14890-1].
When the secure messaging session is closed or if error detection has occurred, MAC value and session keys will be erased. For the treatment of secure messaging errors, refer to sec. 9.3 of [EN 14890-1]. For ending a secure messaging session, refer to sec. 8.12.2 of [EN 14890-1].
The secure messaging security functionality provided by the TOE using cryptographic operations of the platform (see b) and g) of sec. 10.1.5 SF.CRYPTO).

10.1.4. SF.ACCESS *Role authentication*

The Role authentication security functionality provided by the TOE is used by the external entity to present a specific authorization to the TOE.

The TOE establishes the security context by setting a respective value in its security environment and enforces using correct security policy. Prior any operation the application checks the requested access rights to resources and operations on them. If security conditions are fulfilled the access is granted.

Once the authentication was successfully performed, its internal status is set to “authenticated”. The checking of this status allows to the TOE to grant the access condition on its resources and operations.

The TOE maintains the roles for Signatory and for Administrator by this means, to grant different access rights, e.g. The TOE require authentication for a specific operation.

When a Signatory wants authenticated to the TOE he has to prove it with a knowledge based User authentication (SF.USER). The role Signatory exists only in operational phases in signatory environment.
When an Administrator authenticates to the TOE he has to prove it with a challenge-response mechanism. This mechanism is based on symmetric or asymmetric keys and realized through device authentication (SF.DEV) during which both side have authenticated and credentials have exchanged. The role Administrator exists during the preparation and during operational phases in management environment to implement management operations on the TOE.

The symmetric role authentication distinguishes two phases:

1) establishment of the security context by setting a respective value in the security environment of the TOE;
2) external authentication of the IFD.

The asymmetric role authentication distinguishes tree phases:

1) verifying the certificate chain and simultaneously checking the role ID authorization;

2) establishment of the security context by setting a respective value in the security environment of the TOE;
3) external authentication of the IFD.

10.1.5. SF.CRYPTO *Cryptographic functions*

This TOE security functionality (SF) is totally provided by the certified platform, which ensures secure cryptographic key management and cryptographic operation of the TOE.

The exact formulation can be found in the [JCOP_ST] :

a) SCD/SVD Key pair generation – provide RSA key generation algorithm key size of 2048 Bit based on random numbers according to AIS 20 class DRG.2 or DRG.3 according to FCS_CKM.1.1 and FCS_RNG.1, sec. 6.1.2.1 and 6.1.14.4 of [JCOP_ST] (see 9.1.7.1 FCS_CKM.1).
b) Session Key generation – provide DES key generation algorithm key size of 112 bit according to FCS_CKM.1.1 and FCS_RNG.1, sec. 6.1.2.1 and 6.1.14.4 of [JCOP_ST] (see 9.1.8.5 FTP_ITC.1/SCD, 9.1.9.3 FTP_ITC.1/SVD, 9.1.10.2 FTP_ITC.1/VAD and 9.1.10.3 FTP_ITC.1/DTBS).
c) Destruction of cryptographic keys - cryptographic key destruction method by physically overwriting the keys with zeros by method (e.g. clearKey) according to FCS_CKM.4.1 sec. 6.1.2.4 of [JCOP_ST] (see 9.1.2.1 FCS_CKM.4).
d) Symmetric data encryption and decryption – provide cryptographic algorithm in CBC Mode with padding method 2 and cryptographic key sizes for 2-key TDES (112 bit) that meet the ISO 9797-1 padding method 2 [ISO 9797-1] which provides limited side channel resistance according to FCS_COP.1.1/TripleDES, sec. 6.1.2.5 of [JCOP_ST] (see 9.1.9.1 FIA_API.1, 9.1.9.2 FDP_DAU.2/SVD).
e) Asymmetric data encryption and decryption – provide cryptographic algorithm RSA encryption/decryption algorithm with EME-PKCS1-v1_5 encoding and cryptographic key sizes 2048 bits that meet the [PKCS#1 v2.1] according to FCS_COP.1.1/RSACipher, sec. 6.1.2.5 of [JCOP_ST] (see 9.1.2.3 FCS_COP.1/RSACipher, 9.1.9.1 FIA_API.1 and 9.1.9.2 FDP_DAU.2/SVD).
f) Digital signature generation and verification – provide cryptographic algorithm RSA signature algorithm with EMSA-PKCS1-v1_5 of [PKCS#1 v2.1] encoding and SHA-1 and SHA-256 and cryptographic key size 2048 Bit that meet the RSASSA-PKCS1-v1.5., according to FCS_COP.1.1/RSASignaturePKCS#1, sec. 6.1.2.5 of [JCOP_ST] (see 9.1.2.2 FCS_COP.1/Signature_Creation).
g) Secure messaging – provide 8 byte MAC generation and verification in accordance with cryptographic algorithm Triple-DES in outer CBC MAC Mode and cryptographic key size 112 Bit that meet the MAC Algorithm 3 with padding method 2 (Retail MAC) of [ISO 9797-1] according to FCS_COP.1.1/DESMAC, sec. 6.1.2.5 of [JCOP_ST] (see 9.1.8.5 FTP_ITC.1/SCD, 9.1.9.3 FTP_ITC.1/SVD, 9.1.10.2 FTP_ITC.1/VAD and 9.1.10.3 FTP_ITC.1/DTBS)
h) Secure hash computation – provide SHA-1 and SHA-256 that meet the [FIPS 180-3] according to FCS_COP.1.1/SHA-256, sec. 6.1.2.5 of [JCOP_ST]. The mandatory hash algorithm for digital signature is SHA-256. It is recommended to use SHA-256 for all applications, but for compatibility reasons, the TOE also supports SHA-1.

All these algorithms taken from the platform and supported by TOE are listed in the [CEN/TS 15480-2] as mandatory algorithms for the European Citizen Card as follows:

- RSA with SHA-256 are mandatory algorithms for digital signature

- SHA-1 and SHA-256 are mandatory hash algorithms for device authentication and key derivation
- RSA acc. to [PKCS#1 v2.1] is mandatory algorithm for digital signature and input formats
- RSA with to [PKCS#1 v2.1] is mandatory and conditional algorithm for client/server authentication and encryption key decipherment

The [EN 14890-1] (chapters 8 and 9) specification, which is required by the [CEN/TS 15480-2], predicts using 2-key-TDES for symmetrical authentication as well as Retail MAC for secure messaging.

Also, [TR 03116-2] (chapters 1.2.3 and 1.3.1) explicitly allows 2-Key-TDES for national ID cards. As the TOE is the SSCD-part of an ID card, the 2-Key-TDES mentioned in [TR 03116-2] is also valid for this TOE.

10.1.6. SF.PROTECT *Self protection*

This TOE security functionality (SF) is totally provided by the certified platform, which ensures self-protection of the TOE. The exact formulation can be found in the [JCOP_ST] :

a) Subset Residual Information Protection - Ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from the cryptographic buffer, according to FDP_RIP.1/KEYS, sec. 6.1.2.9 of [JCOP_ST] (see 9.1.3.3 FDP_RIP.1).

b) Stored data integrity monitoring and action - Monitoring user data stored in containers for integrity errors on cryptographic keys, PIN values and their associated security attributes, according to FDP_SDI.2.1, sec. 6.1.3.3 of [JCOP_ST] (see 9.1.3.4 FDP_SDI.2/Persistent and 9.1.3.5 FDP_SDI.2/DTBS).

c) TOE Emanation - ensure that unauthorized users are unable to use electrical contacts to gain access to stored data. The TOE shall not emit variations in power consumption or timing during command execution in excess of non-useful information enabling access to stored data according to FPT_EMSEC.1, sec. 6.1.14.6 of [JCOP_ST] (see 9.1.6.1 FPT_EMS.1).

d) Failure with preservation of a Secure State - preserve a secure state when the failures occur, according to FPT_FLS.1.1/SCP, sec. 6.1.12.1 of [JCOP_ST] (see 9.1.6.2 FPT_FLS.1 and 9.1.6.5 FPT_TST.1).

e) Security Alarms - accumulate or combine in monitoring the auditable events and indicate a potential violation. The following reactions by the TOE based on indication of a potential violation of the TSP are possible: throw an exception, terminate the card, reinitialize the Java Card System, respond automatically in the specified way and lock the card session, according to FAU_ARP.1, sec. 6.1.3.1 of [JCOP_ST] (see 9.1.6.2 FPT_FLS.1 and 9.1.6.4 FPT_PHP.1).

f) Resistance to physical attack - The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, —automatic response means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time, according to FPT_PHP.3/SCP, sec. 6.1.12.3 of [JCOP_ST] (see 9.1.6.4 FPT_PHP.3).

10.2. Security Functionality Rational

Table 9: Security Functionality Rational

	SF. USER	SF. DEV	SF.SM	SF.ACCESS	SF.CRYPTO	SF.PROTECT
FCS_CKM.4					X	
FCS_COP.1/Signature_Creation					X	
FCS_COP.1/RSAChiper					X	
FDP_ACC.1/Signature_Creation				X		
FDP_ACF.1/Signature_Creation				X		
FDP_RIP.1						X
FDP_SDI.2/Persistent						X
FDP_SDI.2/DTBS						X
FIA_AFL.1/PIN	X					
FIA_AFL.1/PUK	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		
FMT_MSA.4				X		
FMT_MTD.1/Admin				X		
FMT_MTD.1/Signatory				X		
FMT_SMR.1				X		
FMT_SMF.1				X		
FPT_EMS.1						X
FPT_FLS.1						X
FPT_PHP.1						X
FPT_PHP.3						X
FPT_TST.1						X
FCS_CKM.1					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_UCT.1/SCD			X			
FTP_ITC.1/SCD			X			
FDP_DAU.2/SVD		X				
FIA_API.1		X				
FTP_ITC.1/SVD			X			

11. Statement of Compatibility concerning Composite Security Target

11.1. Separation of the Platform-TSF

This section describes the separation of relevant security functionality described in the ST of the platform (JCOP v. 2.4.2, Revision 3 [JCOP_ST]) being used by this ST.

11.1.1. JCOP-functionality

The security functionality provided by the platform is summarized in [JCOP_ST] , chapter 1.3.1. The following table confronts the relevant security functionality of the platform with those of the composite TOE defined in the present ST. The table lists Security functionality of the platform and of this composite ST with the aim to separate platform functionality.

Table 10: JCOP Functionality

JCOP-functionality	Usage by TOE
Cryptographic algorithms and functionality:	
3DES (112 and 168 bit keys) for en-/decryption (CBC and ECB) and MAC generation and verification (Retail-MAC, CMAC and CBC-MAC)	3DES (112 bit keys) for CBC and Retail-MAC is used for SF.SM.
AES (Advanced Encryption Standard) with key length of 128, 192 and 256 Bit for en-/decryption (CBC and ECB) and MAC generation and verification (CMAC, CBC-MAC).	Not used
RSA and RSA CRT (1976 up to 2048 bits keys) for en-/decryption and signature generation and verification.	2048 bit key is used for SF.CRYPTO
RSA and RSA CRT key generation (1976 up to 2048 bits keys)	Only 2048 bit key is used for SF.CRYPTO
SHA-1, SHA-224, and SHA-256 hash algorithm	SHA-1 and SHA-256 is used for SF.CRYPTO
ECC over GF(p) algorithm that can be used for signature generation and signature verification (ECDSA) from 128 to 320 bits.	Not used
ECC over GF(p) key generation algorithm that can be used to generate ECC over GF(p) key pairs.	Not used
Random number generation according to class DRG.3 and DRG.2 of AIS 20	Used for SF.CRYPTO
Secure point addition for Elliptic Curves over GF(p).	Not used
Diffie-Hellman key agreement and EC-DH over GF(p).	Not used
Java Card 2.2.2 functionality:	
Garbage Collection fully implemented with complete memory reclamation incl. compactification	Used for SF.PROTECT
Support for Extended Length APDUs	Not used
Global Platform 2.2.1 functionality:	
CVM Management (Global PIN) fully implemented: all described APDU and API interfaces for this feature are present	Not used
Secure Channel Protocol (SCP01, SCP02, and SCP03) is supported	Not used
Card manager	Used for SF.PROTECT
Delegated management	Not used
Further platform functionality	
Proprietary SM Accelerator Interface, secure massaging API of JCOP 2.4.2 R3. The purpose of this API is to increase the performance of the secure messaging. It is specially designed for LDS applets which are used for the electronic passport as defined by ICAO.	Used for SF.SM

JCOP-functionality	Usage by TOE
Post-issuance installation and deletion of applets, packages and objects	Not used
Pre-personalization mechanism	Used for SF.PROTECT
A Secure Box concept is implemented within JCOP 2.4.2 R3. The Secure Box is a construct which allows to run non certified third party native code and ensures that this code cannot harm, influence or manipulate the JCOP 2.4.2 R3 operating system or any of the applets executed by the operating system. The separation of the native code in the Secure Box from other code and/or data residing on the hardware is ensured by the Hardware MMU which has been certified in the hardware evaluation.	Not used
MIFARE application accessible via contactless interface and via Java Card API (availability depends on configuration and hardware)	Not used

11.1.2. JCOP-SFRs used by this composite ST

The following table contains the all platform SFRs that are designated as “not used” or “used” by this composite ST. The only SFRs whose functionality is directly used to implement the SFRs of this composite ST are designated as “used”. This limit has been chosen although further security relevant functionality of the platform is necessary for the security of the whole composite TOE but the SFRs of this composite TOE are not directly concerned.

Table 11: JCOP SFRs

	JCOP-SFRs	Usage by TOE / Not used	Ref
6.1.1.	Firewall Policy		
6.1.1.1.	FDP_ACC.2/FIREWALL	Not used	-
6.1.1.2.	FDP_ACF.1/FIREWALL	Not used	-
6.1.1.3.	FDP_IFC.1/JCVM	Not used	-
6.1.1.4.	FDP_IFF.1/JCVM	Not used	-
6.1.1.5.	FDP_RIP.1/OBJECTS	Not used	-
6.1.1.6.	FMT_MSA.1/JCRE	Not used	-
6.1.1.7.	FMT_MSA.1/JCVM	Not used	-
6.1.1.8.	FMT_MSA.2/FIREWALL_JCVM	Not used	-
6.1.1.9.	FMT_MSA.3/FIREWALL	Not used	-
6.1.1.10.	FMT_MSA.3/JCVM	Not used	-
6.1.1.11.	FMT_SMF.1	Not used	-
6.1.1.12.	FMT_SMR.1	Not used	-
6.1.2.	Application Programming Interface		
6.1.2.1.	FCS_CKM.1	Used to implement FCS_CKM.1	10.1.5, a, b
6.1.2.2.	FCS_CKM.2	Not used	-
6.1.2.3.	FCS_CKM.3	Not used	-
6.1.2.4.	FCS_CKM.4	Used to implement FCS_CKM.4	10.1.5, c
6.1.2.5.	FCS_COP.1	Used to implement FCS_COP.1/Signature_Creation: • FCS_COP.1.1/RSASignaturePKCS#1 Used to implement FDP_UCT.1/SCD, FTP_ITC.1, FDP_DAU.2, FIA_API.1 and FDP_UIT.1: • FCS_COP.1.1/RSASignaturePKCS#1 • FCS_COP.1.1/TripleDES • FCS_COP.1.1/DESMAC	10.1.5, d-h

	JCOP-SFRs	Usage by TOE / Not used	Ref
		• FCS_COP.1.1/SHA-1 • FCS_COP.1.1/SHA-256 Used to implement FCS_COP.1.1/RSACipher: • FCS_COP.1.1/RSACipher	
6.1.2.6.	FDP_RIP.1/ABORT	Not used	-
6.1.2.7.	FDP_RIP.1/APDU	Not used	-
6.1.2.8.	FDP_RIP.1/bArray	Not used	-
6.1.2.9.	FDP_RIP.1/KEYS	Used to implement FDP_RIP.1	10.1.6, a
6.1.2.10.	FDP_RIP.1/TRANSIENT	Not used	-
6.1.2.11.	FDP_ROL.1/FIREWALL	Not used	-
6.1.3.	Card Security Management		
6.1.3.1.	FAU_ARP.1	Used to implement FPT_FLS.1 and FPT_PHP.1	10.1.6, e
6.1.3.2.	FDP_SDI.2	Used to implement FDP_SDI.2/Persistent and FDP_SDI.2/DTBS	10.1.6, b
6.1.3.3.	FPR_UNO.1	Not used	-
6.1.3.4.	FPT_FLS.1	Used to implement FPT_FLS.1 and FPT_TST.1	10.1.6,d, e
6.1.3.5.	FPT_TDC.1	Not used	-
6.1.4.	Aid Management		
6.1.4.1.	FIA_ATD.1/AID	Not used	-
6.1.4.2.	FIA_UID.2/AID	Not used	-
6.1.4.3.	FIA_USB.1/AID	Not used	-
6.1.4.4.	FMT_MTD.1/JCRE	Not used	-
6.1.4.5.	FMT_MTD.3/JCRE	Not used	-
6.1.5.	INSTG Security Functional Requirements		
6.1.5.1.	FDP_ITC.2/Installer	Not used	-
6.1.5.2.	FMT_SMR.1/Installer	Not used	-
6.1.5.3.	FPT_FLS.1/Installer	Not used	-
6.1.5.4.	FPT_RCV.3/Installer	Not used	-
6.1.6.	ADELG Security Functional Requirements		
6.1.6.1.	FDP_ACC.2/ADEL	Not used	-
6.1.6.2.	FDP_ACF.1/ADEL	Not used	-
6.1.6.3.	FDP_RIP.1/ADEL	Not used	-
6.1.6.4.	FMT_MSA.1/ADEL	Not used	-
6.1.6.5.	FMT_MSA.3/ADEL	Not used	-
6.1.6.6.	FMT_SMF.1/ADEL	Not used	-
6.1.6.7.	FMT_SMR.1/ADEL	Not used	-
6.1.6.8.	FPT_FLS.1/ADEL	Not used	-
6.1.7.	RMIG Security Functional Requirements		
6.1.7.1.	FDP_ACC.2/JCRMI	Not used	-
6.1.7.2.	FDP_ACF.1/JCRMI	Not used	-
6.1.8.	ODELG Security Functional Requirements		
6.1.8.1.	FDP_RIP.1/ODEL	Not used	-
6.1.8.2.	FPT_FLS.1/ODEL	Not used	-
6.1.9.	CARG Security Functional Requirements		
6.1.9.1.	FCO_NRO.2/CM	Not used	-
6.1.9.2.	FDP_IFC.2/CM	Not used	-
6.1.9.3.	FDP_IFF.1/CM	Not used	-
6.1.9.4.	FDP_UIT.1/CM	Not used	-
6.1.9.5.	FIA_UID.1/CM	Not used	-
6.1.9.6.	FMT_MSA.1/CM	Not used	
6.1.9.7.	FMT_MSA.3/CM	Not used	

	JCOP-SFRs	Usage by TOE / Not used	Ref
6.1.9.8.	FMT_SMF.1/CM	Not used	
6.1.9.9.	FMT_SMR.1/CM	Not used	
6.1.9.10.	FTP_ITC.1/CM	Not used	
6.1.10.	EMG Security Functional Requirements		
6.1.10.1.	FDP_ACC.1/EXT_MEM	Not used	-
6.1.10.2.	FDP_ACF.1/EXT_MEM	Not used	-
6.1.10.3.	FMT_MSA.1/EXT_MEM	Not used	-
6.1.10.4.	FMT_MSA.3/EXT_MEM	Not used	-
6.1.10.5.	FMT_SMF.1/EXT_MEM	Not used	-
6.1.11.	Further Functional Requirements		
6.1.12.	SCPG Security Functional Requirements		
6.1.12.1.	FPT_FLS.1/SCP	Not used	-
6.1.12.2.	FRU_FLT.2/SCP	Not used	-
6.1.12.3.	FPT_PHP.3/SCP	Used to implement FPT_PHP.3	10.1.6, f
6.1.12.4.	FDP_ACC.1/SCP	Not used	-
6.1.12.5.	FDP_ACF.1/SCP	Not used	-
6.1.12.6.	FMT_MSA.3/SCP	Not used	-
6.1.13.	Lifecycle Security Functional Requirements		
6.1.13.1.	FDP_ACC.1/LifeCycle	Not used	-
6.1.13.2.	FDP_ACF.1/LifeCycle	Not used	-
6.1.13.3.	FMT_MSA.1/LifeCycle	Not used	-
6.1.13.4.	FMT_MSA.3/LifeCycle	Not used	-
6.1.14.	Further Functional Requirements		
6.1.14.1.	FIA_AFL.1/PIN	Used to implement FIA_AFL.1/PIN and FIA_AFL.1/PUK	10.1.1
6.1.14.2.	FTP_ITC.1/LifeCycle	Not used	-
6.1.14.3.	FAU_SAS.1/SCP	Not used	-
6.1.14.4.	FCS_RNG.1	Used to implement FCS_CKM.1	10.1.5, a, b
6.1.14.5.	FPT_EMSEC.1	Used to implement FPT_EMS.1	10.1.6,c
6.1.15.	Functional Requirements for the Secure Box		
6.1.15.1.	FDP_ACC.2/SecureBox	Not used	-
6.1.15.2.	FDP_ACF.1/SecureBox	Not used	-
6.1.15.3.	FMT_MSA.3/SecureBox	Not used	-
6.1.15.4.	FMT_MSA.1/SecureBox	Not used	-
6.1.15.5.	FMT_SMF.1/SecureBox	Not used	-

11.2. Security assurance requirements of the composite evaluation

Table 12: JCOP SAR

Assurance class	Assurance component JCOP platform	Compare	Assurance component Composite ST
Development	ADV_ARC.1	=	ADV_ARC.1
	ADV_FSP.5	⊃	ADV_FSP.4
	ADV_IMP.1	=	ADV_IMP.1
	ADV_TDS.4	⊃	ADV_TDS.3
	ADV_INT.2	⊃	-
Guidance documents	AGD_OPE.1	=	AGD_OPE.1
	AGD_PRE.1	=	AGD_PRE.1
Life-cycle support	ALC_CMC.4	=	ALC_CMC.4
	ALC_CMS.5	⊃	ALC_CMS.4

Assurance class	Assurance component JCOP platform	Compare	Assurance component Composite ST
	ALC_DEL.1	=	ALC_DEL.1
	ALC_DVS.2	=	ALC_DVS.2
	ALC_LCD.1	=	ALC_LCD.1
	ALC_TAT.2	⊃	ALC_TAT.1
Security Target evaluation	ASE_CCL.1	=	ASE_CCL.1
	ASE_ ECD.1	=	ASE_ ECD.1
	ASE_INT.1	=	ASE_INT.1
	ASE_OBJ.2	=	ASE_OBJ.2
	ASE_REQ.2	=	ASE_REQ.2
	ASE_SPD.1	=	ASE_SPD.1
	ASE_TSS.1	=	ASE_TSS.1
Tests	ATE_COV.2	=	ATE_COV.2
	ATE_DPT.3	⊃	ATE_DPT.1
	ATE_FUN.1	=	ATE_FUN.1
	ATE_IND.2	=	ATE_IND.2
Vulnerability assessment	AVA_VAN.5	=	AVA_VAN.5

As shown in the table above, the security assurance requirements of the composite evaluation represent a subset of the SARs of the underlying platform.

11.3. Compatibility between the Composite Security Target and the Platform Security Target

The following mapping demonstrates the compatibility between the Composite Security Target (the document at hand) and the Platform Security Target [JCOP_ST] regarding security environments, security objectives, and security requirements. There is no conflict between security environments, security objectives, and security requirements of the Composite Security Target and the Platform Security Target.

Table 13: JCOP Definition

JCOP Definition	Pendant in [ST]	/Remarks
Security objectives		
Platform objectives concerning the ESW	Pendant in ST with similar aim	Remarks
OT.SEC_BOX_FW	-	No contradictions
OT.SID	-	No contradictions
OT.FIREWALL	-	No contradictions
OT.GLOBAL_ARRAYS_CONFID	-	No contradictions
OT.GLOBAL_ARRAYS_INTEG	-	No contradictions
OT.NATIVE	-	No contradictions
OT.OPERATE	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure, OT.Tamper_ID	No contradictions
OT.REALLOCATION	OT.SCD_Secrecy, OT.Sigy_SigF	No contradictions
OT.RESOURCES	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure, OT.Tamper_ID	No contradictions
OT.ALARM	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure, OT.Tamper_ID	No contradictions
OT.CIPHER	OT.Lifecycle_Security, OT.SCD_Secrecy,	No contradictions

JCOP Definition	Pendant in [ST]	/Remarks
	OT.Sig_Secure, OT.DTBS_Integrity_TOE, SVD_Corresp, OT.TOE_SSCD_Auth, OT.TOE_SVD_Exp	
OT.KEY-MNGT	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, SVD_Corresp, OT.SCD OT.TOE_SSCD_Auth, OT.TOE_SVD_Exp	No contradictions
OT.PIN-MNGT	OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE	No contradictions
OT.REMOTE	-	No contradictions
OT.TRANSACTION	OT.SCD_Secrecy, OT.Sigy_SigF	No contradictions
OT.OBJ-DELETION	-	No contradictions
OT.DELETION	-	No contradictions
OT.LOAD	-	No contradictions
OT.INSTALL	-	No contradictions
OT.CARD-MANAGEMENT	-	No contradictions
OT.SCP.IC	OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design	No contradictions
OT.SCP.RECOVERY	-	No contradictions
OT.SCP.SUPPORT	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, SVD_Corresp, OT.TOE_SSCD_Auth, OT.TOE_SVD_Exp	No contradictions
OT.EXT-MEM	-	No contradictions
OT.IDENTIFICATION	-	No contradictions
OT.RND	OT.SCD_Unique	No contradictions
OT.MF_FW	-	No contradictions
Relevant threats of the Platform ST vs. threats of the Composite-ST.		
Threats of Platform ST	According threats of comp. ST	
T.OS_OPERATE	-	No contradictions
T.SEC_BOX_BORDER	-	No contradictions
T.RND	T.SCD_Derive	No contradictions
T.CONFID-APPLI-DATA	T.SCD_Divulg, T.SCD_Derive, T.Hack_Phys, T.SigF_Misuse	No contradictions
T.CONFID-JCS-CODE	-	No contradictions
T.CONFID-JCS-DATA	-	No contradictions
T.INTEG-APPLI-CODE	-	No contradictions
T.INTEG-APPLI-CODE.LOAD	-	No contradictions
T.INTEG-APPLI-DATA	T.SCD_Divulg, T.SCD_Derive, T.Hack_Phys, T.SigF_Misuse	No contradictions
T.INTEG-APPLI-DATA.LOAD	-	No contradictions
T.INTEG-JCS-CODE	-	No contradictions
T.INTEG-JCS-DATA	-	No contradictions
T.SID.1	-	No contradictions
T.SID.2	T.Hack_Phys, T.SCD_Divulg, T.SigF_Misuse	No contradictions
T.EXE-CODE.1	-	No contradictions
T.EXE-CODE.2	-	No contradictions
T.EXE-CODE-REMOTE	-	No contradictions
T.NATIVE	-	No contradictions
T.RESOURCES	T.Hack_Phys, T.SCD_Divulg, T.SigF_Misuse	No contradictions
T.DELETION	-	No contradictions

JCOP Definition	Pendant in [ST]	/Remarks
T.INSTALL	-	No contradictions
T.OBJ-DELETION	-	No contradictions
T.PHYSICAL	T.Hack_Phys	No contradictions
Assumptions (platform) significant for Composite-ST		
Assumptions of Platform ST	Relevancy for Composite-ST	
A.APPLET	Admin guidance, ch. 4.2	Consistent
A.VERIFICATION	Admin guidance, ch. 2.2.1	Consistent
A.USE_DIAG	OE.CGA_TC_SVD_Imp, OE.HID_VAD, OE.DTBS_Protect	Consistent
A.USE_KEYS	A.CGA, A.SCA, A.CSP	Consistent
A.PPROCESS-SEC-IC	User guidance	Consistent
Platform security objectives for the environment and relevancy for the Composite ST		
OE of platform ST	Matching aspects in Composite-ST	Remarks
OE.USE_DIAG	OE.CGA_TC_SVD_Imp, OE.HID_VAD, OE.DTBS_Protect	No contradictions
OE.USE_KEYS	OE.CGA_QCert, OE.SVD_Auth, OE.DTBS_Indend, OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OE.SCD_SVD_Corresp	No contradictions
OE.PROCESS_SEC_IC	User guidance	No contradictions
OE.VERIFICATION	Admin guidance, ch.2.2.1	No contradictions
OE.APPLET	Admin guidance, ch 4.2	No contradictions
Platform organizational security policies for the environment and relevancy for the Composite ST		
OSP of platform ST	Matching aspects in Composite-ST	Remarks
OSP.VERIFICATION	Admin guidance, ch.2.2.1	No contradictions
OSP.PROCESS-TOE	OT.TOE_SSCD_Auth	No contradictions

12. Crypto-Disclaimer

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the *'Technische Richtlinie BSI TR-02102*' (https://www.bsi.bund.de).

Any Cryptographic Functionality that is marked in column 'Security Level above 100 Bits' of the following table with 'no' achieves a security level of lower than 100 Bits (in general context).

Table 14: TOE cryptographic functionality

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Authenticity	RSA signature verification (RSASSA-PKCS1-v1_5) of CV certificates using SHA-256	[PKCS#1 v2.1] (RSA),[FIPS 180-3] (SHA)	Modulus length= 2048	yes	Sec 14.3 of [EN 14890-1]

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
2	Authenticity	RSA signature verification (RSASSA-PKCS1-v1_5) of CV certificates using SHA-1	[PKCS#1 v2.1] (RSA),[FIPS 180-3] (SHA)	Modulus length= 2048	no	Sec 14.3 of [EN 14890-1]
3	Authentication	Symmetric Authentication Scheme based on TDES	Sec 8.8 of [EN 14890-1], [FIPS 46-3] (DES), [SP 800-38B] (CBC),[ISO 9797-1] (Retail MAC)	|k|=112, |challenge|=64	no	-
4	Authentication	Device authentication with privacy protection based on DH and RSA signature generation and verification (RSASSA-PKCS1-v1_5) using SHA-256	Sec 8.5 of [EN 14890-1], [PKCS#3] (DH),[PKCS#1 v2.1] (RSA),[FIPS 180-3] (SHA)	Plength= 2048,Moduluslength= 2048	yes	-
5	Authentication	Device authentication with privacy protection based on DH and RSA signature generation and verification (RSASSA-PKCS1-v1_5) using SHA-1	Sec 8.5 of [EN 14890-1], [PKCS#3] (DH),[PKCS#1 v2.1] (RSA),[FIPS 180-3] (SHA)	Plength= 2048,Moduluslength= 2048	no	-
6	Key Agreement	Key derivation using SHA-1 or SHA-256	Sec. 8.10 of [EN 14890-1], [FIPS 180-3] (SHA)	-	yes	-
7	Integrity	Triple-DES in Retail MAC Mode with padding method 2	[FIPS 46-3] (DES), MAC Algorithm 1 of [ISO9797-1]	|k|=112	no	-
8	Trusted Channel	Secure Messaging based on asymmetric authentication	Sec 9 of [EN 14890-1] additionally cf. lines 1, 4, 5, 6, 7, 8	-	no	-
9	Trusted Channel	Secure Messaging based on symmetric authentication	Sec 9 of [EN 14890-1] additionally cf. lines 1, 3, 4, 5, 6, 7, 8	-	no	-
10	Cryptographic Primitive	RSA signature generation (RSASSA-PKCS1-v1_5) using SHA-256	[PKCS#1 v2.1] (RSA),[FIPS 180-3] (SHA)	Modulus length= 2048	yes	Only after PIN-authentication
11	Cryptographic Primitive	RSA encryption and decryption (RSAES-PKCS1-v1_5)	[PKCS#1 v2.1] (RSA)	Modulus length= 2048	yes	-

Table of content