SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 –
Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD)

Security Target Lite

NSCIB-CC-0189594

Common Criteria / ISO 15408 / EAL 5+

Document Version 1.6 • 2021-06-11

Content

Version Control

Version	Date	Author	Changes to Previous Version
1.3	2021-05-05	Thomas Zeggel	ST-Lite based on ST version 1.3.
1.4	2021-05-28	Thomas Zeggel	ST-Lite based on ST version 1.4.
1.5	2021-06-02	Thomas Zeggel	ST-Lite based on ST version 1.5.
1.6	2021-06-11	Thomas Zeggel	ST-Lite based on ST version 1.6.

1 Introduction

1.1 ST/TOE Identification

Title:	SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Secure Signature Creation De-vice with key import (SSCD) – Security Target Lite
Document Version:	v1.6
Origin:	cv cryptovision GmbH
Compliant to:	Protection profiles for secure signature creation device – Part 3: Device with key import; English version EN 419211-3:2013, English translation of DIN EN 419211-3:2014-03; PP Registration: BSI-CC-PP-0075-2012-MA-01; October 2013 [PP0075]
Product identification:	SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0
TOE identification:	SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD)
Javacard OS platform:	SECORA™ ID X v1.1 (SLJ52GxAyyyzX), NSCIB-CC-0031318-CR2 [Cert_Secora]
Security controller:	IFX_CCI_000010 [ST_IC], BSI-DSZ-CC-1079-2020-v2
TOE documentation:	Administration and user guide [Guidance]

1.2 ST overview

This document contains the security target for SSCD compliant configuration of the SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0. SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 is a set of Javacard applications intended to be used exclusively on the SECORA ID-X Javacard OS platforms, which is certified according to CC EAL 5+ [Cert_Secora]. SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 as well as the SECORA ID-X operating system are provided on a smart card chip based on the Infineon IFX_CCI_000010 security controller, which is itself certified according to CC EAL 5+ [Cert_IC].

This security target is strictly conformant to the Protection Profile *Protection profiles for Secure Signature Creation Device — Part 3: Device with key import* (BSI-CC-PP-0075-2012-MA-01) [PP0075].

The main objectives of this ST are:

- to introduce TOE and the SSCD application,
- to define the scope of the TOE and its security features,
- to describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- to describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.
- to specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functionalities.

The assurance level for the TOE is CC EAL5 augmented with AVA_VAN.5 and ALC_DVS.2.

1.3 TOE overview

The TOE is a Java Card (SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0) configured to provide a secure signature creation device (SSCD) with key import for the creation of legally binding qualified electronic signatures and qualified electronic seals as defined in the eIDAS regulation [Regulation][1]. To allow secure access to the signature functionality over the contactless interface, it provides an optional PACE mechanism to build up a secure channel for the signature PIN.

1.4 TOE description

1.4.1 Overview of SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0

SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 is a set of Java Card applets for e-ID document applications built upon an underlying core library. The following *Table 1* provides an overview of the individual applications included in SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0:

Product / Application	Specification	Configuration[2]
ICAO MRTD application with Basic Access Contro (BAC) and Supplemental Access Control (SAC)	ICAO Doc 9303	ePasslet3.5/MRTD-BAC
ISO File System application	ISO 7816	ePasslet3.5/ISO-FS
ISO Driving License application with Basic Access Protection (BAP) or Supplemental Access Control (SAC)	ISO 18013	ePasslet3.5/IDL-Basic
ISO Driving License application with Extended Access Protection (EAP) or Extended Access Control (EACv1)	ISO 18013	ePasslet3.5/IDL-Extended
ICAO MRTD application with Extended Access Control (EACv1)	ICAO Doc 9303, TR03110v1.11	ePasslet3.5/MRTD-EAC
Secure Signature Creation Device application supporting PKI utilization – Device with key generation	ISO 7816, PKCS#15	ePasslet3.5/SSCD
Secure Signature Creation Device application supporting PKI utilization – Device with key import	ISO 7816, PKCS#15	ePasslet3.5/SSCD-IMP
EU Electronic Vehicle Registration application	EU Council Directive 1999/37/EC	ePasslet3.5/eVR
EU Electronic Health Insurance application	CWA 15974	ePasslet3.5/eHIC
German eID Document application	ICAO Doc 9303, TR03110v2.11, TR03127 v1.15	ePasslet3.5/GeID

---

[1] The TOE creates an electronic signature or electronic seal, respectively. The TOE meets the requirements of [PP0059], and with the key certificate created as specified in Annex I and Annex III of the eIDAS regulation [Regulation], the result of the signing process can be used as to create either a qualified electronic signature or a qualified electronic seal.

[2] The names of the configurations reflect that the TOE is based on version 3.5 of ePasslet suite.

Customizable eID Document application	ICAO Doc 09303 and TR03110v2.11	ePasslet3.5/GenID
EU Electronic Residence Permit application	TR03127 v1.15	ePasslet3.5/eRP

*Table 1: Configurations of the SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0. Please note that not all configurations are certified according to Common Criteria. **The TOE of this ST is marked in yellow.***

These configurations are based on one or more predefined applets; different configurations might use the same underlying applet.

The whole applet code resides in the Flash memory; the applets providing these different configurations are instantiated into Flash memory. Multiple configurations (and hence support for different applications) can be present at the same time by instantiating multiple applets with their distinct configurations with some restrictions detailed below. A common combination could be an ICAO MRTD applet and an SSCD applet providing a travel application with LDS data and EAC authentication together with a signature application.

Via configuration the instanciated applets can be tied to the contactless and/or the contact interface, respectively.

1.4.2 TOE definition

The TOE is a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD). The TOE consists of

- the circuitry of the chip (the integrated circuit, IC) including the contact-based interface with hardware for the contactless interface including contacts for the antenna, providing basic cryptographic functionalities,

- the platform with the Java Card operation system SECORA ID-X (SLJ52GxAyyyzX; please refer to the platform security target [ST_SECORA] for details of this designation),

- the guidance documentation of SECORA ID-X (SLJ52GxAyyyzX) according to [ST_SECORA], section 1.4.1.4.,

- SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing a secure signature creation device (SSCD) with key import[3],

- the associated Administrator and User Guidance [Guidance] in PDF format.

---

[3] Please note that there are two different options: a configuration for the contact-based interface, or cofiguration for the contactless interface with additional PACE mechanism.
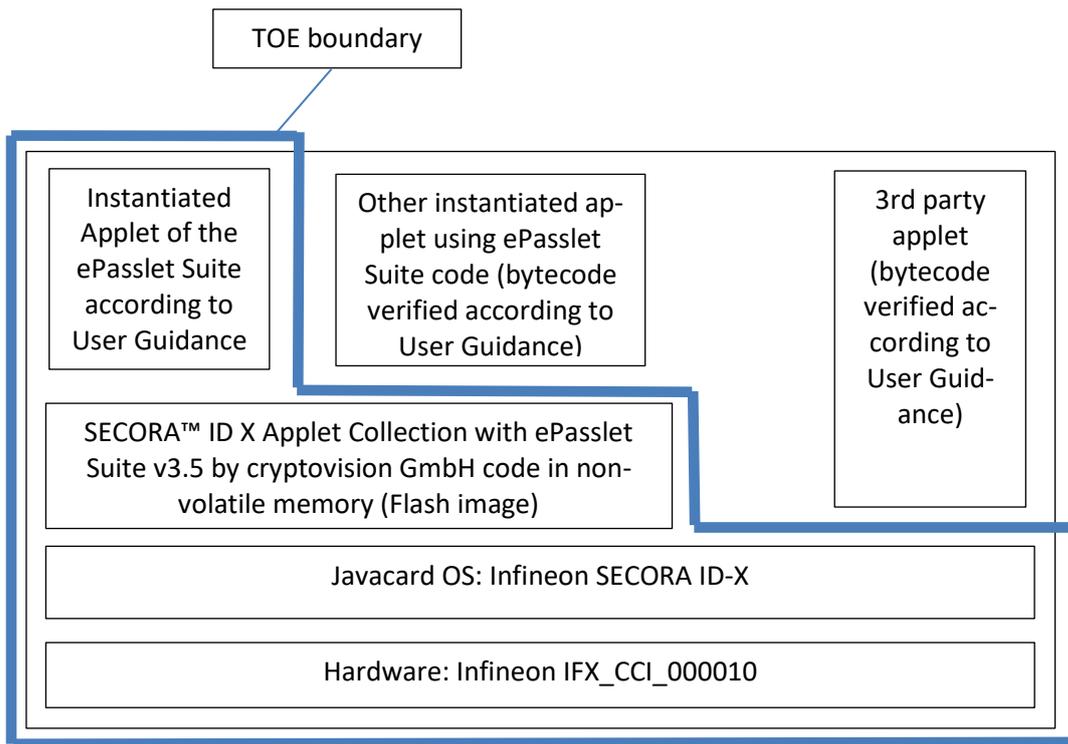
Figure 1: Schematic view on the Target of Evaluation (TOE) and its boundaries. The TOE is based on the certified hardware and Javacard OS. Besides the SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH code in non-volatile memory and the applet instantiated from it which forms the TOE of this security target, it may also contain additional applets which are not part of the TOE.

The TOE's functionality claimed by this security target is realized by the SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 in SSCD with key import configuration. The SSCD configuration with key import provides a PKCS#15 compliant file structure and a separate DF for the SSCD functionality (D.Sig). While D.Sig provides the TOE's functionality claimed by this security target, the PKCS#15 part is out of scope of the certification.

1.4.3   TOE package types and forms of delivery

The TOE can be delivered in the following forms:

- Packaged as
  - contact based modules
  - dual interface modules
  - contactless modules
- Packageless as sawn or unsawn wafer

The TOE supports Coil on Module antennas for dual interface modules [ST_SECORA].

The delivery is carried out in the following form:

TOE component	Delivered format	Delivery method	Comment
Underlying platform with SECORA™ ID X Applet Collection	Packaged as • contact based modules	Postal transfer in cages	All materials are delivered to distribution centers in cages, locked.

	dual interface modules • contactless modules Packageless as sawn or unsawn wafer		
All User Guidance documents including the SECORA ID-X guidance documentation	Personalized PDF	SecureX transfer	

1.4.4 TOE identification

Identification of the platform is performed by the procedure according to [AGD_PRE].

Once the platform is identified correctly, the correct version of the Java card layer of the TOE (SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0) can be verified as descibed in [Guidance].

1.4.5 TOE functions

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

- to import signature creation data (SCD) and, optionally, the correspondent signature verification data (SVD),
- to, optionally, receive and store certificate info,
- to switch the TOE from a non-operational state to an operational state, and
- if in an operational state, to create electronic 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)
  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) [CADES], ETSI TS 101 903 (XAdES) [XADES] and ETSI TS 101 903 (PADES) [PADES].

The TOE is prepared for the signatory's use by

- import at least one set of SCD, and
- 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 a TOE the signatory shall verify its non-operational state and change the SCD state to operational.

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

After preparation the intended legitimate user should be informed of the signatory's verification authentication data (VAD) required for use of the TOE in signing. If the VAD is a password or PIN, 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 should be destroyed (e.g. by erasing it from memory) as well as the associated certificate info, if any exists.

1.4.6   Operation of the TOE

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

- The preparation environment, 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 initialisation environment interacts further with the TOE to personalise it with the initial value of the reference authentication data (RAD).

- The signing environment where the TOE interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation application provides the data to be signed (DTBS), or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting digital signature[4].

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

The preparation environment, the signing environment and the management environment are secure and protect data exchanged with the TOE. Figure 3 in prEN 14169-1:2011 illustrates the operational environment.

The TOE stores signature creation data (SCD) and reference authentication data (RAD). The TOE may store multiple instances of SCD. In this case the TOE provides a function to identify each SCD and the SCA can provide an interface to the signer to select an SCD for use in the signature creation function of the SSCD. The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. The digital signature created by the TOE may be used to create an advanced electronic signature as defined in Article 5.1 of the [Directive][5]. 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 authorised 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 value 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.

---

[4] At a pure functional level the SSCD creates a digital signature; for an implementation of the SSCD, in that meeting the requirements of this PP and with the key certificate created as specified in the Directive, Annex I, the result of the signing process can be used as to create a qualified electronic signature.

[5] Please note that while this security target - following the according protection profile BSI-CC-PP-0075-2012-MA-01 - references the [Directive], it also incorporates the requirements of the eIDAS regulation [Regulation] and the according commission implementing regulation [Implementing].

The TOE stores signatory reference authentication data (RAD) 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 (SCA). 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.

In the case at hand the TOE is a smart card or electronic ID document. In this case a smart-card terminal may 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 electronic signature creation function of the smart card through the terminal.

The RAD verification is typically performed by direct PIN verification (VERIFY PIN command); to further protect the RAD (password or PIN) – especially in a contactless application scenario – the Password Authenticated Connection Establishmanet (PACE) protocol according to [TR03110] can be used.

1.4.7   Major security features of the TOE

The TOE provides the following TOE security functionalities:

- TSF_Access manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data[6].

- TSF_Admin manages the storage of manufacturing data, pre-personalization data and personalization data.

- TSF_Secret ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These mechanisms are mainly provided by TSF_OS.

- TSF_Crypto performs high level cryptographic operations. The implementation is mainly based on the Security Functionalities provided by TSF_OS.

- TSF_SecureMessaging realizes a secure communication channel.

- TSF_Auth realizes two authentication mechanisms: PIN verification and alternatively authentication with the PACE protocol.

- TSF_Integrity protects the integrity of internal applet data like the Access control lists.

---

[6] In the context of this security target the three categories are defined as follows: initialization comprises the preparation of the TOE based on proprietary operations of the platform with the Java Card operation system; pre-personalization comprises the configuration of the card manager and security domains as well as the generation of applet instances using Global Platform commands. Personalization is carried out afterwards using commands of the applet layer of the TOE.

- TSF_OS contains all security functionalities provided by the certified platform (IC, Javacard operation system). The cryptographic operations needed for this TOE are provided by the platform:
  - Electronic signature-generation with RSA and key sizes of 1976 up to 4096 bit with CRT and 2048 bit without CRT, or ECDSA with key sizes of 224, 256, 320, 384, 512, 521 bit.
  - Secure messaging with AES (128, 192 or 256 bit key length).
  - PACE authentication with key lengths of 224, 256, 384, 512, 521 bit (ECC).

1.4.8 TOE life cycle

This paragraph is based on the protection profile [PP0075].

1.4.8.1 General

The TOE life cycle distinguishes stages for development, production, preparation and operational use. The development and production of the TOE (cf. CC part 1 [CC_1], para.139) together constitute the development phase of the TOE.
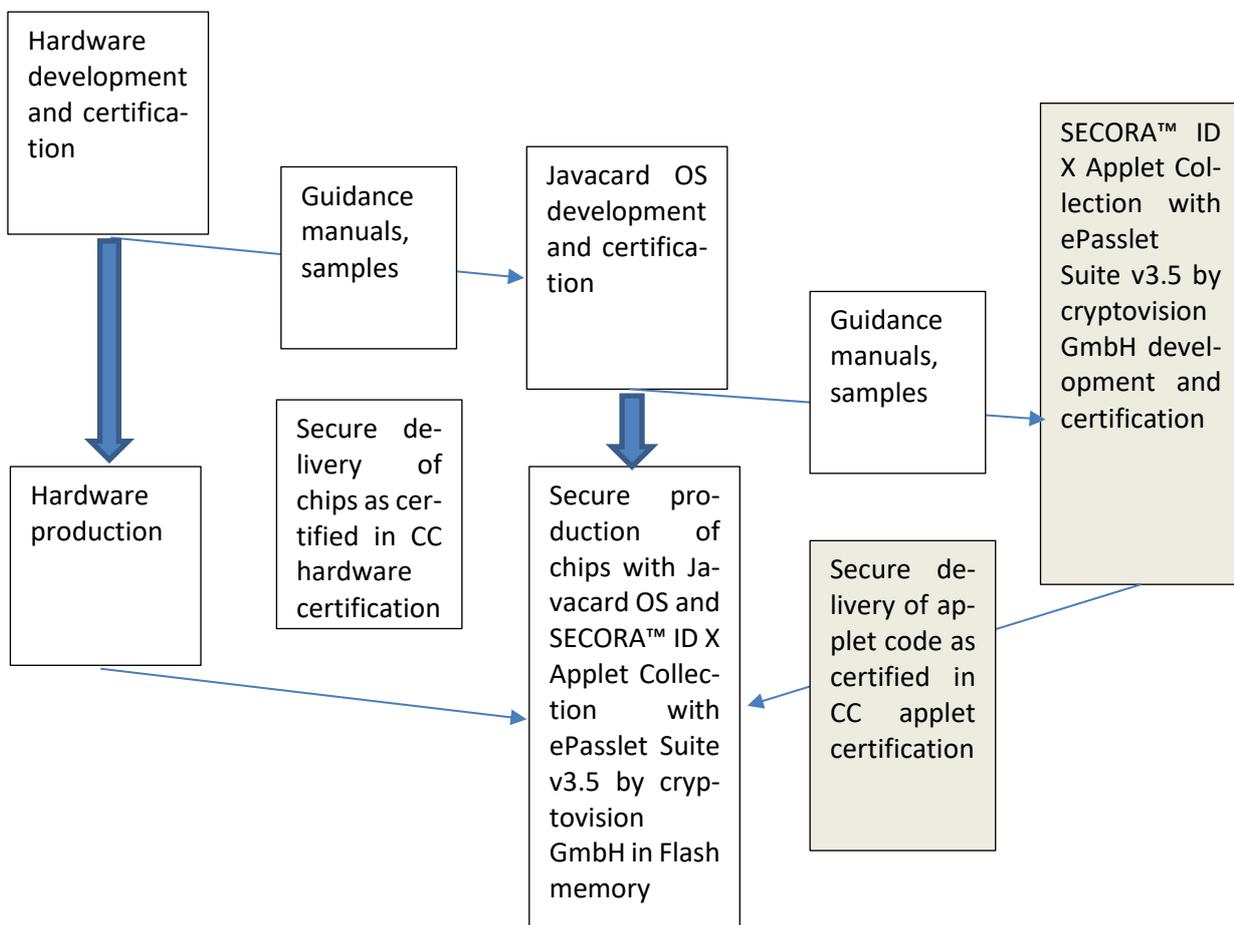
Figure 2: Overview of the development phase of the TOE, which contains development and production of the TOE. After the secure production following the process certified for the Javacard OS, the chips are delivered to the SSCD provisioning service using the delivery process already established for the OS. Gray boxes indicate the steps which are subject to evaluation according to the assurance life cycle (ALC) class.

The development phase ends with the delivery of the TOE to an SSCD-provisioning service provider or a card manufacturer. This is also the end of the scope of the certification according to Common Criteria.
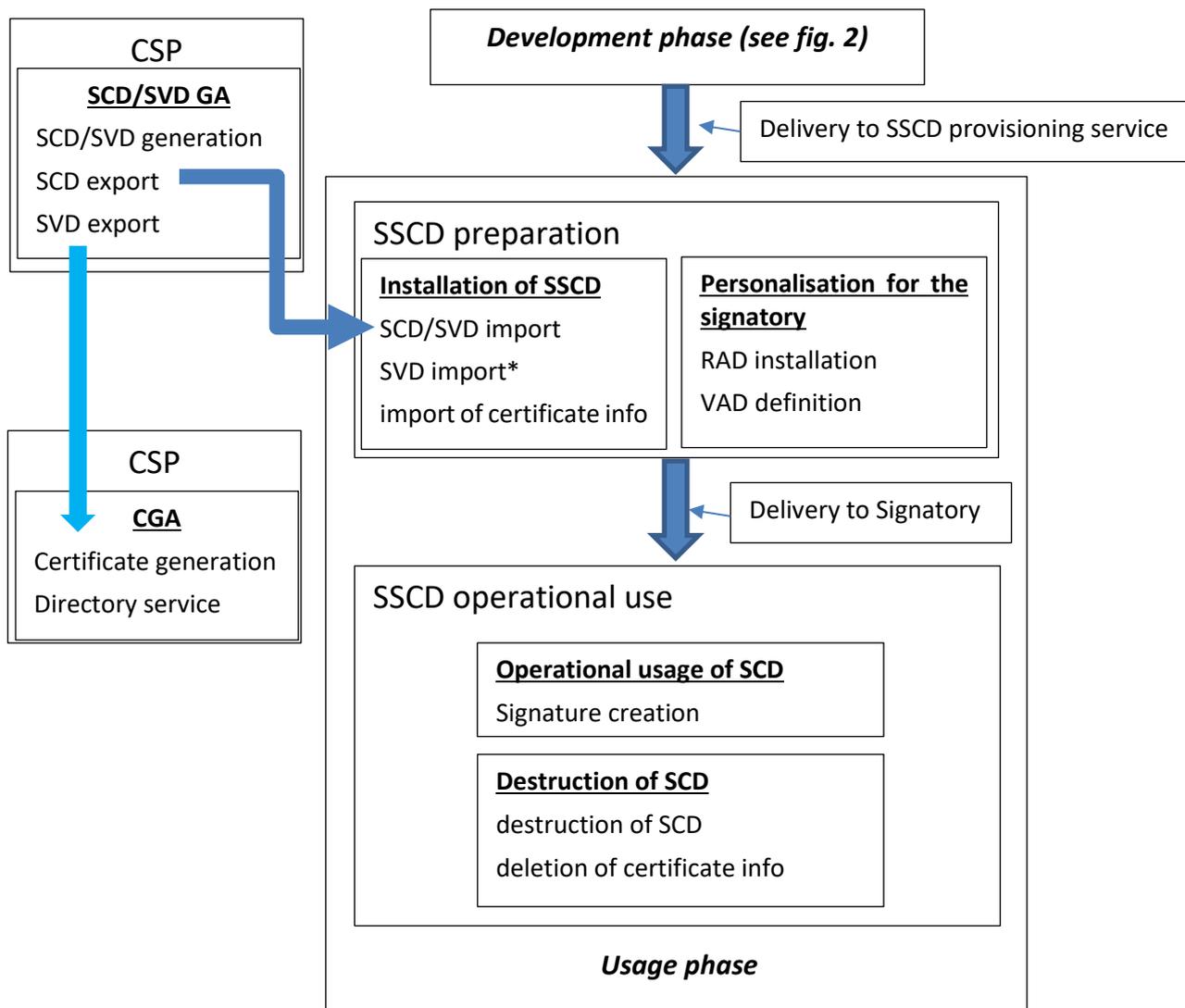
Figure 3: Example of TOE lifecycle following figure 1 of [PP0075]. Note that import of certificate info during TOE preparation and deletion of certificate info when SCD is destroyed are optional. The delivery to the SSCD provisioning service after the development phase is also the end of the scope of the certification according to Common Criteria.

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. Enabling the TOE for signing requires at least one set of SCD stored in its memory.

Figure 3 shows an example of the lifecycle where an SCD or SCD/SVD pair is imported from SSCD-provisioning service before delivery to the signatory. The lifecycle may allow import of SCD or SCD/SVD key pairs after delivery to the signatory as well.

The TOE life cycle ends when all keys stored in it have been rendered permanently unusable. Rendering a key in the SSCD unusable may include deletion of any stored corresponding certificate info. The lifecycle allows import of SCD or SCD/SVD key pairs after delivery to the signatory as well.

1.4.8.2 Preparation stage

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

- Create and configure the signature application according to AGD_PRE; this step involves applet instanciation as well as creation of the file system (card profile).[7]
- The personalisation 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.
- The initialisation 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.
- The generation of the (qualified) certificate containing among others (cf. [1], Annex II)
    a) the SVD which correspond to SCD under the control of the signatory;
    b) the name of the signatory or a pseudonym, which is to be identified as such,
    c) an indication of the beginning and end of the period of validity of the certificate.

- The 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. [Directive], article 2, Clause 9).

This security target requires the TOE to provide mechanisms for import of SCD, implementation of the SCD and personalisation. 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.

1.4.8.3 Operational use stage

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

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

---

[7] This preparation step has been added to the life cycle definition of the underlying Protection Profile and is necessary to provide the basic functionality (i.e. application and file system) for the following steps. It may be performed by the SSCD-provisioning service provider directly or by a separate entity (card manufacturer).

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 certificate5. 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 SCD stored in the TOE are destructed. This may include deletion of the corresponding certificates.

2 Conformance claims

2.1 CC conformance

This security target claims conformance[8] to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017; CCMB-2017-04-001, [CC_1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-002, [CC_2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-003, [CC_3],

as follows:

- Part 2 extended,
- Part 3 conformant,
- Package conformant to EAL5 augmented with AVA_VAN.5 and ALC_DVS.2 defined in CC part 3 [CC_3].

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017; CCMB-2017-04-004, [CC_4]

has to be taken into account.

This security target is strictly conformant to the protection profile [PP0075]. To cover the additional PACE functionality the following SFR have been added:

- FCS_COP.1/PACE
- FCS_RND.1

The evaluation of the TOE uses the result of the CC evaluation of the Infineon IFX_CCI_000010 chip claiming conformance to the PP [PP0084]. The hardware part of the composite evaluation is covered by the certification report [Cert_IC]. In addition, the evaluation of the TOE uses the result of the CC evaluation of the SECORA ID-X Javacard OS. The Javacard OS as part of the composite evaluation is covered by the certification report [Cert_Secora].

2.2 Statement of Compatibility concerning Composite Security Target

2.2.1 Assessment of the Platform TSFs

The following table lists all Security Functionalities of the underlying Platform ST and shows, which Security Functionalities of the Platform ST are relevant for this Composite ST and which are irrelevant. The first column addresses specific Security Functionality of the underlying platform, which is assigned to Security Functionalities of the Composite ST in the second column. The last column provides additional information on the correspondence if necessary.

---

[8] The referenced version of the Common Criteria has been updated to version 5.

Platform TSF-group	Correspondence in this ST	References/Remarks
SF.Firewall	No correspondence, internal Java card mechanism.	This security function provides an applet firewall. Each applet on the TOE must have been passed the Bytecode Verifier in order to ensure correct applet isolation.
SF.RIP	TSF_Secret	This security function ensures that sensitive information are made unavailable after usage by overwriting them with zeros or random values.
SF.Rollback	No correspondence, internal Java card mechanisms.	This security function implements atomicity and rollback mechanism for Global Platform management functions.
SF.SCP	TSF_SecureMessaging, TSF_Crypto (regarding Secure Messaging)	The TOE implements secure channel protocols according to [GP_v23], chapter 10. The protocols SCP02 and SCP03 are supported.
SF.CM	TSF_Access, TSF_Admin	This security function implements an access control policy for Global Platform card management functions according to [GP_v23], chapters 9.3 – 9.6.
SF.Physical	TSF_Integrity, TSF_Secret	This security function provides means to protect SFRs against physical tampering and leakage.
SF.CS	TSF_Crypto	This security function provides the cryptographic services for applets.
SF.PIN	TSF_Access	This security function implements secure PIN compare functions and integrity protection of the PIN.

Table 2: Relevant platform TSF-groups and their correspondence

2.2.2 Assessment of the Platform SFRs

The following table provides an assessment of all Platform SFRs. The Platform SFRs are listed in the order used within the security target of the platform [ST_Secora].

Platform SFR	Correspondence in this ST	References/Remarks
CoreG_LC Security Functional Requirements (chapter 7.2.1 in platform ST)		
FDP_ACC.2/FIREWALL	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
FDP_ACF.1/FIREWALL	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FDP_IFC.1/JCVM	No correspondence	Out of scope (internal Java Virtual Machine). No contradiction to this ST.
FDP_IFF.1/JCVM	No correspondence	Out of scope (internal Java Virtual Machine). No contradiction to this ST.
FDP_RIP.1/OBJECTS	No correspondence.	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_MSA.1/JCRE	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_MSA.1/JCVM	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_MSA.2/FIREWALL-JCVM	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FMT_MSA.3/FIREWALL	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FMT_MSA.3/JCVM	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_SMF.1	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_SMR.1	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FCS_CKM.1 (FCS_CKM.1.1/RSA, FCS_CKM.1.1/EC, FCS_CKM.1.1/AES, FCS_CKM.1.1/TDES)	No correspondence	Out of scope of the TOE. No contradiction to this ST.
FCS_CKM.2	No correspondence	Out of scope (managed within Java Card OS). No contradiction to this ST.
FCS_CKM.3	No correspondence	Out of scope (managed within Java Card OS). No contradiction to this ST.
FCS_CKM.4	FCS_CKM.4	Tbd. ("clearKey method")
FCS_COP.1	FCS_COP.1/SIG	The requirement FCS_COP.1/SIG of this ST targets electronic signature

Platform SFR	Correspondence in this ST	References/Remarks
(FCS_COP.1.1/JCAPI, FCS_COP.1.1/SCP, FCS_COP.1.1/SM)	FCS_COP.1/PACE	generation and is fulfilled by the platform SFR targeting RSA signature generation (FCS_COP.1.1/JCAPI with iteration /RSA-SIG and /ECDSA_SIG). FCS_COP.1/PACE uses the platform functionality required by FCS_COP.1.1/JCAPI/AES and FCS_COP.1.1/JCAPI/PACE). The according hash functions of FCS_COP.1/SIG of this ST are provided by FCS_COP.1.1/JCAPI/HASH. No contradictions to this ST.
FDP_RIP.1/ABORT	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/APDU	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/bArray	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/KEYS	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/TRANSIENT	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ROL.1/FIREWALL	No correspondence.	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FAU_ARP.1	FPT_FLS.1, FPT_PHP.3	Not directly corresponding, but platform SFR is basis of fulfillment of FPT_FLS.1 and FPT_PHP.3. Internal counter for security violations complement Java Card OS mechanisms- No contradiction to this ST.
FDP_SDI.2	FPT_FLS.1, FPT_PHP.3	Not directly corresponding, but platform SFR is basis of fulfillment of FPT_FLS.1 and FPT_PHP.3. No contradiction to this ST.
FPR_UNO.1	FPT_EMS.1	Not directly corresponding, but relevant for the fullfillment of FPT_EMS.1. No contradiction to this ST.
FPT_FLS.1	FPT_FLS.1	The fulfillment of the platform SFR is part of the basis of the fulfillment of the SFR of this ST. Internal countermeasures for detecting security violations complement Java Card OS

Platform SFR	Correspondence in this ST	References/Remarks
		mechanisms. No contradiction to this ST.
FPT_TDC.1	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_ATD.1/AID	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_UID.2/AID	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_USB.1/AID	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MTD.1/JCRE	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MTD.3/JCRE	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
INSTG Security Functional Requirements (chapter 7.2.2 in platform ST)		
This group consists of the SFRs related to the installation of the applets, which addresses security aspects outside the runtime.		
FDP_ITC.2/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMR.1/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_RCV.3/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
ADELG Security Functional Requirements (chapter 7.2.3 in platform ST)		
This group consists of the SFRs related to the deletion of applets and/or packages, enforcing the applet deletion manager (ADEL) policy on security aspects outside the runtime.		
FDP_ACC.2/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ACF.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.3/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMF.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMR.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
FPT_FLS.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
ODELG Security Functional Requirements (chapter 7.2.4 in platform ST)		
The following requirements concern the object deletion mechanism. This mechanism is triggered by the applet that owns the deleted objects by invoking a specific API method.		
FDP_RIP.1/ODEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/ODEL	FPT_FLS.1	The fulfillment of the platform SFR is part of the basis of the fulfillment of the SFR of this ST. Internal countermeasures for detecting security violations complement Java Card OS mechanisms. No contradiction to this ST.
CARG Security Functional Requirements (chapter 7.2.5 in platform ST)		
This group includes requirements for preventing the installation of packages that has not been bytecode verified, or that has been modified after bytecode verification. All SFRs of the platform are mapped to SFRs in CMGRG.		
CMGR Security Functional Requirements (chapter 7.2.6 in platform ST)		
FDP_UIT.1/CCM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ROL.1/CCM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FTP_ITC.2/CCM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/CCM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FCS_COP.1/DAP	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ACC.1/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ACF.1/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.1/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.3/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMF.1/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMR.1/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FTP_ITC.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
FCO_NRO.2/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_IFC.2/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_IFF.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.3/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMF.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_UID.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_UAU.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_UAU.4/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
SCPG Security Functional Requirements (chapter 7.2.7 in platform ST)		
The group SCPG contains the security requirements from the underlying platform. The following SFRs are taken from [ST_IC]. Their exact definition will not be repeated here. For details, please see [ST_IC].		
FPT_PHP.3	FPT_PHP.3 FPT_EMS.1	The fulfillment of the SFR in this ST is based on the platform SFR (together with additional countermeasures).
FPT_TST.1	FPT_TST.1	Self-testing is provided by the Java Card platform during initial start-up.
FCS_RNG.1	FCS_RND.1	In this ST, random numbers according to AIS20 class PTG.3 are required. The platform generates random numbers with a defined quality metric that can be used directly.

Table 3: Assessment of the platform SFRs.

2.2.3   Assessment of the Platform Objectives

The following table provides an assessment of all relevant Platform objectives.

Platform Objective	Correspondence in this ST	References/Remarks
O.SID	No correspondence	Out of scope. No contradiction to this ST.
O.FIREWALL	No correspondence	Out of scope. No contradiction to this ST.
O.GLOBAL_ARRAYS_CONFID	OT.SCD_Secrecy	No contradiction to this ST.

Platform Objective	Correspondence in this ST	References/Remarks
O.GLOBAL_ARRAYS_INTEG	OT.DTBS_Integrity_TOE	No contradiction to this ST.
O.NATIVE	No correspondence	Out of scope. No contradiction to this ST.
O.OPERATE	No correspondence	Out of scope. No contradiction to this ST.
O.REALLOCATION	No correspondence	Out of scope. No contradiction to this ST.
O.RESOURCES	No correspondence	Out of scope. No contradiction to this ST.
O.ALARM	OT.Tamper_ID OT.Tamper_Resistance	Relevant for the protection against physical tampering. No contradiction to this ST.
O.CIPHER	No correspondence	Indirectly relevant for the correct function of the TOE of this ST, but no corresponding objectives for the TOE of this ST. No contradictions.
O.KEY-MNGT	OT.SCD_Secrecy	Secure key management of the platform leads to secrecy of SCD. No contradiction to this ST.
O.PIN-MNGT	No correspondence	Out of scope. No contradiction to this ST.
O.TRANSACTION	No correspondence	Out of scope. No contradiction to this ST.
O.OBJ-DELETION	No correspondence	Out of scope. No contradiction to this ST.
O.DELETION	No correspondence	Out of scope. No contradiction to this ST.
O.LOAD	No correspondence	Out of scope. No contradiction to this ST.
O.INSTALL	No correspondence	Out of scope. No contradiction to this ST.
O.CARD-MANAGEMENT	No correspondence	Out of scope. No contradiction to this ST.
O.COMMUNICATION	No correspondence	Out of scope. No contradiction to this ST.
O.SCP.IC	OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design	The objectives are related. No contradiction to this ST.
O.SCP.RECOVERY	No correspondence	Out of scope. No contradiction to this ST.
O.SCP.SUPPORT	No correspondence	Out of scope. No contradiction to this ST.

Platform Objective	Correspondence in this ST	References/Remarks
O.SCP.RNG	OT.SCD_Secrecy: Secrecy	The TOE objective is related to the platform objective. No contradiction to this ST.

Table 4: Assessment of the platform objectives.

2.2.4 Assessment of Platform Threats

The following table provides an assessment of all relevant Platform threats.

Platform Threat	Correspondence in this ST	References/Remarks
T.CONFID-APPLI-DATA	T.SCD_Divulg, T.SCD_Derive	No contradiction to this ST.
T.CONFID-JCS-CODE	No correspondence	Out of scope. No contradiction to this ST.
T.CONFID-JCS-DATA	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-APPLI-CODE	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-APPLI-CODE.LOAD	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-APPLI-DATA	T.DTBS_Forgery, T.Sig_Forgery	No contradiction to this ST.
T.INTEG-APPLI-DATA.LOAD	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-JCS-CODE	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-JCS-DATA	No correspondence	Out of scope. No contradiction to this ST.
T.SID.1	No correspondence	Out of scope. No contradiction to this ST.
T.SID.2	No correspondence	Out of scope. No contradiction to this ST.
T.EXE-CODE.1	No correspondence	Out of scope. No contradiction to this ST.
T.EXE-CODE.2	No correspondence	Out of scope. No contradiction to this ST.
T.NATIVE	No correspondence	Out of scope. No contradiction to this ST.
T.RESOURCES	No correspondence	Out of scope. No contradiction to this ST.
T.DELETION	No correspondence	Out of scope. No contradiction to this ST.
T.INSTALL	No correspondence	Out of scope. No contradiction to this ST.

Platform Threat	Correspondence in this ST	References/Remarks
T.COMMUNICATION	No correspondence	Out of scope. No contradiction to this ST.
T.UNAUTHORIZED_CARD_MNGT	No correspondence	Out of scope. No contradiction to this ST.
T.LIFE_CYCLE	No correspondence	Out of scope. No contradiction to this ST.
T.OBJ-DELETION	No correspondence	Out of scope. No contradiction to this ST.
T.PHYSICAL	T.Hack_Phys	No contradiction to this ST.
T.RNG	No direct correspondence	RNG is necessary for optional PACE and ECDSA, but this is not directly modeled as Threat. No contradiction to this ST.

Table 5: Threats of the platform ST.

2.2.5 Assessment of Platform Organisational Security Policies

The Organisational Security Policy "OSP.VERIFICATION" focuses on the integrity of loaded applets, which is fulfilled by the TOE of this ST since the applet is loaded secured by platform security measures into the flash memory. This policy does not contradict to the policies of this ST.

2.2.6 Assessment of Platform Operational Environment

2.2.6.1 Assessment of Platform Assumptions

In the first column, the following table lists all assumptions of the Platform ST. The last column provides an explanation of relevance for the Composite TOE.

Platform Assumption	Relevance for Composite ST
A.APPLET	A.APPLET states that applets loaded post-issuance do not contain native methods. This assumption leads to appropriate directives in the user guidance [Guidance].
A.VERIFICATION	This assumption targets the applet code verification. Regarding post-issuance loading of third party applets, this assumption leads to appropriate directives in the user guidance [Guidance].

Table 6: Assumptions of the Platform ST.

2.2.6.2 Assessment of Platform Objectives for the Operational Environment

There are the following Platform Objectives for the Operational Environment that have to be considered.

Platform Objective for the Environment	Relevance for Composite ST
OE.APPLET	The platform objective for the environment states that applets loaded post-issuance do not contain

	native methods. This objective for the environment leads to appropriate directives in the user guidance [Guidance].
OE.VERIFICATION	The platform objective for the environment targets the applet code verification. This is fulfilled by the TOE of this ST; regarding third-party-code, this objective for the environment leads to appropriate directives in the user guidance [Guidance]. There it is stated that all applets loaded to the TOE have to be verified.
OE.CODE-EVIDENCE	The platform objective for the environment focusses on application code loaded pre-issuance or post-issuance. It has to be ensured that the loaded application has not been changed since the code verification. This objective for the environment leads to appropriate directives in the user guidance [Guidance].

Table 7: Platform Security Objectives and SFRs for the Operational Environment

3 Security problem definition

This chapter has been taken from [PP0075] with minor modifications.

3.1 Assets, users and threat agents

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

Assets and objects:

1. SCD: private key used to perform an electronic signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.

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

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

User and subjects acting for users:

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

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

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

Threat agents:

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

3.2 Threats

3.2.1 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.

3.2.2 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.

3.2.3 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.

3.2.4   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.

3.2.5   T.SigF_Misuse: Misuse of the signature-creation function of the TOE

An attacker misuses the signature-creation function of the TOE to create a 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.

3.2.6   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.

3.2.7   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.

3.3   Organisational Security Policies

3.3.1   P.CSP_QCert: Qualified certificate

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate ([Directive]: 2:9, 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.

3.3.2   P.QSign: Qualified electronic signatures

The signatory uses a signature-creation system to sign data with an advanced electronic signature ([Directive]: 1, 2), which is a qualified electronic signature if it is based on a valid qualified certificate ([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.

3.3.3   P.Sigy_SSCD: TOE as secure signature-creation device

The TOE meets the requirements for an SSCD laid down in [Directive], Annex III This implies the SCD is used for electronic signature creation under sole control of the signatory and the SCD can practically occur only once.

3.3.4   P.Sig_Non-Repud: Non-repudiation of signatures

The life cycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

3.4 Assumptions

3.4.1 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.

3.4.2 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.

3.4.3 A.CSP: Secure SCD/SVD management by CSP

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

4 Security Objectives

4.1 Security Objectives for the TOE

4.1.1 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.

PP application note 1: The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD import. 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.

4.1.2 OT.SCD_Auth_Imp: Authorised SCD import

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

4.1.3 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.

PP application note 2: The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD import, signature creation operation, storage and secure destruction.

4.1.4 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.

4.1.5 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.

4.1.6 OT.DTBS_Integrity_TOE: DTBS/R integrity inside the TOE

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

4.1.7 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.

4.1.8 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.

4.1.9   OT.Tamper_Resistance: Tamper resistance

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

4.2   Security Objectives for the Operational Environment

4.2.1   OE.SCD_Auth_Gen: Authorised 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.

4.2.2   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.

4.2.3   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.

4.2.4   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.

4.2.5   OE.SVD_Auth: Authenticity of the SVD

The operational environment shall ensure the authenticity 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.

4.2.6   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.

4.2.7   OE.SSCD_Prov_Service: Authentic SSCD provided by SSCD-provisioning service

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

4.2.8   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.

4.2.9   OE.DTBS_Intend: SCA sends data intended to be signed

The signatory shall use a trustworthy SCA that

(a) 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,

(b) sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,

(c) attaches the signature produced by the TOE to the data or provides it separately.

PP application note 3: The SCA should be able to support advanced electronic signatures. Currently, there exist three formats defined by ETSI recognised 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.

4.2.10   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.

4.2.11   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.

4.3   Security Objectives Rationale

4.3.1   Security Objectives Coverage

The following table shows the mapping of the Security problem definition to the security objectives.

	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OE.SCD_Auth_Gen	OESCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.CGA_Qcert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory
T.SCD_Divulg		x	x							x	x									

	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OE.SCD_Auth_Gen	OESCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.CGA_Qcert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory
T.SCD_Derive				x								x								
T.Hack_Phys			x				x	x	x											
T.SVD_Forgery													x		x					
T.SigF_Misuse	x				x	x											x	x	x	x
T.DTBS_Forgery						x												x	x	
T.Sig_Forgery				x								x			x					
P.CSP_QCert	x	x								x				x	x					
P.QSign				x	x									x				x		
P.Sigy_SSCD	x	x	x	x	x	x	x			x	x	x				x				
P.Sig_Non-Repud	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x
A.CGA														x	x					
A.SCA																			x	
A.CSP										x	x	x	x							

Table 8: Mapping of security problem definition to security objectives.

4.3.2 Security Objectives Sufficiency

4.3.2.1 Countering of threats by security objectives:

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

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

- OT.SCD_Secrecy, which assures the secrecy of the SCD during use by the TOE for signature creation.

Furthermore, generation and/or import of SCD known by an attacker is countered by OE.SCD_Auth_Gen, which ensures that only authorised 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. 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 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 SDO for data the signatory has not decided to sign, as required by the Directive [Directive], Annex III, paragraph 1, literal (c). OT.Lifecycle_Security, (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD on demand of 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 the human interface for the user authentication, OE.HID_VAD (Protection of the VAD) provides confidentiality and integrity of the VAD as needed by the authentication method employed. OE.Signatory ensures also that the signatory keep their VAD confidential.

T.DTBS_Forgery (Forgery of the DTBS/R) addresses the threat arising from modifications of the DTBS/R sent to the TOE for signing which than does not correspond to the DTBS/R corresponding to the DTBS the signatory intends to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of

- OE.DTBS_Intend, which ensures that the SCA sends only those DTBS intended to be signed by the signatory, and
- 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, 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. OE.SCD_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

4.3.2.2 Enforcement of OSPs by security objectives:

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

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- OE.SCD_Auth_Gen, which ensures that the SCD/SVD generation can be invoked by authorised users only,
- OT.SCD_Auth_Imp which ensures that authorised users only may invoke the import of the SCD,

- OE.SCD_SVD_Corresp, which requires the CSP to ensure the correspondence between the SVD and the SCD during their generation, and

- OE.CGA_QCert for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature 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 the Annex II of the Directive [Directive]. This is ensured as follows

- OE.SCD_Unique meets the paragraph 1(a) of the Directive [1], 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 [1], 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 SCD against specific attacks.

- OT.SCD_Secrecy and OT.Sig_Secure meet the paragraph 1(b) of the Directive [1], Annex III, by the requirements to ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE.

- OT.Sigy_SigF and OE.SCD_Secrecy meet the paragraph 1(c) of the Directive [1], 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 the paragraph 2 of the Directive [1], Annex III, The TOE shall not alter the DTBS/R.

Please take note, the requirements of the Directive [Directive], Annex III, 2., that the 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 them to the SSCD for signing.

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

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

- OE.SCD_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.

- OT.Sigy_SigF, which requires the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.

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

P.Sig_Non-Repud (Non-repudiation of signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures created with the TOE.

OE.SSCD_Prov_Service ensures that the signatory uses an authentic copy of the TOE, initialised and personalised for the signatory.

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

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

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

4.3.2.3   Upkeep of assumptions by security objectives:

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

A.CGA (Trustworthy 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 (CGA proves the authenticity of the SVD), which ensures the verification of the authenticity of the received SVD and 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 authorised users is addressed by OE.SCD_Auth_Gen (Authorised SCD/SVD Generation), that the generated SCD is unique and cannot be derived by the SVD is addressed by OE.SCD_Unique (Uniqueness of the signature creation data), that

SCD and SVD correspond to each other is addressed by OE.SCD_SVD_Corresp (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are deleted in the environment once exported to the TOE is addressed by OE.SCD_Secrecy (SCD Secrecy).

5 Extended Component Definition

5.1 Definition of the Family FPT_EMS

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

5.1.1 FPT_EMS TOE Emanation

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS TOE Emanation	—	1
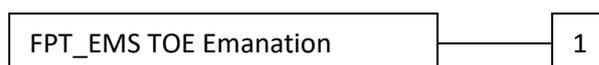
FPT_EMS.1 TOE Emanation has two constituents:

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

Management: FPT_EMS.1

> There are no management activities foreseen.

Audit: FPT_EMS.1

> There are no actions identified that shall be auditable if FAU_GEN (Security audit data generation) is included in a protection profile or security target.

FPT_EMS.1: TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1

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

FPT_EMS.1.2

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

5.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here[9].

The family "Generation of random numbers (FCS_RND)" is specified as follows.

5.2.1 FCS_RND Generation of random numbers

Family behavior

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:

FCS_RND Generation of random numbers	1
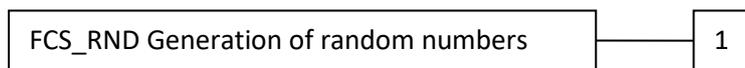
FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RND.1
	There are no management activities foreseen.
Audit:	FCS_RND.1
	There are no actions defined to be auditable.
FCS_RND.1	Quality metric for random numbers
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

---

[9] FCS_RND.1 is needed for the TOE option which uses PACE and consecutive secure messaging.

6   IT Security Requirements

6.1   General

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

Section 6.2 provides the security functional requirements.

The TOE security assurance requirements statement is given in section 6.3.

6.2   TOE Security Functional Requirements

6.2.1   Use of requirement specifications

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph C.4 of Part 1 [CC_1] of the CC. Each of these operations is used in this ST and the underlying PP.

Operations already performed in the underlying PP [PP0075] are uniformly marked by **_bold italic_** font style; for further information on details of the operation, please refer to [PP0075].

Operations performed within this security target are marked by **bold underlined** font style; further information on details of the operation is provided in foot notes.

6.2.2   Cryptographic support (FCS)

6.2.2.1   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: **overwriting the key values**[10] that meets the following: **none**[11]**.**

PP application note 4: <applied>

6.2.2.2   FCS_COP.1/SIG: 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

---

[10] [assignment: cryptographic key destruction method]

[11] [assignment: list of standards]

FCS_COP.1.1/SIG

>   The TSF shall perform ***digital signature creation*** in accordance with a specified cryptographic algorithm
>
>   - **RSA (straight and CRT variant) without internal hash calculation, with SHA-224, SHA-256, SHA-384 or SHA-512; or ECDSA without internal hash calculation, with SHA-224, SHA-256, SHA-384 or SHA-512**[12]
>
>   and specified cryptographic key sizes:
>
>   - **1976 - 2048 bit (without CRT) or 1976 - 4096 bit (with CRT); with 224, 256, 320, 384, 512 or 521 bit corresponding to the used elliptic curves P224, P256, P384, P521 and Brainpool{P224r1, P256r1, P320r1, P384r1, P512r1, P224t1, P256t1, P320t1, P384t1, P512t1}**[13]
>
>   that meet the following:
>
>   - **standard PKCS#1v2.2 [PKCS1] (RSASSA-PKCS1-v15 and RSASSA-PSS) chapter 8, and [FIPS180-4]; or standard [SEC1] (ECDSA), and [FIPS180-4], with elliptic curves defined in [FIPS186-3] and [RFC5639]** [14][15]

PP application note 5: <applied>

The following SFR is only required for variants with a contactless interface:

6.2.2.3   FCS_COP.1/PACE: PACE authentication protocol

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or
	FDP_ITC.2 Import of user data with security attributes, or
	FCS_CKM.1 Cryptographic key generation]
	FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/PACE

>   The TSF shall perform ***an authentication protocol*** in accordance with a specified cryptographic algorithm
>
>   - **PACE version 2**
>
>   and specified cryptographic key sizes:
>
>   - **224, 256, 384, 512, 521 bit (ECC); 128, 192, 256 bit (AES)**
>
>   that meet the following:
>
>   - **BSI-TR-03110 [TR03110].**

---

[12] [assignment: cryptographic algorithm]

[13] [assignment: cryptographic key sizes]

[14] [assignment: list of standards]

[15] The combination of the two cryptographic algorithms with an „or" is due to the fact that the final TOE may be configured in a way that only one of the two cryptographic algorithms is activated.

Application note: It must be underlined that the SFR FCS_COP.1/PACE SFR is only required for variants with a contactless interface. The specification of the AES can be found in [FIPS197].

Application note: The elliptic curves corresponding to the key sizes are defined in FCS_COP.1.1/SIG.

Application note: BSI-TR-03110 [TR03110] allows arbitrary combinations of ECC key sizes and AES key lengths in the PACE protocol. It should be noted that ECC key lengths smaller than the AES key length will lead to a reduced AES key space (e.g. a 224 bit entropy in a 256 bit AES key).

6.2.2.4   FCS_RND.1: Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1   The TSF shall provide a mechanism to generate random numbers that meet **the AIS20/31 Class PTG.3 quality metric**[16]**.**

Application note: This SFR was added to the standard set of SFRs to address the requirements of the PACE protocol. The random number generation is provided by the underlying SECORA ID-X platform.

Developer note: The corresponding platform SFR (FCS_RNG.1) states that the platform provides a hybrid deterministic random number generator (RNG) that fulfills the following:

- A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output.
- If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.
- The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG is started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 [AIS20] post-processing algorithm have been finished successfully or when a defect has been detected.
- The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.
- The online test procedure checks the raw random number sequence. It is triggered continuously. The online test is suitable for detecting nontolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.
- The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.

Thus the platform RNG implements AIS20/31 [AIS31] class PTG.3.

6.2.3   User data protection (FDP)

6.2.3.1   General

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

---

[16] [assignment: a defined quality metric]

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

Table 9: Security attributes and related status.

PP application note 6: <not applicable>

6.2.3.2   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.

6.2.3.3   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 user 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.

6.2.3.4   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.

6.2.3.5 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".

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

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

    FDP_IFC.1 Subset information flow control]

    FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1/SCD

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

FDP_ITC.1.2/SCD

The TSF shall ignore any security attributes associated with the ***SCD*** when imported from outside the TOE.

FDP_ITC.1.3/SCD

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**[17].

6.2.3.7   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.

PP application note 7: The component FDP_UCT.1/SCD requires the TSF to ensure the confidentiality of the SCD during import. The refinement substituting "user data" by "SCD" highlights that confidentiality of other imported user data like DTBS is not required.

6.2.3.8   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":

6.2.3.9   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.

---

[17] [assignment: additional importation control rules].

6.2.3.10 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.

PP application note 8: 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).

6.2.4   Identification and authentication (FIA)

6.2.4.1   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) Receiving DTBS[18]

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.

PP application note 9: <applied>

6.2.4.2   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) Receiving DTBS[19]

---

[18] [assignment: list of additional TSF-mediated actions]

[19] [assignment: list of additional TSF-mediated actions]

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.

PP application note 120 <applied>

6.2.4.3 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

The TSF shall detect when **an administrator configurable positive integer within 2-16**[20] unsuccessful authentication attempts occur related to *consecutive failed authentication attempts.*

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall *block RAD*.

PP application note 11: <applied>

Application note: This SFR is met by TSF_Auth. Note that TSF_Auth contains two configurable mechanisms (cf. chapter 7) based on the standard ISO7816 Verify_PIN command (for contact interface only) and on the PACE protocol.

Developer note: The blocking of the RAD after the defined number of unsuccessful authentication attempts can – depending on the configuration and the specific configuration data – be permanent or unblocked with a personal unblocking key (PUK). While the RAD should have a minimum of six digits, an optional PUK should have a minimum size of 10 digits and the usage counter of the PUK should be restricted to a maximum of 20.

6.2.5 Security management (FMT)

6.2.5.1 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.

6.2.5.2 FMT_SMF.1 Security management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1

---

[20] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

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) none[21]

PP application note 12: <applied>

6.2.5.3 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**.

6.2.5.4 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_Import_SFP** to restrict the ability to **modify** the security attributes **SCD / SVD management** to **R.Admin**.

6.2.5.5 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**.

6.2.5.6 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]

---

[21] [assignment: list of other security management functions to be provided by the TSF]

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*.

PP application note 13: <applied>

Application note: The following values of the security attribute SCD/SVD Management are secure for the TOE and the TOE lifecycle Operational:

Subject	Security Attribute SCD/SVD Management
S.Sigy	No
S. Admin	Yes

6.2.5.7   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_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.

6.2.5.8   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 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.*

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

6.2.5.9   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**.

6.2.5.10 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* the **RAD** to **R.Sigy**.

PP application note 14: No other operation besides "modify" was added as assignment in FMT_MTD.1/Signatory Managamenet of TSF data.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 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, electromagnetic radiation or timing during command execution**[22] in excess of **non-useful information**[23] enabling access to **RAD** and **SCD**.

FPT_EMS.1.2

The TSF shall ensure **any users**[24] are unable to use the following interface: **smart card circuit contacts or contactless interface**[25] to gain access to **RAD** and **SCD**.

PP application note 15: 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.

6.2.6.2 FPT_FLS.1 Failure with preservation of secure state

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

---

[22] [assignment: types of emissions]

[23] [assignment: specified limits]

[24] [assignment: type of users]

[25] [assignment: type of connection]

FPT_FLS.1.1

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

(1) Self-test according to FPT_TST fails,

(2) **none**[26]

PP application note 16: <applied>

6.2.6.3   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.

6.2.6.4   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**[27] to the **security IC**[28] by responding automatically such that the SFRs are always enforced.

PP application note 17: 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 shall 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 an failure of TOE start-up as indication of physical tampering.

6.2.6.5   FPT_TST.1 TSF testing

---

[26] [assignment: list of other types of failures in the TSF]

[27] [assignment: physical tampering scenarios]

[28] [assignment: list of TSF devices/elements]

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

FPT_TST.1.1

The TSF shall run a suite of self-tests **during initial start-up** [29] 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*.

PP application note 18: <applied>

6.2.6.6   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**.

PP application note 19: <applied>

6.3   TOE Security Assurance Requirements

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Architectural Design with domain separation and non-bypassability
	ADV_FSP.5 Complete semi-formal functional specification with additional error information

---

[29] [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: conditions under which self test should occur]]

Assurance Class	Assurance components
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.4 Semiformal modular design
	ADV_INT.2 Well-structured internals
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.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.2 Compliance with implementation standards
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.3 Testing: modular design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 10: Assurance Requirements: EAL5 augmented with AVA_VAN.5 and ALC_DVS.2.

6.4 Security Requirements Rationale

6.4.1 Security Requirement Coverage

	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.4	x		x						
FCS_COP.1/SIG	x			x					
FCS_COP.1/PACE					x				
FCS_RND.1					x				
FDP_ACC.1/ SCD_Import	x	x							
FDP_ACC.1/Signature-creation	x				x				
FDP_ACF.1/ SCD_Import	x	x							
FDP_ACF.1/Signature-creation	x				x				
FDP_ITC.1/SCD	x								
FDP_UCT.1/SCD	x		x						
FDP_RIP.1			x		x				
FDP_SDI.2/Persistent			x	x					
FDP_SDI.2/DTBS					x	x			
FIA_AFL.1					x				
FIA_UAU.1		x			x				
FIA_UID.1		x			x				
FMT_MOF.1	x				x				
FMT_MSA.1/Admin	x								
FMT_MSA.1/Signatory	x				x				
FMT_MSA.2	x				x				
FMT_MSA.3	x				x				
FMT_MSA.4	x				x				
FMT_MTD.1/Admin	x				x				
FMT_MTD.1/Signatory	x				x				
FMT_SMR.1	x				x				
FMT_SMF.1	x				x				
FPT_EMS.1			x				x		
FPT_FLS.1			x						
FPT_PHP.1								x	
FPT_PHP.3			x						x
FPT_TST.1	x		x	x					
FTP_ITC.1/SCD	x		x						

Table 11: Functional Requirement to TOE security objective mapping.

6.4.2 TOE Security Requirements Sufficiency

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

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

The secure SCD usage is ensured cryptographically according to FCS_COP.1. The SCD usage is controlled by access control FDP_ACC.1/Signature_Creation, FDP_AFC.1/Signature_Creation which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory. The FMT_SMF.1 and FMT_SMR.1 defines security management rules and functions. The test functions FPT_TST.1 provides failure detection throughout the lifecycle. The SFR FCS_CKM.4 ensures a secure SCD destruction.

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

OT.SCD_Secrecy (Secrecy of signature creation data) is provided by the security functions specified by the following SFR. FDP_UCT.1/SCD and FTP_ICT.1/SCD ensures the confidentiality for SCD import.

The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).

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

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1, which ensure the cryptographic robustness of the signature algorithms. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensures self-tests ensuring correct signature creation.

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

The FIA_UAU.1 and FIA_UID.1 that ensure that no signature creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. The SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS.

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.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. FMT_MOF.1 ensures that only the signatory can enable/disable the signature creation function. The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory.

Furthermore, the security functionality specified by FDP_RIP.1 will ensure that no attacker can get hold of the SCD (to create signatures outside the TOE) once SCD have been deleted by the legitimate signatory.

For variants with a contactless interface, FCS_COP.1/PACE and FCS_RND.1 secure the transmission of the RAD (e.g. PIN) and the set-up of a secure messaging channel. These SFRs are not required for other variants of the TOE.

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

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

6.4.3   Satisfaction of dependencies of security requirements

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

Requirement	Dependencies	Fulfilled
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1/SCD
FCS_COP.1/SIG	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FDP_ITC.1/SCD, FCS_CKM.4
FCS_COP.1/PACE	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.4 See justification No. 1 for non-satisfied dependencies
FCS_RND.1	No dependencies	n. a.
FDP_ACC.1/ SCD_Import	FDP_ACF.1	FDP_ACF.1/SCD_Import
FDP_ACC.1/ Signature-creation	FDP_ACF.1	FDP_ACF.1/Signature-Creation
FDP_ACF.1/ SCD_Import	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_ACF.1/ Signature-creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature-creation, 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]	FPT_ITC.1/SCD, FDP_ACC.1/SCD_Import
FDR_RIP.1	No dependencies	n. a.
FDP_SDI.2/Persistent	No dependencies	n. a.

Requirement	Dependencies	Fulfilled
FDP_SDI.2/DTBS	No dependencies	n. a.
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/ Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD_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/Signature_Creation, FDP_ACC.1/SCD_Import, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD_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.
FTP_ITC.1/SCD	No dependencies	n. a.

Table 12: Functional Requirements Dependencies.

Justification for non-satisfied dependencies between the SFR for TOE:

- No. 1: The PACE authentication protocol uses specific RAD (e.g. a PIN) as equivalent of a cryptographic key. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

6.4.4   Rationale for EAL 5 Augmented

The assurance level for the protection profile [PP0075] is EAL4 augmented with AVA_VAN.5. This security target enhances the security level by choosing EAL 5 augmented with AVA_VAN.5 and ALC_DVS.2 due to market demands.

Augmentation results from the selection of:

AVA_VAN.5 Advanced methodical vulnerability analysis

ALC_DVS.2 Sufficiency of security measures

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. The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Architectural Design with domain separation and non-bypassability
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: basic design

All of these dependencies are met or exceeded in the EAL5 assurance package.

The component ALC_DVS.2 has no dependencies.

7 TOE summary specification

7.1 Security Functionality

7.1.1 TSF_Access: Access rights

This security functionality manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data. Access control for initialization and pre-personalization in the preparation phase – while the actual applet is not yet present – is based on platform functionality and on the card manager of the underlying SECORA ID-X Java Card platform (SF.CM).

It allows among others the maintenance of different users (Administrator, Signatory). Access is granted (or denied) in accordance to access rights that depend on appropriate identification and authentication mechanisms.

TSF_Access covers the following SFRs:

- FDP_ACC.1.1/ SCD_Import requires that the TSF shall enforce the SCD_Import_SFP on subjects: S.User, objects: SCD, and operations: import of SCD. Access to these operations is realized by TSF_Access (while user authentication is performed by TSF_Auth).

- FDP_ACC.1.1/Signature-creation requires that the TSF shall enforce the Signature Creation SFP on (1) subjects: S.User, (2) objects: DTBS/R, signature creation data (SCD), and (3) operations: signature-creation. Access to these operations is realized by TSF_Access (while user authentication is performed by TSF_Auth).

- FDP_ACF.1.1/SCD_Import requires that the TSF shall enforce the SCD_Import_SFP to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management". Access to these operations is realized by TSF_Access (while user authentication is performed by TSF_Auth).

- FDP_ACF.1.2/SCD_Import requires that 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. This is realized by TSF_Access and TSF_Auth.

- FDP_ACF.1.3/SCD_Import requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none. This is realized by TSF_Access and TSF_Auth.

- FDP_ACF.1.4/SCD_Import requires that the TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute "SCD / SVD management" set to "not authorized" is not allowed to import SCD. This is realized by TSF_Access and TSF_Auth.

- FDP_ACF.1.1/Signature-creation requires that 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 signature creation data (SCD) with the security attribute "SCD Operational". These rules and attributes are controlled by TSF_Access and TSF_Auth.

- FDP_ACF.1.2/Signature-creation requires that 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 signature creation data (SCD) which security attribute "SCD operational" is set to "yes". These rules and attributes are controlled by TSF_Access and TSF_Auth.

- FDP_ACF.1.3/Signature-creation requires that the TSF shall explicitly authorise access of subjects to objects. This is realized by TSF_Access and TSF_Auth.

- FDP_ACF.1.4/Signature-creation requires that 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 signature creation data (SCD) which security attribute "SCD operational" is set to "no". These rules and attributes are controlled by TSF_Access and TSF_Auth.

- FDP_ITC.1.1/SCD requires that the TSF shall enforce the SCD Import SFP when importing user data, controlled under the SFP, from outside of the TOE. This is realized by TSF_Access and TSF_Auth.

- FDP_ITC.1.2/SCD requires that the TSF shall ignore any security attributes associated with the user data SCD when imported from outside the TOE. This is realized by TSF_Access and TSF_Auth.

- FDP_ITC.1.3/SCD requires taht the TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none. This is realized by TSF_Access and TSF_Auth.

- FDP_UCT.1.1/SCD requires that the TSF shall enforce the SCD Import SFP to receive SCD in a manner protected from unauthorised disclosure. This is realized by TSF_Access and TSF_Auth.

- FDP_RIP.1.1 requires that the TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from the following objects: signature creation data (SCD). This is realized by TSF_Access.

- FIA_AFL.1.2 requires that when the defined number of unsuccessful authentication attempts has been met, the TSF shall block the reference authentication data (RAD). This is realized by TSF_Auth and TSF_Access.

- FIA_UID.1.1 requires that the TSF shall allow (1) self test according to FPT_TST.1, and (2) receiving DTBS on behalf of the user to be performed before the user is identified. This is realized by TSF_Access and TSF_Auth.

- FIA_UID.1.2 requires that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. This is realized by TSF_Access and TSF_Auth.

- FIA_UAU.1.1 requires that 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, and (3) receiving DTBS on behalf of the user to be performed before the user is authenticated. This is realized by TSF_Access, TSF_Auth and TSF_SecureMessaging.

- FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. This is realized by TSF_Access and TSF_Auth.

- FMT_MOF.1.1 requires that the TSF shall restrict the ability to enable the functions signature-creation function to R.Sigy. This is realized by TSF_Access.

- FMT_MSA.1.1/Admin requires that the TSF shall enforce the SCD_Import_SFP to restrict the ability to modify [assignment: other operations] the security attributes SCD / SVD management to R.Admin. This is realized by TSF_Access.

- FMT_MSA.1.1/Signatory requires that the TSF shall enforce the Signature Creation SFP to restrict the ability to modify the security attributes SCD operational to R.Sigy. This is realized by TSF_Access.

- FMT_MTD.1.1/Admin requires that the TSF shall restrict the ability to create the reference authentication data (RAD) to R.Admin. This is realized by TSF_Access and TSF_Auth.

- FMT_MTD.1.1/ Signatory requires that the TSF shall restrict the ability to modify [assignment: none] the reference authentication data (RAD, e.g. a PIN) to R.Sigy. This is realized by TSF_Access and TSF_Auth.

- FMT_SMR.1.1 requires that the TSF shall maintain the roles R.Admin and R.Sigy. This is realized by TSF_Access and TSF_Admin.

- FTP_ITC.1.1/SCD requires that 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. While the access is controlled by TSF_Access, the security mechanism is provided by TSF_Crypto.

- FTP_ITC.1.2/SCD requires that the TSF shall permit another trusted IT product to initiate communication via the trusted channel. While the access is controlled by TSF_Access, the security mechanism is provided by TSF_Crypto.

- FTP_ITC.1.3/SCD requires that the TSF shall initiate communication via the trusted channel for (1) Data exchange integrity according to FDP_UCT.1/SCD, and (2) none. While the access is controlled by TSF_Access, the security mechanism is provided by TSF_Crypto.

7.1.2   TSF_Admin: Administration

This Security Functionality manages the storage of manufacturing data, pre-personalization data and personalization data. This storage area is a write-only-once area and write access is subject to Manufacturer or Personalization Agent authentication. Management of manufacturing and pre-personalization data in the preparation phase – while the actual applet is not yet present – is based on platform functionality and on the card manager of the underlying SECORA ID-X Java Card platform (SF.CM). During Operational Use phase, read access is only possible after successful authentication.

TSF_Admin covers the following SFRs:

- FIA_AFL.1.1 requires that the TSF shall detect when an administrator configurable positive integer within [assignment: 1-16] unsuccessful authentication attempts occur related to consecutive failed authentication attempts. This is realized within TSF_Admin and TSF_Auth.

- FMT_SMR.1.1 requires that the TSF shall maintain the roles R.Admin and R.Sigy. This is realized by TSF_Access and TSF_Admin.

- FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. This is realized by TSF_Auth and TSF_Admin.

- FMT_SMF.1.1 requires that the TSF shall be capable of performing the following management functions: (1) Creation and modification of the reference authentication data (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. This is realized by TSF_Admin.

- FMT_MSA.3.1 requires that the TSF shall enforce the SCD_Import_SFP, and Signature Creation SFP to provide restrictive default values for security attributes that are used to enforce the SFP. This is realized by TSF_Admin.

- FMT_MSA.3.2 requires that the TSF shall allow the R.Admin to specify alternative initial values to override the default values when an object or information is created. This is realized by TSF_Admin.

- FMT_MSA.4.1 requires that 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. This is realized by TSF_Admin and TSF_Crypto.

7.1.3 TSF_Secret: Secret key management

This Security Functionality ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These functions make use of SF.CryptoKey of the underlying SECORA ID-X Java Card OS.

TSF_Secret covers the following SFRs:

- FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method, i.e. overwriting the key value. This is realized by TSF_Secret (also using TSF_OS).

7.1.4 TSF_Crypto: Cryptographic operations

This Security Functionality performs high level cryptographic operations. The implementation is based on the Security Functionalities provided by TSF_OS.

TSF_Crypto covers the following SFRs:

- FCS_COP.1/PACE requires that for variants with a contactless interface the TOE must provide the PACE authentication protocol with AES. This is covered by TSF_Crypto which itself uses the crypto-graphic mechanisms realized by TSF_OS.

- FCS_COP.1.1/SIG requires that the TSF shall perform electronic signature-generation in accordance with specified cryptographic signature generation algorithms and specified cryptographic key sizes. This is covered by TSF_Crypto which itself uses the cryptographic mechanisms realized by TSF_OS.

- FTP_ITC.1.1/SCD requires that the TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and pro-vides assured identification of its end points and protection of the channel data from modification or disclosure. While the access is controlled by TSF_Access, the security mechanism is provided by TSF_Crypto.

- FTP_ITC.1.2/SCD requires that the TSF shall permit another trusted IT product to initiate communi-cation via the trusted channel. While the access is controlled by TSF_Access, the security mecha-nism is provided by TSF_Crypto.

- FTP_ITC.1.3/SCD requires that the TSF shall initiate communication via the trusted channel for (1) Data exchange integrity according to FDP_UCT.1/SCD, and (2) none. While the access is controlled by TSF_Access, the security mechanism is provided by TSF_Crypto.

- FMT_MSA.4.1 requires that the TSF shall use the following rules to set the value of security attrib-utes: (1) 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; and (2) if S.Admin imports SCD while S.Sigy is currently authenticated, the security attribute "SCD oper-ational" of the SCD shall be set to "yes" as a single operation. This is realized by TSF_Admin and TSF_Crypto, where TSF_Crypto implements the import.

7.1.5 TSF_ SecureMessaging: Secure Messaging

This Security Functionality realizes a secure communication channel after successful authentication.

TSF_SecureMessaging covers the following SFRs:

- FIA_UAU.1.1 requires that 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, and (3) receiving DTBS on behalf of the user to be performed before the user is authenticated. This is realized by TSF_SecureMessaging, TSF_Access and TSF_Auth.

7.1.6 TSF_Auth: Authentication protocols

This security function realizes the following two configurable mechanisms based on the standard ISO7816 Verify_PIN command (for contact interface only) and on the PACE protocol:

- **TSF_Auth_VERIFY_PIN**

  TSF_Auth_PIN performs the VERIFY PIN (RAD) authentication mechanism.

- **TSF_Auth_PACE**

  TSF_Auth_PACE provides an additional authentication mechanism based on the PACE protocol [TR03110]. It is used for secure PIN entry especially over contactless interface. To prevent denial of service attacks on the PACE PIN (that could be performed unnoticed via contactless interface), the suspend mode as defined in TR03110 [TR03110] is used. After two consecutive unsuccessful PIN verification attempts the PIN will be suspended and can only be verified after successful verification of an additional PIN (e.g. Card Access Number, CAN).

  Note that TSF_Auth contains two configurable mechanisms (cf. chapter 7) based on the standard ISO7816 Verify_PIN command (for contact interface only) and on the PACE protocol.

The above two authentication mechanisms cover the following SFRs:

- FCS_COP.1/PACE requires that for variants with the contactless interface the TOE must provide the PACE authentication protocol.

- FDP_ACC.1.1/ SCD_Import requires that the TSF shall enforce the SCD_Import_SFP on subjects: S.User, objects: SCD, and operations: import of SCD. Access to these operations is realized by TSF_Access and TSF_Auth.

- FDP_ACF.1.1/SCD_Import requires that the TSF shall enforce the SCD_Import_SFP to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management". Access to these operations is realized by TSF_Access and TSF_Auth.

- FDP_ACF.1.2/SCD_Import requires that 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. This is realized by TSF_Access and TSF_Auth.

- FDP_ACF.1.3/SCD_Import requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none. This is realized by TSF_Access and TSF_Auth.

- FDP_ACF.1.4/SCD_Import requires that the TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute "SCD / SVD management" set to "not authorized" is not allowed to import SCD. This is realized by TSF_Access and TSF_Auth.

- FDP_ACC.1.1/Signature-creation requires that the TSF shall enforce the Signature Creation SFP on (1) subjects: S.User, (2) objects: DTBS/R, signature creation data (SCD), and (3) operations: signature-creation. This is realized by TSF_Auth and TSF_Access.

- FDP_ACF.1.1/Signature-creation requires that 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 signature creation data (SCD) with the security attribute "SCD Operational". This is realized by TSF_Auth and TSF_Access.

- FDP_ACF.1.2/Signature-creation requires that 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 signature creation data (SCD) which security attribute "SCD operational" is set to "yes". This is realized by TSF_Auth and TSF_Access.

- FDP_ACF.1.3/Signature-creation requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none. This is realized by TSF_Auth and TSF_Access.

- FDP_ACF.1.4/Signature-creation requires that 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 signature creation data (SCD) which security attribute "SCD operational" is set to "no". This is realized by TSF_Auth and TSF_Access.

- FDP_ITC.1.1/SCD requires that the TSF shall enforce the SCD Import SFP when importing user data, controlled under the SFP, from outside of the TOE. This is realized by TSF_Access and TSF_Auth.

- FDP_ITC.1.2/SCD requires that the TSF shall ignore any security attributes associated with the user data SCD when imported from outside the TOE. This is realized by TSF_Access and TSF_Auth.

- FDP_ITC.1.3/SCD requires taht the TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none. This is realized by TSF_Access and TSF_Auth.

- FDP_UCT.1.1/SCD requires that the TSF shall enforce the SCD Import SFP to receive SCD in a manner protected from unauthorised disclosure. This is realized by TSF_Access and TSF_Auth.

- FIA_UID.1.1 requires that the TSF shall allow (1) self test according to FPT_TST.1, and (2) receiving DTBS on behalf of the user to be performed before the user is identified. This is realized by TSF_Auth and TSF_Access.

- FIA_UID.1.2 requires that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. This is realized by TSF_Auth and TSF_Access.

- FIA_UAU.1.1 requires that 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, and (3) receiving DTBS on behalf of the user to be performed before the user is authenticated. This is realized by TSF_Auth, TSF_Access and TSF_SecureMessaging.

- FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. This is realized by TSF_Auth and TSF_Access.

- FIA_AFL.1.1 requires that the TSF shall detect when an administrator configurable positive integer within [assignment: 1-16] unsuccessful authentication attempts occur related to consecutive failed authentication attempts. This is realied by TSF_Admin and TSF_Auth.

- FIA_AFL.1.2 requires that when the defined number of unsuccessful authentication attempts has been met, the TSF shall block the reference authentication data (RAD). This is realized by TSF_Auth and TSF_Access.

- FMT_SMR.1.1 requires that the TSF shall maintain the roles R.Admin and R.Sigy. This is realized by TSF_Access and TSF_Admin.

- FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. This is realized by TSF_Auth and TSF_Admin.

- FMT_MSA.2.1 requires that the TSF shall ensure that only secure values are accepted for SCD / SVD Management and SCD operational. This is realized by TSF_Auth.

- FMT_MTD.1.1/Admin requires that the TSF shall restrict the ability to create the reference authentication data (RAD) to R.Admin. This is realized by TSF_Auth and TSF_Access.

- FMT_MTD.1.1/ Signatory requires that the TSF shall restrict the ability to modify [assignment: none] the reference authentication data (RAD, e.g. a PIN) to R.Sigy. This is realized by TSF_Auth and TSF_Access.

7.1.7 TSF_Integrity: Integrity protection

This Security Functionality protects the integrity of internal applet data like the Access control lists.

TSF_Integrity covers the following SFRs:

- FDP_SDI.2.1/Persistent requires that 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. This is realized by TSF_Integrity and TSF_OS.

- FDP_SDI.2.2/Persistent requires that upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data and (2) inform the S.Sigy about integrity error. This is realized by TSF_Integrity and TSF_OS.

- FDP_SDI.2.1/DTBS requires that 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. This is realized by TSF_Integrity and TSF_OS.

- FDP_SDI.2.2/DTBS requires that upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data and (2) inform the S.Sigy about integrity error. This is realized by TSF_Integrity and TSF_OS.

- FPT_PHP.1.1 requires that the TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. This is realized by TSF_Integrity and TSF_OS.

- FPT_PHP.1.2 requires that the TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. This is realized by TSF_Integrity and TSF_OS.

7.1.8 TSF_OS: Javacard OS security functions

The Javacard operation system (part of the TOE) features the following Security Functionalities. The exact description can be found in the Javacard OS security target [ST_Secora]; the realization is partly based on the security functions of the certified IC platform:

- Applet firewall (SF.Firewalll)

- Secure overwriting of data (SF.RIP)

- Atomicity and rollback mechanism for Global Platform management functions (SF.Rollback)

- Secure channel protocols (SF.SCP)

- Access control policy for Global Platform card management functions (SF.CM)

- Security measures against physical tampering and leakage (SF.Physical)

- Cryptographic services for applets (SF.CS)

- Secure PIN compare functions and integrity protection of the PIN (SF.PIN)

Since the applet layer of the TOE is based on the Javacard OS, the realization of all TOE security functionalities and thus the fulfillment of all SFRs has dependencies to TSF_OS. The following items list all SFRs where TSF_OS has an impact above this level:

- FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method. This is realized in the security functions provided by TSF_OS (and TSF_Secret).

- FCS_COP.1/PACE requires that for variants with the contactless interface the TOE must provide the PACE authentication protocol. This is realized using security functionality provided by TSF_OS.

- FCS_COP.1.1/SIG requires that the TSF shall perform electronic signature-generation in accordance with specified cryptographic signature generation algorithms and specified cryptographic key sizes. This is realized by TSF_OS.

- FCS_RND.1 requires that the TSF should provide random numbers with a defined quality metric. This is provided by TSF_OS.

- FDP_SDI.2.2/Persistent requires that upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data and (2) inform the S.Sigy about integrity error. This is realized by TSF_Integrity and TSF_OS.

- FDP_SDI.2.1/DTBS requires that 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. This is realized by TSF_Integrity and TSF_OS.

- FDP_SDI.2.2/DTBS requires that upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data and (2) inform the S.Sigy about integrity error. This is realized by TSF_Integrity and TSF_OS.

- FPT_EMS.1.1 requires that the TOE shall not variations in power consumption, electromagnetic radiation or timing during command execution in excess of non-useful information enabling access to RAD and SCD. This is mainly realized by appropriate measures in TSF_OS together with the strict following of the security implementation guidelines of the Javacard platform.

- FPT_EMS.1.2 requires that the TSF shall ensure any users are unable to use the following interface: smart card circuit contacts or contactless interface to gain access to RAD and SCD. This is mainly realized by appropriate measures in TSF_OS together with the strict following of the security implementation guidelines of the Javacard platform.

- FPT_FLS.1.1 requires that the TSF shall preserve a secure state when the following types of failures occur: (1) self-test according to FPT_TST fails, or (2) exposure to out-of-range operating conditions where therefore a malfunction could occur. This is realized by TSF_OS (together with TSF_Integrity).

- FPT_PHP.1.1 requires that the TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.

- FPT_PHP.1.2 requires that the TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.

- FPT_PHP.3.1 requires that the TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.

- FPT_TST.1.1 requires that the TSF shall run a suite of self-tests periodically during normal operation to demonstrate the correct operation of the TSF. This is realized by TSF_OS.

- FPT_TST.1.2 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF data. This is realized by TSF_OS.

- FPT_TST.1.3 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF. This is realized by TSF_OS.

7.2 TOE summary specification rationale

This summary specification shows that the TSF and assurance measures are appropriate to fulfill the TOE security requirements.

7.2.1 Mapping of TOE Security Requirements and TOE Security Functionalities

Each TOE security functional requirement is implemented by at least one security functionality. The mapping of TOE Security Requirements and TOE Security Functionalities is given in the following table. If iterations of a TOE security requirement are covered by the same TOE security functionality the mapping will appear only once. The description of the TSF is given in section 7.1.

	TSF_Access	TSF_Admin	TSF_Secret	TSF_Crypto	TSF_SecureMessaging	TSF_Auth	TSF_Integrity	TSF_OS
FCS_CKM.4			x					x
FCS_COP.1/SIG				x				x
FCS_COP.1/PACE				x		x		
FCS_RND.1								x
FDP_ACC.1/SCD_Import	x					x		
FDP_ACC.1/Signature_Creation	x					x		
FDP_ACF.1/SCD_Import	x					x		
FDP_ACF.1/Signature_Creation	x					x		
FDP_ITC.1/SCD	x					x		
FDP_UCT.1/SCD	x					x		
FDP_RIP.1	x							
FDP_SDI.2/Persistent							x	x
FDP_SDI.2/DTBS							x	x
FIA_AFL.1	x	x				x		
FIA_UAU.1	x				x	x		
FIA_UID.1	x					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		x				
FMT_MTD.1/Admin	x					x		
FMT_MTD.1/Signatory	x					x		
FMT_SMR.1	x	x				x		
FMT_SMF.1		x						

	TSF_Access	TSF_Admin	TSF_Secret	TSF_Crypto	TSF_SecureMessaging	TSF_Auth	TSF_Integrity	TSF_OS
FPT_EMS.1								x
FPT_FLS.1								x
FPT_PHP.1							x	x
FPT_PHP.3								x
FPT_TST.1								x
FTP_ITC.1/SCD	x			x				

Table 13: Mapping of TOE Security Requirements and TOE Security Functionalities.

8   References

In the following tables, the references used in this document are summarized.

Common Criteria

[CC_1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017; CCMB-2017-04-001.
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-002.
[CC_3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-003.
[CC_4]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017; CCMB-2017-04-004.

Protection Profiles

[PP0075]	Protection profiles for secure signature creation device - Part 3: Device with key import, version 1.0.2, Author: CEN / CENELEC (TC224/WG17), English version EN 419211-3:2013, Publication date: 2012-07-24, Registration: BSI-CC-PP-0075-2012-MA-01, Approved: 14 September 2013.
[PP_Javacard]	Java Card Protection Profile - Open Configuration, Version 3.0 (May 2012), Published by Oracle, Inc.
[PP0006]	Protection Profile Secure Signature-Creation Device Type 3, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0006-2002, also short SSVG-PPs or CWA14169
[PP0084]	Security IC Platform Protection Profile, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Rev 1.0, 13 January 2014.

TOE and Platform References

[ST_Secora]	Security target Infineon SECORA™ ID X v1.1 (SLJ52GxAyyyzX), Rev1.3, 22 March 2021.
[Cert_Secora]	Certification Report SECORA™ ID X v1.1 (SLJ52GxAyyyzX), Report number NSCIB-CC-0031318-CR2, 6 April 2021.
[ST_IC]	Security Target Lite BSI-DSZ-CC-1079-V2-2020 for Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware from Infineon Technologies AG
[Cert_IC]	BSI-DSZ-CC-1079-V2-2020 for Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware from Infineon Technologies AG, 16 June 2020.
[Guidance]	[Guidance] consists of three documents:

	(1) Secora ID X Applet Collection v1.0 with cryptovision ePasslet Suite v3.5 – Java Card Applet Suite providing Electronic ID Documents applications. Guidance Manual. Document Version 1.0.9, 2021-06-02. (2) Secora ID X Applet Collection v1.0 with cryptovision ePasslet Suite v3.5 – Java Card applet configuration providing a Secure Signature Creation Device application with on-chip key generation / key import - Preparation Guidance (AGD_PRE). Document Version 1.0.6, 2021-05-25. (3) Secora ID X Applet Collection v1.0 with cryptovision ePasslet Suite v3.5 – Java Card applet configuration providing a Secure Signature Creation Device application with on-chip key generation / key import - Operational Guidance (AGD_OPE). Document Version 1.0.5, 2021-05-05.
[GP_CIC]	GlobalPlatform Card Common Implementation Configuration Version 1.0, February 2014
[GP_v23]	Global Platform Card Specification v2.3
[AGD_PRE]	SECORA ID X Administration Guide, Revision 1.50, 2021-02-05.

EU regulation

[Regulation]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[Implementing]	COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

The DIRECTIVE

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

Application and Cryptography standards

[CADES]	ETSI Technical Specification 101 733, CMS Advanced Electronic Signatures (CAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp
[XADES]	ETSI Technical Specification 101 903, XML Advanced Electronic Signatures (XAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp
[PADES]	ETSI Technical Specification 102 778: PDF Advanced Electronic Signatures (PAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp
[TR03110]	Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1, Version 2.20, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[AIS20]	Anwendungshinweise und Interpretationen zum Schema (AIS); AIS 20, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
[AIS31]	Anwendungshinweise und Interpretationen zum Schema (AIS); AIS 31, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
[FIPS180-4]	Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD (SHS), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, March 2012
[FIPS186-3]	Digital Signature Standard (DSS) - FIPS PUB 186-3, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, June, 2009
[FIPS197]	Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001
[PKCS1]	PKCS #1: RSA Encryption Standard – An RSA Laboratories Technical Note Version 2.2
[RFC5639]	RFC 5639 ECC Brainpool Standard Curves & Curve Generation, March 2010; available at: http://tools.ietf.org/html/rfc5639
[TR03111]	Technical Guideline TR-03111, "Elliptic Curve Cryptography", Version 2.0, BSI, 2012-06-28.
[SEC1]	Standards for Efficient Cryptography SEC 1: Elliptic Curve Cryptography, Certicom Research, May 21, 2009, Version 2.0. http://www.secg.org/sec1-v2.pdf
[SEC2]	Standards for efficient cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research, September 20, 2000, Version 1. http://www.secg.org/collateral/sec2_final.pdf

Glossary

The following glossary lists the main abbreviations and gives terms and definitions. It includes the terms and definitions given in [PP0075], chapter 3.2.3 and 4.

Administrator	User who performs TOE initialisation, TOE personalisation, or other TOE administrative functions
Advanced electronic signature	Electronic signature which meets specific requirements in [Directive]. According to the Directive a electronic signature qualifies as an 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
Authentication	Authentication defines a procedure that verifies the identity of the communication partner. The most elegant method is based on the use of so called electronic signatures.
CA	Certification authority.
CC	Common criteria.
Certificate	Electronic signature used as electronic attestation binding an SVD to a person confirming the identity of that person as legitimate signer ([Directive]: 2.9).
Certificate info	Information associated with a SCD/SVD pair that may be stored in a secure signature creation device. 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.
	Certificate info may be combined with 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 electronic signature of the certificate
Certificate revocation list	A list of revoked certificates issued by a certificate authority
Certification service provider (CSP)	Entity that issues certificates or provides other services related to electronic signatures ([Directive]: 2.11).
CGA	Certification generation application.
CRL	See Certificate Revocation List.
Data to be signed (DTBS)	All electronic data to be signed including a user message and signature attributes

Data to be signed or its unique representation DTBS/R	Data received by a 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.
DTBS	Data to be signed.
DTBS/R	Data to be signed or its unique representation.
EAL	Evaluation assurance level.
ECC	(Elliptic Curve Cryptography) class of procedures providing an attractive alternative for the probably most popular asymmetric procedure, the RSA algorithm.
Hash function	A function which forms the fixed-size result (the hash value) from an arbitrary amount of data (which is the input). These functions are used to generate the electronic equivalent of a fingerprint. The significant factor is that it must be impossible to generate two entries which lead to the same hash value (so called collisions) or even to generate a matching message for a defined hash value.
Integrity	The test on the integrity of data is carried out by checking messages for changes during the transmission by the receiver. Common test procedures employ Hashfunctions, MACs (Message Authentication Codes) or – with additional functionality – electronic signatures.
IT	Information technology.
Javacard	A smart card with a Javacard operation system.
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.
MAC	Message Authentication Code. Algorithm that expands the message by means of a secret key by special redundant pieces of information, which are stored or transmitted together with the message. To prevent an attacker from targeted modification of the attached redundancy, requires its protection in a suitable way.
Non-repudiation	One of the objectives in the employment of digital signatures. It describes the fact that the sender of a message is prevented from denying the preparation of the message. The problem cannot be simply solved with cryptographic routines, but the entire environment needs to be considered and respective framework conditions need to be provided by pertinent laws.
Notified body	Organizational entity designated by a member state of the European Union as responsible for accreditation and algorithms and algorithm parameters ([Directive]: 1.1b and 3.4).
PP	Protection profile.
Private key	Secret key only known to the receiver of a message, which is used in asymmetric ciphers for encryption or generation of electronic signatures.
Pseudo random number	Many cryptographic mechanisms require random numbers (e.g. in key generation). The problem, however, is that it is difficult to implement true ran-

dom numbers in software. Therefore, so called pseudo-random number generators are used, which then should be initialized with a real random element (the so called *seed*).

Public key	Publicly known key in an asymmetric cipher which is used for encryption and verification of electronic signatures.
Public key infrastructure (PKI)	Combination of hardware and software components, policies, and different procedures used to manage electronic certificates.
Qualified certificate	Public key certificate that meets the requirements laid down in [Directive], Annex I and that is provided by a CSP that fulfils the requirements laid down in [Directive], Annex II.
Qualified electronic signature	advanced electronic signature that has been created with an SSCD with a key certified with a qualified certificate ([Directive]: 5.1).
RAD	Reference authentication data.
Random numbers	Many cryptographic algorithms or protocols require a random element, mostly in form of a random number, which is newly generated in each case. In these cases, the security of the procedure depends in part on the suitability of these random numbers. As the generation of real random numbers within computers still imposes a problem (a source for real random events can in fact only be gained by exact observation of physical events, which is not easy to realize for a software), so called pseudo random numbers are used instead.
Reference authentication data (RAD)	Data persistently stored by the TOE for authentication of a user as authorised for a particular role.
SCA	Signature creation application.
SCD	Signature creation data.
SCS	Signature creation system.
SDO	Signed data object.
Secure messaging	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.
Secure signature creation device (SSCD)	Personalized device that meets the requirements laid down in [Directive], Annex III by being evaluated according to a security target conforming to this ST ([Directive]: 2.5 and 2.6).
SFP	Security function policy.
SFR	Security functional requirement.
Signatory	Legitimate user of an SSCD associated with it in the certificate of the signature-verification and who is authorized by the SSCD to operate the signature-creation function ([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 ([Directive]: 2.4).
Signature creation system (SCS)	Complete system that creates an electronic signature consists of the SCA and the SSCD.
Signature verification data (SVD)	Public cryptographic key that can be used to verify an electronic signature ([Directive] 2.7).
Smart card	A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (ROM, EEPROM, Flash) memory, i.e. which can carry out its own calculations in contrast to a simple storage card. Sometimes a smart card has a numerical coprocessor (NPU) to execute public key algorithms efficiently. Smart cards have all of their functionality comprised on a single chip (in contrast to chip cards, which contain several chips wired to each other). Therefore, such a smart card is ideal for use in cryptography as it is almost impossible to manipulate its internal processes.
SSCD	Secure signature creation device.
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.
ST	Security target.
SVD	Signature verification data.
TOE	Target of evaluation.
Travel document	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel.
TSF	TOE security functionality.
User	Entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User Message	Data determined by the signatory as the correct input for signing.
VAD	See Verification authentication data.
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.
X.509	Standard for certificates, CRLs and authentication services. It is part of the X.500 standard of the ITU-T for realization of a worldwide distributed directory service realized with open system.