Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0

Security Target

About this document

Scope and purpose

This document contains the Security Target for the evaluation of the **Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0.**

Intended audience

Common Criteria evaluators, Common Criteria certification bodies, Composite product (applet) developers

Table of contents

1 Security Target Introduction (ASE_INT)

1.1 ST Reference

The title of this document is “Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0”.

Version: Rev 0.9

Publication date: 2025-06-05

Sponsor: Infineon Technologies AG, 81726 Munich, Germany

Editor: Infineon Technologies AG, 81726 Munich, Germany

1.2 TOE Reference

The name of the TOE is “Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0” interchangeably called eSign in this ST.

The TOE is a secure chip implementing an eSign. The TOE is subject to a composite certification based on the Infineon Java Card ‘SECORA™ ID v2.01 (SLJ38Gxymm1ap)’ platform, for details on the latter refer to [ST_JC_Platform].

CC certificate number of underlying Java Card OS Platform: NSCIB-2400062-01

CC certificate number of underlying HW: BSI-DSZ-CC-1169-V4-2024

1.3 TOE Identification

The TOE identification data is as shown in the following table:

Table 1 TOE identification data

Topic	Value	
TOE release date	29-April-2025 (date coded as ‘29 04 25’)	
Applet version	1.3.0.0 (build number coded as ‘01 03 00 00’)	
TOE version number	1.0	
JC OS Platform related identification data	CC Identifier of underlying hardware platform	IFX_CCI_00005D
	Embedded OS version	'01 00 02 FA 15 00 00 13 05' (CONF1) '01 00 0C FA 15 00 00 13 05' (CONF2)
	Assymetric Crypto Library (ACL) version	03.35.001
	Symetric Crypto Library (SCL) Version	02.15.000
	Hardware Support Library (HSL) Version	03.52.9708
	Hash Crypto Library (HCL) version	01.13.002
	UMSLC version	01.30.0564
	Firmware version	80.309.05.0

The TOE provides a command ‘GET DATA’ with tag 00C1 which provides the release date and the version of the product.

The underlying SECORA™ ID v2.01 (SLJ38Gxymm1ap) platform provides the APDU command "GET TOE Info" which returns the Common Criteria identifier of the platform, the OS version, the specific versions of the cryptographic and hardware support libraries.

The underlying Java Card OS supports two product confirguations, such as CONF1 (without In-Field-Update (IFU) Loader feature and CONF2 (with IFU loader feature). The SSCD delivery covers both the product confirguations and based on the customer's request, the required product configuration is chosen during the prepersonalization.

This ST covers the Java Card OS versions listed in Table 1. Any other Java Card OS version (e.g. loaded using the IFU Loader) is not in the scope of this ST.

1.4 TOE Overview

1.4.1 TOE Definition

The Target of Evaluation (TOE) addressed by this ST is a Java Card Applet "Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0" a combination of hardware and software configured to securely create, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole lifecycle as to be used in a signature creation process solely by its signatory. configured to perform key generation and signature creation operations. Applet also supports authentication mechanisms like PACE, Active Authentication, Chip Authntication and Terminal Authentication.

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

1.5 Guidance Documentation

The following guidance documentation is delivered to the customer together with the TOE.

Table 2 TOE identification data

Document name	Version	Date
SLJ38Gxymm1ap Infineon Applet Collection - eSign V1.0 Administration Guide	Rev. 1.2	2025-06-05
SLJ38Gxymm1ap Infineon Applet Collection - eSign V1.0 Extended datasheet	Rev. 1.1	2025-05-14
Additional guidance for Java Card platform with open mode: Underlying OS platform guidances as listed in section 1.4.1.4 of [ST_JC_Platform].		

1.6 TOE Description

1.6.1 Component Overview

The TOE is a DI chip with the Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0.

Figure 1 shows the TOE in terms of its components.

The two lower layers in the picture represent the smart card controller referenced by IFX_CCI_00005D together with the Firmware, Asymmetric Cryptographic Library (ACL) and a Symmetric Crypto Library (SCL). Note that these components are certified by the same CC certificate BSI-DSZ-CC-1169-V4-2024. The hardware platform provides effective protection mechanisms against fault attacks. The platform contains hardware coprocessors, which support cryptographic standards such as TDES, AES, RSA and EC. The hardware co-processor SCP has integrated measures against successful SCA.

The white color indicates optional components which are not in the scope of the security claims of this ST, in CC terminology these are non interefering with the TSF of the TOE. The eSign V1.0 applet optionally supports the Match on Card (MoC) operations. This does not interfere with the any of the claimed security features. That means, both PIN and Biometric assets maintains its own control parameters. The personalizer could configure the required verification operation either with PIN or Biometric or both. However, the Biometric operation is not part of the certification claim in the eSign v1.0 Applet.

The OS platform called "SECORA™ ID v2.01 (SLJ38Gxymm1ap)" is a Java Card OS and offers services for:

- The standard Java Card features like API, the Java Card Runtime Environment and the Java Card Virtual Machine
- Proprietary PACE API providing special countermeasures against side channel leakage.
- GP for content management
- Crypto operations (hash, EC, RSA, TDES and AES)
- Communication via the contactless interface and contact interface.
- It is certified in Common Criteria under the Certificate: NSCIB-CC-2400062-01.

The Java Card OS supports the standard open Java Card mode as well as the proprietary static mode (installation of preloaded code is possible) and the proprietary mode native (specially tailored mode for eMRTD usecase which enforces non traceablity of the TOE). Open and static modes are the two possible modes during personalization of the TOE. The TOE goes into native mode once the personalization is terminated. See [ST_JC_Platform] for more details on the supported modes in the Java Card OS.

Optionally the ISO File SystemV2 applet (here after referred as ISO-FS) can co-exists along with the eMRTD V2 applet configurations. The ISO-FS applet provides support to generate file system structures and provide functionalities and commands based on the standards [ISO7816-4], [ISO7816-8] and [ISO7816-9]. The ISO-FS applet is non-interfering with the TSFs of the TOE. No other claims of the security for the ISO-FS applet.

The eSign applet uses the services of the Java Card OS described above. It manages the various stages of the product's lifecycle once the application is onto the hardware up to its end of life. The application implements following key features:

- Generation of Asymmetric key pair for ECC and RSA algorithm
- Computation of Digital Signature using a combination of hash algorithm and digital signature algorithm
- Encipher and Decipher of Data
- Active authentication using RSA or ECDSA algorithm
- Chip authentication using ECDH algorithm
- Terminal authentication using ECDSA algorithm
- PACE with ECDH generic mapping, Chip Authentication Mapping and password types MRZ, CAN, PIN and PUK
- PACE password management feature
- Secure messaging based on 3DES and AES as per the ICAO specification

- Support for PIN and its management
- Optionally supports Match on Card with comparison of stored reference data with data from interface device

For more information on the eSign v1.0 Applet features refer to [UserGuideDataBook] and [UserGuideAdmin].

It does not implement any cryptographic primitives, as these are provided by the underlying Java Card OS. Further it manages file access control and authentication failure handling. Also the application controls the secure messaging including error handling using the Java Card OS Crypto services, which subsequently relies on the features of the underlying hardware providing high integrity and side channel protection. The claims in terms of SFRs in this ST target of Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0.

Third party applications can be installed by the customer and running on the card. Note that in this case the Java Card OS is delivered in open mode, see [ST_JC_Platform] to the customer which will be then able to load and install 3rd party applications.

The TOE user guidance comprises:

[UserGuideDataBook] and [UserGuideAdmin] which provide guidance, how to perform personalization and maintain the targeted security level during Personalisation and Operation phase. Additionally, when the TOE is delivered with Java Card open mode to load and install the third party applications, the underlying OS platform provides guidance as listed in section 1.4.1.4 of [ST_JC_Platform].

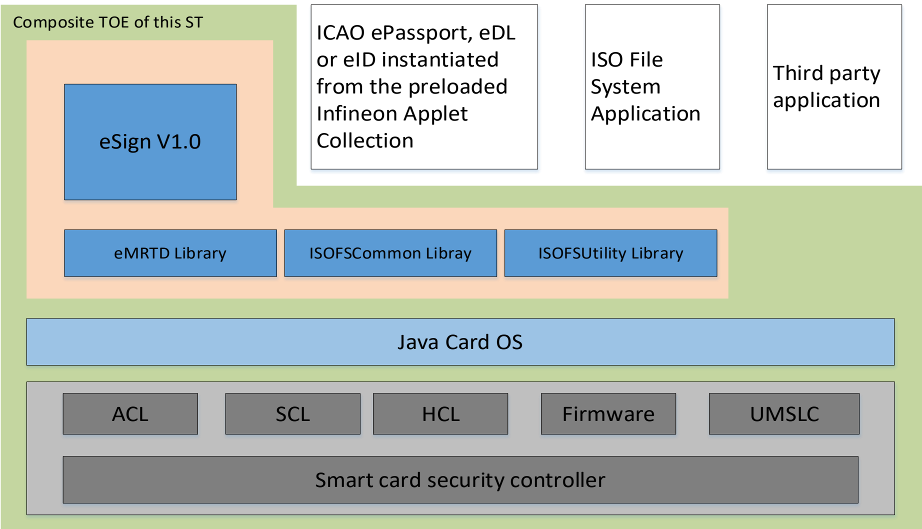

Figure 1 TOE components overview

1.6.2 Operation of the TOE

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

- The preparation environment, where it interacts with a certification service provider through a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with the SCD the TOE has generated. The initialisation environment interacts further with the TOE to personalise it with the initial value of the reference authentication data (RAD).
- The signing environment where it interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation application provides

the data to be signed (DTBS), or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting digital signature8).

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

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

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case, the TOE provides a function to identify each SCD and the SCA can provide an interface to the signer to select an SCD for use in the signature creation function of the SSCD. The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. The digital signature created by the TOE may be used to create an advanced electronic signature as defined in Article 5.1 of the directive. 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 values required. The TOE may augment the DTBS/R with signature parameters it stores and then computes a hash value over the input as needed by the kind of input and the used cryptographic algorithm.

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

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

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

A typical example of an SSCD is a smart card. In this case, a smart card terminal may be deployed that provides the required secure environment to handle a request for signatory authorisation. A signature can be obtained on a document prepared by a signature creation application component running on a personal computer connected to the card terminal. The signature creation application, after presenting the document to the user and after obtaining the authorisation PIN, initiates the digital signature creation function of the smart card through the terminal.

The RAD verification is typically performed by PIN verification using VERIFY PIN command. Optionally, PACE or Active Authentication or Chip Authentication also can be used.

1.6.3 Functionality of the TOE

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

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

The TOE provides the following functions:

a) to generate signature creation data (SCD) and the correspondent signature-verification data (SVD);

b) to export the SVD for certification;

c) to, optionally, receive and store certificate info;

d) to switch the TOE from a non-operational state to an operational state; and

e) if in an operational state, to create digital signatures for data with the following steps:

   1) select an SCD if multiple are present in the SSCD;

   2) authenticate the signatory and determine its intent to sign;

   3) receive data to be signed or a unique representation thereof (DTBS/R);

   4) apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R.

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

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

a) generating at least one SCD/SVD pair; and

b) personalising for the signatory by storing in the TOE:

   1) the signatory's reference authentication data (RAD);

   2) optionally, certificate info for at least one SCD in the TOE.

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

After preparation, the intended, legitimate user should be informed of the signatory's verification authentication data (VAD) required for use of the TOE in signing. If the VAD is a password or PIN, the means of providing this information is expected to protect the confidentiality and the integrity of the corresponding RAD.

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

1.6.4 Interfaces of the TOE

The physical interface of the TOE to the external environment is the entire surface of the IC.

The RF interface (radio frequency power and signal interface) enabling contactless communication between a PICC (proximity integration chip card, PICC) and a terminal reader/writer (proximity coupling device, terminal). The transmission protocol meets [ISO14443-3] and [ISO14443-4]. The contact based interface [ISO7816-3] also supported.

1.6.5 Package Types

The TOE package types and formats are exactly the same as for the underlying Java Card OS. The package types and formats of the Java Card OS are described in [ST_JC_Platform], section 1.4.3 and 1.4.6.

1.6.6 Lifecycle and Delivery

The [PP0059] defines the lifecycle phases for the TOE as follows:

1. Development phase
2. Preparation phase
3. Operational Use

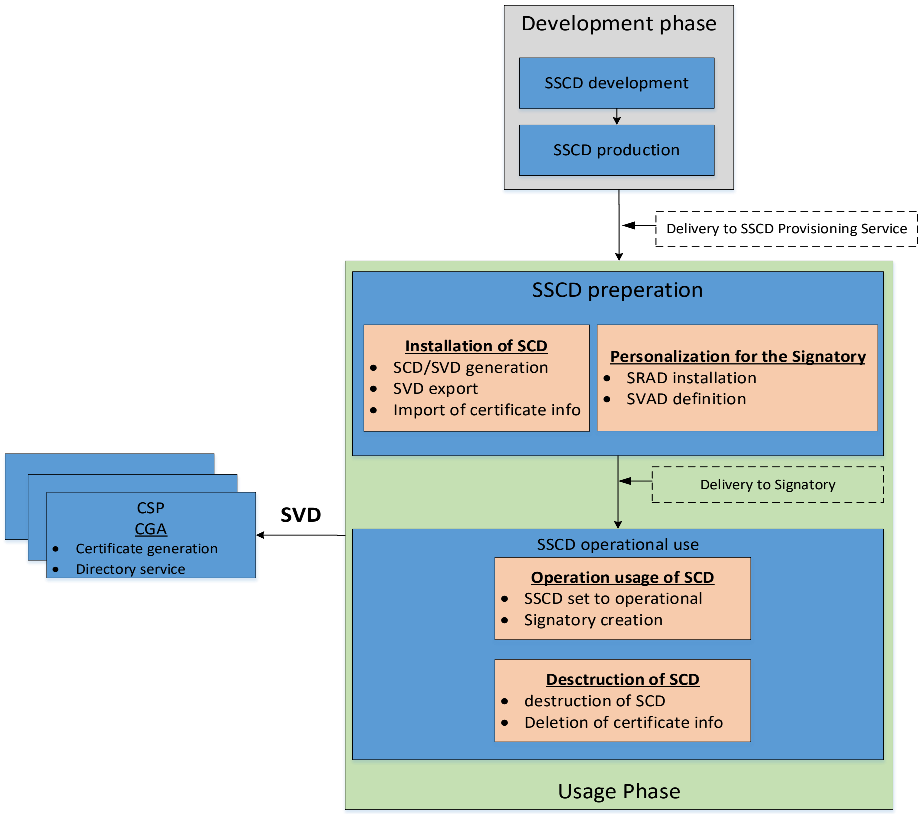

Figure 2 Lifecycle overview

1.6.6.1 Development phase

Development:

- Development of hardware and IC dedicated software (firmware)
- Development of IC embedded software

Production:

- Manufacturing of IC and IC dedicated software. As the TOE does not provide any user ROM, manufacturing of IC embedded software parts in ROM are not relevant here.
- (Prepersonalization): loading on the device of the executable Java Card OS image. Loading of the application JC package containing the TOE code.
- TOE is delivered to SSCD-provisioning service provider.

1.6.6.2 Preparation phase

An SSCD-provisioning service provider having accepted the TOE from a manufacturer prepares the TOE for use and delivers it to its legitimate user. The preparation phase ends when the legitimate user has received the TOE from the SSCD-provisioning service and any SCD it might already hold have been enabled for use in signing.

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

a) Obtain information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user of the TOE.

b) Generate a PIN and/or obtain a biometric sample of the legitimate user, store this data as RAD in the TOE and prepare information about the VAD for delivery to the legitimate user.

c) Generate a certificate for at least one SCD either by:

    1) the TOE generating an SCD/SVD pair and obtaining a certificate for the SVD exported from the TOE; or

    2) initialising security functions in the TOE for protected export of the SVD and obtaining a certificate for the SVD after receiving a protected request from the TOE.

d) Optionally, present certificate info to the SSCD.

e) Deliver the TOE and the accompanying VAD info to the legitimate user.

The SVD certification task (third item listed above) of an SSCD-provisioning service provider as specified in [PP0059] may support a centralised, pre-issuing key generation process, with at least one key generated and certified, before delivery to the legitimate user. Alternatively, or additionally, that task may support key generation by the signatory after delivery and outside the secure preparation environment. A TOE may support both key generation processes, for example with a first key generated centrally and additional keys generated by the signatory in the operational use stage.

Data required for inclusion in the SVD certificate at least includes ([Directive], Annex II)

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

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

Before initiating the actual certificate signature, the certificate generation application verifies the SVD received from the TOE by:

a) establishing the sender as genuine SSCD;

b) establishing the integrity of the SVD to be certified as sent by the originating SSCD;

c) establishing that the originating SSCD has been personalised for the legitimate user;

d) establishing correspondence between SCD and SVD; and

e) an assertion that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

The proof of correspondence between an SCD stored in the TOE and an SVD may be implicit in the security mechanisms applied by the CGA. Optionally, the TOE may support a function to provide an explicit proof of correspondence between an SCD it stores and an SVD realised by self-certification. Such a function may be performed implicitly in the SVD export function and may be invoked in the preparation environment without explicit consent of the signatory. Security requirements to protect the SVD export function and the certification data if the SVD is generated by the signatory and then exported from the SSCD to the CGA are are not part of this ST.

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

1.6.6.3 Operational use

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

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

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

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

The TOE may support functions to generate additional signing keys. If the TOE supports these functions it will support further functions to securely obtain certificates for the new keys. For an additional key the signatory may be allowed to choose the kind of certificate (qualified, or not) to obtain for the SVD of the new key. The signatory may also be allowed to choose some of the data in the certificate request for instance to use a pseudonym instead of the legal name in the certificate11). If the conditions to obtain a qualified certificate are met the new key can also be used to create advanced electronic signatures. The optional TOE functions for additional key generation and certification may require additional security functions in the TOE and an interaction with the SSCD-provisioning service provider in an environment that is secure.

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

1.6.7 Forms of delivery

The composite TOE is delivered to customers with the deliverey forms mentioned in chapter 1.6.5 via Postal

transfer in cages. All materials are delivered to distribution centers in cages, locked.

All User Guidance documents mentioned in chapter 1.5 are delivered as a personalized PDF via webservice

portal MyICP.

2 Conformance Claims (ASE_CCL)

2.1 CC Conformance Claim

This Security Target and the TOE is Common Criteria version CC:2022 revision 1 part 2 [CCPart2] extended, Common Criteria version CC:2022 revision 1 part 3 [CCPart3], part 4 [CCPart4] and part 5 [CCPart5] conformant. Also conformant to Common Criteria evaluation methods and activities [CEM2022]. [CCErrata] and [CCTrans] is taken into consideration.

2.2 PP Claim

The TOE is strictly conformant to the Protection Profile Protection profiles for Secure Signature Creation Device - Part 2: Device with key generation (BSI-CC-PP-0059-2009-MA-02) [PP0059].

2.3 Package Claim

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

2.4 Conformance Rationale

With CC:2022 several SFR changes are introduced. Due to this ST claiming conformance to CC:2022 and [PP0059], rationales are provided that these changes do not affect the conformance claim to [PP0059]:

- FCS_COP.1: for this SFR dependencies are changed in CC:2022. FCS_CKM.4 is removed and instead FCS_CKM.6 added. Further FCS_CKM.5 is added for key derivation as an alternative.
- FCS_CKM.1: for this SFR dependencies are changed in CC:2022. Additionally to FCS_CKM.2 and FCS_COP.1, one further SFR is introduced as alternative: FCS_CKM.5. This SFR targets key derivation, subsequent to FCS_CKM.1. In CC:2022 key derivation would have been part of FCS_CKM.1 and thus conformancy to [PP0059] can still be claimed. FCS_CKM.4 is removed and instead FCS_CKM.6 added. All other dependencies (i.e. FCS_RNG.1 or FCS_RBG.1) are in addition to the already existing ones, i.e. add stricter requirements.
- FCS_CKM.6 replaces FCS_CKM.4 and adds further requirements on the timing of key destruction. As an alternative dependency to FCS_CKM.1, FCS_CKM.5 (key derivation) can be used. As FCS_CKM.5 is neither used within [PP0059] nor within this ST, it has no relevance in this context.
- FMT_LIM.1 and FMT_LIM.2 in CC:2022 are slightly rephrased (i.e. removing redundancy from FMT_LIM.1) and availability and capability policy mentioned in both SFR's. The meaning though is the same as in [PP0059] and therefore conformancy can still be claimed.
- Further with CC:2022 some SAR changes were introduced. Rationales are provided that these changes do not affect the conformance claim to [PP0059]:
- ASE_CCL.1: for CC:2022 several extensions were introduced (e.g. exact conformance to PP), which add to the already existing assurance requirements. No relaxation was introduced.
- ASE_INT.1: introduction of multi-assurance in combination with PP-configuration: not relevant for [PP0059]
- ASE_REQ.2: extended for multi assurance: not relevant for [PP0059]
- AVA_VAN.5: extension about third party components introduced. No relaxation was introduced.
- ALC_TAT.1: extension with guidance on the minimum content for an implementation standards description and rules with ADV_COMP.1. No relaxation was introduced.

3 Security Problem Definition (ASE_SPD)

All assets, subjects and external entities, threats, organisational security policies and assumptions from [PP0059] section 7 “Security Problem Definition” are applicable for this TOE.

4 Security Objectives (ASE_OBJ)

Here follows a concise description of the security objectives applying to this ST followed by the security objective rationale.

4.1 Security Objectives defined in the claimed PPs

All Security Objectives provided by the TOE or by the operational environment as well as the security objectives rationale from the claimed PPs [PP0059] section 8 “Security Objectives” are applicable for this TOE.

4.2 Security Objective Rationale

The Security Objective Rationale from the claimed PP [PP0059] stays the same here.

5 Extended Components Definition (ASE_ECD)

[PP0059] respective section "Extended Components Definition" is applicable for this TOE. However, the SFRs from CC:2022 replces them. The mappings and its correspondence are shown in Table 3.

Table 3 Extended SFRs from PP0059 mapped to SFRs in CC:2022

Extended SFRs from PP	Mapping to SFRs in CC:2022	Correspondance
SFRs from [PP0059]		
FPT_EMS.1	FPT_EMS.1	Replaced and refined with SFR from CC:2022. However, the content is identical.
FPT_TST.1	FPT_TST.1	Replaced and refined with SFR from CC:2022. The SFR from CC:2022 additionally specifies the list of self-tests run by the TSF.
SFRS from CC:2022		
n.a.	FCS_RNG.1	Introduced in this ST from CC:2022.

6 Security Requirements (ASE_REQ)

6.1 TOE Security Functional Requirements

The security functional requirements (SFR) for this TOE are defined in this chapter.
This ST covers the SFRs from [PP0059] and SFRs introduced in this ST listed in Table 4 which are related to the Active Authentication mechanism supported by the TOE.

Operations already performed in the underlying PP [PP0059] are marked by underlined font style. Please refer to [PP0059] for further information on details of the operation. Operations performed within this Security Target are marked by *italic underlined* font style.

Table 4 TOE SFRs introduced in this ST

SFRs
FCS_COP.1/PACE_AUTH
FCS_COP.1/AA
FCS_COP.1/CA
FCS_COP.1/TA
FCS_RNG.1

6.1.1 About the Application Notes in this ST

Note that if an SFR has application notes as per the [PP0059] then these application notes apply and can be found in PP itself.

Some SFRs contain additional application notes to ease the understanding of the specificities of this TOE. These application notes do not come from the PPs and are prefixed with [IFX specific].

6.1.2 Class FCS: Cryptographic Support

6.1.2.1 FCS_CKM.6: Timing and event of cryptographic key destruction – Session keys

Table 5 FCS_CKM.6

FCS_CKM.6	Timing and event of 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, or FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6.1	The TSF shall destroy *cryptographic keys* when *no longer needed*.
FCS_CKM.6.2	The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method *overwriting the key values with random values* that meets the following: *none*.

FCS_CKM.6	**Timing and event of cryptographic key destruction**
[IFX specific] Application Note:	Application note 6 applied. FCS_CKM.4 from [PP0059] fulfilled using FCS_CKM.6 since FCS_CKM.4 is replaced by FCS_CKM.6 in CC:2022.

6.1.2.2 FCS_CKM.1: Cryptographic key generation

Table 6 FCS_CKM.1

FCS_CKM.1	**Cryptographic key generation**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_CKM.5 Cryptographic key derivation or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation or FCS_RNG.1 Generation of random numbers]
FCS_CKM.1.1	The TSF shall generate an *SCD/SVD* pair in accordance with a specified cryptographic key generation *Table 7 column Algorithm* and specified cryptographic key sizes *Table 7 column Key size* that meet the following: *Table 7 column Standard*.
Application Note:	PP application note 5 applied.

Table 7 Cryptographic key generation

Algorithm	**Key size**	**Standard**
RSA CRT	1024 – 4096 bits	According to [PKCS v2.2]
ECDSA	192, 224, 256, 320, 384, 512, 521 with NIST curves P192, P224, P256, P384, P521 and Brainpool curves Brainpool192r1, Brainpool224r1, Brainpool256r1, Brainpool320r1, Brainpool384r1, Brainpool512r1, Brainpool224t1, Brainpool256t1, Brainpool320t1, Brainpool384t1, Brainpool512t1	For elliptic curves according to chapters 4.3.3 and 4.3.3.2 in the appendix A4.3 in [X9.62], according to section 6.4.2 in "Generation of signature key and verification key" in [ISO14888-3], and according to appendix A.16.9 "An algorithm for generating EC keys" in [IEEE P1363] with elliptic curves defined in [FIPS186-3] and [RFC5639].

6.1.2.3 FCS_COP.1/SIG_GEN: Cryptographic operation – Signature generation

Table 8 FCS_COP.1/SIG_GEN

FCS_COP.1/SIG_GEN	**Cryptographic operation – Signature generation**
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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1/SIG_GEN	**Cryptographic operation – Signature generation**
FCS_COP.1.1/SIG_GEN	The TSF shall perform *digital signature creation* in accordance with a specified cryptographic algorithm *Table 9 column Algorithm* and cryptographic key sizes *Table 9 column Key size* that meet the following: *Table 9 column Standard*.
[IFX specific] Application Note:	Application Note 7 applied.

Table 9 Cryptographic signature generation

Algorithm	Key size	Standard
RSA signature Generation: RSASSA-PSS w/o hash and with hash in {SHA-1, SHA224, SHA256, SHA384, SHA512}}	1024 – 4096 bits	According to [PKCS v2.2]
RSA signature Generation: RSASSA-PKCS-v1_5 w/o hash and with hash in {SHA-1, SHA224, SHA256, SHA384, SHA512}	1024 – 4096 bits	According to [PKCS v2.2]
RSA signature Generation: ISO 9796-2, scheme 1 with SHA-1	1024 – 4096 bits	According to [ISO9796-2]
EC signature generation	192, 224, 256, 320, 384, 512, 521 with NIST curves P192, P224, P256, P384, P521 and Brainpool curves Brainpool192r1, Brainpool224r1, Brainpool256r1, Brainpool320r1, Brainpool384r1, Brainpool512r1, Brainpool224t1, Brainpool256t1, Brainpool320t1, Brainpool384t1, Brainpool512t1	According to [SEC1]. For elliptic curves according to chapters 4.3.3 and 4.3.3.2 in the appendix A4.3 in [X9.62], according to section 6.4.2 in “Generation of signature key and verification key” in [ISO14888-3], and according to appendix A.16.9 “An algorithm for generating EC keys” in [IEEE P1363] with elliptic curves defined in [FIPS186-3] and [RFC5639].

6.1.2.4 FCS_COP.1/PACE_AUTH: Cryptographic operation – PACE Authentication

Table 10 FCS_COP.1/PACE

FCS_COP.1/PACE_AUTH	**Cryptographic operation – PACE Authentication**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or

FCS_COP.1/PACE_AUTH	Cryptographic operation – PACE Authentication
	FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/PACE_AUTH	The TSF shall perform *authentication protocol* in accordance with a specified cryptographic algorithm *- PACE-ECDH-GM-3DES-CBC-CBC* *- PACE-ECDH-GM-AES-CBC-MAC-128* *- PACE-ECDH-GM-AES-CBC-MAC-192* *- PACE-ECDH-GM-AES-CBC-MAC-256* *- PACE-ECDH-CAM-AES-CBC-CMAC-128* *- PACE-ECDH-CAM-AES-CBC-CMAC-192* *- PACE-ECDH-CAM-AES-CBC-CMAC-256* and cryptographic key sizes *224, 256, 320, 384, 512, 521 bit (ECC); 112 bit (3DES); 128, 192, 256 bit (AES)* that meet the following: *[TR_03110_1]* and *[ICAO_9303_11].*
[IFX specific] Application Note:	Application Note 7 applied.

6.1.2.5 FCS_COP.1/AA: Cryptographic operation -Active Authentication

Table 11 FCS_COP.1/AA

FCS_COP.1/AA	Cryptographic operation – Active Authentication
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/AA	The TSF shall perform *authentication protocol* in accordance with a specified cryptographic algorithm: *RSA based Digital Signature scheme 1 with SHA1, SHA224, SHA256, SHA384 or SHA512 with RSA CRT 1024 to 2048 key length bits* *or* *ECDSA with SHA1, SHA224, SHA256, SHA384 or SHA512 and cryptographic key sizes of 192, 224, 256, 320, 384, 512 or 521 bits;* that meet the following: *[ISO9796-2]* for RSA signatures and *[ICAO_9303_11]* for ECDSA.
[IFX specific] Application Note:	Application Note 7 applied.

6.1.2.6 FCS_COP.1/CA: Cryptographic operation – Chip Authentication

Table 12 FCS_COP.1/CA

FCS_COP.1/CA	Cryptographic operation – Chip Authentication
Hierarchical to:	No other components.

FCS_COP.1/CA	Cryptographic operation – Chip Authentication
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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/CA	The TSF shall perform *authentication protocol* in accordance with a specified cryptographic algorithm *- CA-ECDH-3DES-CBC-CBC* *- CA-ECDH-AES-CBC-CMAC-128* *- CA-ECDH-AES-CBC-CMAC-192* *- CA-ECDH-AES-CBC-CMAC-256* and cryptographic key sizes *192, 224, 256, 320, 384, 512, 521 bit (ECC)* that meet the following: *[TR_03110_1]*.
[IFX specific] Application Note:	Application Note 7 applied.

6.1.2.7 FCS_COP.1/TA: Cryptographic operation – Terminal Authentication

Table 13 FCS_COP.1/TA

FCS_COP.1/TA	Cryptographic operation – Terminal Authentication
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/TA	The TSF shall perform *authentication protocol* in accordance with a specified cryptographic algorithm *- TA-ECDSA-SHA-1* *- TA-ECDSA-SHA-224* *- TA-ECDSA-SHA-256* *- TA-ECDSA-SHA-384* *- TA-ECDSA-SHA-512* and cryptographic key sizes *192, 224, 256, 320, 384, 512, 521 bit (ECC)* that meet the following: *[TR_03110_1]*.
[IFX specific] Application Note:	Application Note 7 applied.

6.1.2.8 FCS_RNG.1: Quality metric for random numbers

Table 14 FCS_RNG.1

FCS_RNG.1	**Quality metric for random numbers**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a *hybrid physical* random number generator that implements: *Random numbers generation Class PTG.3 according to [AIS31]*: (1) (PTG.3.1) 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. (2) (PTG.3.2) 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*. (3) (PTG.3.3) 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 postprocessing algorithm have been finished successfully or when a defect has been detected. (4) (PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon. (5) 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. (6) (PTG.3.6) 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.
FCS_RNG.1.2	The TSF shall provide *octets of bits* that meet: (1) (PTG.3.7) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A. (2) (PTG.3.8) The internal random numbers shall *use PTRNG of class PTG.2 as random source for the post-processing*.
[IFX specific] Application Note:	This SFR was introduced in this ST to address the PACE protocol requirement. The random number generation is provided by the underlying platform SECORA™ ID X V2.01. Refer to [ST_JC_Platform] for more details on the RNG fulfillment.

6.1.3 Class User data protection (FDP)

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

Table 15 Subjects and security attributes for access control

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorised, not authorized
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value
SVD	([PP0059] does not define security attributes for SVD)	([PP0059] does not define security attributes for SVD)

6.1.3.1 FDP_ACC.1/SCD/SVD_Generation: Subset access control

Table 16 FDP_ACC.1/SCD/SVD_Generation

FDP_ACC.1/SCD/SVD_Generation	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/SCD/SVD_Generation	The TSF shall enforce the SCD/SVD Generation SFP on: 1) subjects: S.User, 2) objects: SCD, SVD, 3) operations: generation of SCD/SVD pair.
[IFX specific] Application Note:	None

6.1.3.2 FDP_ACF.1/SCD/SVD_Generation: Security attribute based access control

Table 17 FDP_ACF.1/SCD/SVD_Generation

FDP_ACF.1/SCD/SVD_Generation	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1/SCD/SVD_Generation	The TSF shall enforce the SCD/SVD Generation SFP to objects based on the following: the user S.User is associated with the security attribute “SCD/SVD Management“.
FDP_ACF.1.2/SCD/SVD_Generation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute “SCD/SVD Management” set to “authorised” is allowed to generate SCD/SVD pair.
FDP_ACF.1.3/SCD/SVD_Generation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none

FDP_ACF.1/SCD/SVD_Generation	**Security attribute based access control**
FDP_ACF.1.4/SCD/SVD_Generation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.
[IFX specific] Application Note:	None

6.1.3.3 FDP_ACC.1/SVD_Transfer: Subset access control

Table 18 FDP_ACC.1/SVD_Transfer

FDP_ACC.1/SVD_Transfer	**Subset access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/SVD_Transfer	The TSF shall enforce the SVD Transfer SFP on: 1) subjects: S.User; 2) objects: SVD; 3) operations: export.
[IFX specific] Application Note:	None

6.1.3.4 FDP_ACF.1/SVD_Transfer: Security attribute based access control

Table 19 FDP_ACF.1/SVD_Transfer

FDP_ACF.1/SVD_Transfer	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/SVD_Transfer	The TSF shall enforce the SVD Transfer SFP to objects based on the following: 1) the S.User is associated with the security attribute Role; 2) the SVD.
FDP_ACF.1.2/SVD_Transfer	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *R.Admin, R.Sigy* is allowed to export SVD.
FDP_ACF.1.3/SVD_Transfer	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/SVD_Transfer	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.
[IFX specific] Application Note:	Application Note 9 applied.

6.1.3.5 FDP_ACC.1/Signature_Creation: Subset access control

Table 20 FDP_ACC.1/Signature_Creation

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.
[IFX specific] Application Note:	None.

6.1.3.6 FDP_ACF.1/Signature_Creation: Security attribute based access control

Table 21 FDP_ACF.1/Signature_Creation

FDP_ACF.1/Signature_Creation	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
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".
[IFX specific] Application Note:	None.

6.1.3.7 FDP_RIP.1: Subset residual information protection

Table 22 FDP_RIP.1

FDP_RIP.1	**Subset residual information protection**
Hierarchical to:	No other components.

FDP_RIP.1	Subset residual information protection
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.
[IFX specific] Application Note:	None.

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".

6.1.3.8 FDP_SDI.2/Persistent: Stored data integrity monitoring and action

Table 23 FDP_SDI.2/Persistent

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.
[IFX specific] Application Note:	None.

6.1.3.9 FDP_SDI.2/DTBS: Stored data integrity monitoring and action

Table 24 FDP_SDI.2/DTBS

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.
[IFX specific] Application Note:	Application Note 10: 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).

6.1.4 Identification and authentication (FIA)

6.1.4.1 FIA_UID.1: Timing of identification

Table 25 FIA_UID.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* 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.
[IFX specific] Application Note:	Application Note 11 applied.

6.1.4.2 FIA_UAU.1: Timing of authentication

Table 26 FIA_UAU.1

FIA_UAU.1	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
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* 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.
[IFX specific] Application Note:	Application Note 12 applied.

6.1.4.3 FIA_AFL.1: Authentication failure handling

Table 27 FIA_AFL.1

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 [01h to 7Fh]* 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.
[IFX specific] Application Note:	Application Note 13 applied.

6.1.5 Security management (FMT)

6.1.5.1 FMT_SMR.1: Security roles

Table 28 FMT_SMR.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.

6.1.5.2 FMT_SMF.1: Security management functions

Table 29 FMT_SMF.1

FMT_SMF.1	Security management functions
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: (1) Creation and modification of RAD, (2) Enabling the signature creation function, (3) Modification of the security attribute SCD/SVD management, SCD operational, (4) Change the default value of the security attribute SCD Identifier, (5) (5) *none.*
[IFX specific] Application Note:	Application Note 14 applied.

6.1.5.3 FMT_MOF.1: Management of security functions behaviour

Table 30 FMT_MOF.1

FMT_MOF.1	**Management of security functions behaviour**
Hierarchical to:	FMT_SMR.1 Security roles.
Dependencies:	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.

6.1.5.4 FMT_MSA.1/Admin: Management of security attributes

Table 31 FMT_MSA.1/Admin

FMT_MSA.1/Admin	**Management of security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1/Admin	The TSF shall enforce the SCD/SVD Generation SFP to restrict the ability to modify the security attributes SCD/SVD management to R.Admin.

6.1.5.5 FMT_MSA.1/ Signatory: Management of security attributes

Table 32 FMT_MSA.1/Signatory

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.

6.1.5.6 FMT_MSA.2: Secure security attributes

Table 33 FMT_MSA.2

FMT_MSA.2	**Secure security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or

FMT_MSA.2	**Secure security attributes**
	FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for SCD/SVD Management and SCD operational.
[IFX specific] Application Note:	Application Note 15 applied. Following values of the security attribute SCD/SVD Management are secure for the TOE and the operational TOE lifecycle: S.Admin to “yes” and of S.Sigy to “no”.

6.1.5.7 FMT_MSA.3: Static attribute initialisation

Table 34 FMT_MSA.3

FMT_MSA.3	**Static attribute initialisation**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the SCD/SVD Generation SFP, SVD Transfer SFP 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.

6.1.5.8 FMT_MSA.4: Security attribute value inheritance

Table 35 FMT_MSA.4

FMT_MSA.4	**Security attribute value inheritance**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_MSA.4.1	The TSF shall use the following rules to set the value of security attributes: (1) If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute “SCD operational of the SCD” shall be set to “no” as a single operation. (2) If S.Sigy successfully generates an SCD/SVD pair the security attribute “SCD operational of the SCD” shall be set to “yes” as a single operation.
[IFX specific] Application Note:	Application Note 16 applied.

FMT_MSA.4	Security attribute value inheritance
	The TOE may not support generating an SVD/SCD pair by the signatory alone, in which case rule (2) is not relevant.

6.1.5.9 FMT_MTD.1/Admin: Management of TSF data

Table 36 FMT_MTD.1/Admin

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.

6.1.5.10 FMT_MTD.1/Signatory: Management of TSF data

Table 37 FMT_MTD.1/Signatory

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.
[IFX specific] Application Note:	No other operation added other than “modify” in FMT_MTD.1/Signatory Managamenet of TSF data

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_EMS.1: TOE Emanation

Table 38 FPT_EMS.1

FPT_EMS.1	TOE Emanation
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in Table 39.

Table 39 FPT_EMS1.1 Emanation of TSF and User data

ID	Emissions	Attack surface	TSF data	User data
1	variations in Integrated Circuit	secure chip contact or contactless	• RAD • SCD	*none*

ID	Emissions	Attack surface	TSF data	User data
	power consumption or electronic emissions or variations in command execution time			

6.1.6.2 FPT_FLS.1: Failure with preservation of secure state

Table 40 FPT_FLS.1

FPT_FLS.1	**Failure with preservation of secure state**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: (1) self-test according to FPT_TST fails, *(2) None.*
[IFX specific] Application Note:	Application Note 19 applied.

6.1.6.3 FPT_PHP.1: Passive detection of physical attack

Table 41 FPT_PHP.1

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 tamper-ing with the TSF’s devices or TSF’s elements has occurred.

6.1.6.4 FPT_PHP.3: Resistance to physical attack

Table 42 FPT_PHP.3

FPT_PHP.3	**Resistance to physical attack**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist *physical manipulation and physical probing* to the *TSF* by responding automatically such that the SFRs are always enforced.
[IFX specific] Application Note:	Application Note 20:

FPT_PHP.3	Resistance to physical attack
	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. For example, the TSF may provide an appropriate message during start-up or the guidance documentation may describe a failure of TOE start-up as indication of physical tampering.

6.1.6.5 FPT_TST.1: TSF testing

Table 43 FPT_TST.1

FPT_TST.1	TST Testing
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of following self tests *during initial start-up* to demonstrate the correct operation of the TSF: *the Java Card OS the UMSLC (User Mode Security Life Control) selftest offered by the hardware platform is performed*.
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.
[IFX specific] Application Note:	Application Note 21 applied.

6.2 Security Assurance Requirements

Table 44 Security assurance requirements: EAL5 augmented with AVA_VAN.5 and and ALC_DVS.2.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Architectural Design with domain separation and non-bypassability

Assurance class	Assurance components
	ADV_FSP.5 Complete semi-formal functional specification with additional error information
	ADV_IMP.1 Implementation representation of the TSF
	ADV_INT.2 Well-structured internals
	ADV_TDS.4 Semi-formal modular design
	ADV_COMP.1 Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority
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
	ALC_COMP.1 Integration of the dependent component into the related base component and consistency check for delivery and acceptance procedures
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
	ASE_COMP.1 Consistency of Security Target
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
	ATE_COMP.1 Composite product functional testing
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis
	AVA_COMP.1 Composite product vulnerability assessment

6.3 Security Requirements Rationale

6.3.1 Security requirement coverage

Table 45 Mapping of functional requirements to security objectives for the TOE

TOE security objectives (→) Functional requirements (↓)	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.1	X		X	X	X						
FCS_CKM.6	X				X						
FCS_COP.1/SIG_GEN	X					X					
FCS_COP.1/PACE_AUTH							X				
FCS_COP.1/AA							X				
FCS_COP.1/CA							X				
FCS_COP.1/TA							X				
FCS_RNG.1							X				
FDP_ACC.1/SCD/SVD_Generation	X	X									
FDP_ACC.1/SVD_Transfer	X										
FDP_ACC.1/Signature_Creation	X						X				
FDP_AFC.1/SCD/SVD_Generation	X	X									
FDP_AFC.1/SVD_Transfer	X										
FDP_AFC.1/Signature_Creation	X						X				
FDP_RIP.1					X		X				
FDP_SDI.2/Persistent				X	X	X					
FDP_SDI.2/DTBS							X	X			
FIA_AFL.1							X				
FIA_UAU.1		X					X				
FIA_UID.1		X					X				
FMT_MOF.1	X						X				
FMT_MSA.1/Admin	X	X									
FMT_MSA.1/Signatory	X						X				
FMT_MSA.2	X	X					X				
FMT_MSA.3	X	X					X				
FMT_MSA.4	X	X		X			X				
FMT_MTD.1/Admin	X						X				
FMT_MTD.1/Signatory	X						X				
FMT_SMR.1	X						X				
FMT_SMF.1	X			X			X				
FPT_EMS.1					X				X		
FPT_FLS.1					X						
FPT_PHP.1										X	

TOE security objectives (→) Functional requirements (↓)	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FPT_PHP.3					X						X
FPT_TST.1	X				X	X					

6.3.2 TOE Security Requirements Sufficiency

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

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

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

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

OT.SCD_Secrecy (Secrecy of signature creation data) is provided by the security functions specified by the following SFR. FCS_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.

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

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

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

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

FIA_UAU.1 and FIA_UID.1 ensure that no signature creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process).

The security functions specified by FDP_ACC.1/Signature_Creation and FDP_ACF.1/Signature_Creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory. FMT_MOF.1 restricts the ability to enable the signature creation function to the signatory. FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

FCS_COP.1/PACE, FCS_COP.1/AA, FCS_COP.1/CA, FCS_COP.1/TA and FCS_RNG.1 secure the transmission of the RAD (e.g. PIN) and the set-up of a secure messaging channel.

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

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

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

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

6.3.3 Satisfaction of dependencies of security requirements

Table 46 Satisfaction of dependencies of security functional requirements

Functional requirement	Dependencies	Satisfied by
FCS_CKM.1	[FCS_CKM.2 FCS_CKM.5 or FCS_COP.1], FCS_CKM.6, [FCS_RBG.1 or FCS_RNG.1]	FCS_COP.1, FCS_CKM.6, FCS_RNG.1

Functional requirement	Dependencies	Satisfied by
FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1/SIG_GEN	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or], FCS_CKM.6	FCS_CKM.1, FCS_CKM.6
FCS_COP.1/PACE_AUTH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or], FCS_CKM.6	FCS_CKM.6 PACE protocol uses PIN based cryptographic key mechanism. So FCS_CKM.1 nor FDP_ITC.1 is required.
FCS_COP.1/AA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or], FCS_CKM.6	FCS_CKM.6 FCS_CKM.1
FCS_COP.1/CA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or], FCS_CKM.6	FCS_CKM.6 FCS_CKM.1
FCS_COP.1/TA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or], FCS_CKM.6	FCS_CKM.6 FCS_CKM.1
FCS_RNG.1	No dependencies	n/a
FDP_ACC.1/SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACC.1/SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACF.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_ACF.1/SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDR_RIP.1	No dependencies	n/a
FDP_SDI.2/Persistent	No dependencies	n/a
FDP_SDI.2/DTBS	No dependencies	n/a
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	n/a
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation, 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

Functional requirement	Dependencies	Satisfied by
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_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_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

6.3.4 Security Assurance Requirements Rationale

[PP0059] and its respective section “Rationale for chosen security assurance requirements” is also applicable for this chapter with one additional rationale justifying the security assurance dependencies. With the exception of ALC_DVS.2 and AVA_VAN.5, all assurance components are part of the EAL5 package, which by package design does not have any dependency conflicts and is hierarchical to EAL4.

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.

6.4 Statement of compatibility

The statement of compatibility is described in the document [SOC].

7 TOE Summary Specification

This TOE summary specification described in this section relies on the security services provided by the platform product. For a description of these services please refer to [ST_JC_Platform].

The composite TOE provides the security functions as follows:

7.1 SF.AccessControl

The TOE implements this security functionality to manage the access rights to the objects that are maintanined in the applet's file system. This includes the write access, pre-personalization and personlaization contents. This Security Functionality covers following SFRs:

- FDP_ACC.1/SCD/SVD_Generation
- FDP_ACC.1/SVD_Transfer
- FDP_ACC.1/Signature-creation
- FDP_ACF.1/SCD/SVD_Generation
- FDP_ACF.1/ SVD_Transfer
- FDP_ACF.1/Signature-creation
- FDP_RIP.1
- FIA_AFL.1
- FIA_UID.1
- FIA_UAU.1
- FMT_MOF.1
- FMT_MSA.1/Admin
- FMT_MSA.1/Signatory
- FMT_MTD.1/Admin
- FMT_MTD.1/ Signatory
- FMT_SMR.1

7.2 SF.CryptoOperation

The TOE supports the following cryptographic operations which are based on the security functionalities supported by the underlying OS platform. This security functionality covers the followig SFRs:

- FCS_CKM.1 Cryptographic key generation
- FCS_COP.1/SIG_GEN Cryptographic operation – Signature generation
- FCS_COP.1/PACE_AUTH Cryptographic operation – PACE Authentication
- FCS_COP.1/AA Cryptographic operation – Active Authentication
- FCS_COP.1/CA Cryptographic operation – Chip Authentication
- FCS_COP.1/TA Cryptographic operation – Terminal Authentication
- FCS_RNG.1 Quality metric for random numbers

The underlying platform supports this TSF by the following SFRs from [ST_JC_Platform]:

- FCS_CKM.1 Cryptographic key generation
- FCS_CKM.4 Cryptographic key destruction
- FCS_COP.1 Cryptographic operation
- FCS_RNG.1 Random number generation (Class PTG.3)

7.3 SF.Admin

This secure functionality provides the services to manage the pre-personalization and personalization data. Underlying OS platform functionality is used with required authentication performed:

- FIA_AFL.1: Authentication failure handling
- FMT_SMR.1: Security roles
- FMT_SMF.1: Security management functions
- FMT_MSA.3: Static attribute initialization
- FMT_MSA.4: Security attribute value inheritance

The underlying platform supports this TSF by the following SFRs from [ST_JC_Platform]:

- FCS_COP.1 Cryptographic operation

7.4 SF.Keys

This secure functionality provides the services to manage the secret data like cryptographic keys. This includes key generation, storage, access and destruction.

- FCS_CKM.1 Cryptographic key generation
- FCS_CKM.6 Timing and event of cryptographic key destruction

The underlying platform supports this TSF by the following SFRs from [ST_JC_Platform]:

- FCS_CKM.1 Cryptographic key generation
- FCS_CKM.4 Cryptographic key destruction

7.5 SF.SecureMessaging

This security functionality provides secure channel communication after establishing a successful authentication. The following SFRs covers this functionality:

- FIA_UAU.1: Timing of authentication
- FIA_UID.1: Timing of identification

The underlying platform supports this TSF by the following SFRs from [ST_JC_Platform]:

- FCS_COP.1 Cryptographic operation

7.6 SF.Authentication

This security function provides various authentication services based on the configuration. It provides VERIFY PIN command-based authentication mechanism which is based on [ISO7816-4]. Additonally, the following authentication mechanisms are provided and covers SFRs:

- FCS_COP.1/PACE_AUTH Cryptographic operation – PACE Authentication
- FCS_COP.1/AA Cryptographic operation -Active Authentication
- FCS_COP.1/CA Cryptographic operation – Chip Authentication
- FCS_COP.1/TA Cryptographic operation – Terminal Authentication

- FMT_MSA.2 Secure Security Attributes

The underlying platform supports this TSF by the following SFRs from [ST_JC_Platform]:

- FCS_COP.1 Cryptographic operation
- FCS_RNG.1 Random number generation (Class PTG.3)

7.7 SF.Physical

This security functionality protects the internal applet data for integrity. This covers the following SFRs:

- FDP_SDI.2/Persistent Stored data integrity monitoring and action
- FDP_SDI.2/DTBS Stored data integrity monitoring and action
- FPT_PHP.1 Passive detection of physical attack
- FPT_PHP.3 Resistance to physical attacks
- FPT_TST.1 TSF Testing
- FPT_EMS1 TOE Emanation
- FPT_FLS.1 Failure presertaion of secure state

The underlying platform supports this TSF by the following SFRs from [ST_JC_Platform]:

- FPT_PHP.3 Resistance to physical attacks
- FPT_TST.1 TSF testing

References

[AIS31] Functionality classes and evaluation methodology for physical random number generators. AIS31, Version 2.1, 2011-12-02, Bundesamt für Sicherheit in der Informationstechnik.

[CCPart1] Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 1: Introduction and general model

[CCPart2] Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 2: Security functional components

[CCPart3] Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 3: Security assurance components

[CCPart4] Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 4: Framework for the specification of evaluation methods and activities

[CCPart5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022, Revision 1

[CCErrata] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), V1.1, 2024-07-22

[CCTrans] CCMC-2023-04-001, Transition Policy to CC:2022 and CEM:2022, 2023-04-20

[CEM2022] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, November 2022, CEM:2022, Revision 1

[CompositeEvaluation] Composite product evaluation for Smart Cards and similar devices, April 2012, Version 1.2, CCDB-2012-04-001

[EU-eMRTD] EU – eMRTD Specification. ANNEX to the Commission Implementing Decision laying down the technical specifications regarding the standards for security features and biometrics in passports and travel documents issued by Member States and repealing Decisions C(2006) 2909 and C(2008) 8657

[TR_ECC] Federal Office for Information Security (BSI) TR-03111 Elliptic Curve Cryptography Version 2.0, 2012-06-28

[ICAO_SAC] International Civil Aviation Organization Machine Readable Travel DocumentsTechnical Report Supplemental Access Control for Machine Readable Travel Documents Version 1.00, November 2010

[ICAO_9303_01] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Eighth Edition, 2021, International Civil Aviation Organization

[ICAO_9303_10] International Civil Aviation Organization, DOC 9303 Machine Readable Travel Documents Eighth Edition – 2021, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

[ICAO_9303_11] International Civil Aviation Organization, DOC 9303 Machine Readable Travel Documents Eighth Edition – 2021 Part 11: Security Mechanisms for MRTD's

[ISO9797-1] ISO/IEC International Standard 9797-1:2011-(E), Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechnanisms using a block cipher, Second Edition 2011-03-01

[ISO14443-3] ISO/IEC International Standard 14443-3 Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision, Fourth edition 2018-07

[ISO14443-4] ISO/IEC International Standard 14443-4 Cards and security devices for personal identification Contactless proximity objects, Part 4: Transmission protocol, Fourth edition 2018-07

[ISO7816-3] ISO/IEC 7816-3:2006(E): International Standard ISO 7816-3: Identification cards - Integrated circuit cards, Part 3: Electronic signals and transmission protocols, Third edition 2006-11-01

[ISO7816-4] ISO/IEC JTC1/SC17 International Standard 7816-4: Identification Cards - Integrated circuit cards, Part 4: Organization, security and commands for interchange, Third edition 2013-04-15

[ISO7816-8] International Standard 7816-8: Identification Cards - Integrated circuit cards, Part 8: Commands and Mechanisms for Security Operations, Fifth edition 2021-08

[ISO7816-9] International Standard 7816-9: Identification Cards - Integrated circuit cards, Part 9: Commands for card management, Third edition 2017-12

[ISO9796-2] ISO/IEC International Standard ISO9796-2 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms

[NIST_Hash] FIPS PUB 180-4, Federal Information Processing Standards Publication Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, March 2012

[NIST_DES] FIPS PUB 46-3: Data Encryption Standard (DES), Reaffirmed, 1999 October 25

[GPv2_3_1] Global Platform Card Specification v2.3.1, March 2018

[UserGuideAdmin] SLJ38Gxymmmap Infineon Applet Collection - eSign V1.0 Administration Guide, Revision 1.1, 2025-02-25

[UserGuideDataBook] SLJ38Gxymmmap Infineon Applet Collection - eSign V1.0 Administration Guide, Revision 1.1, 2025-03-28

[ST_HW_Platform] Security Target for BSI-DSZ-CC-1169-V4-2024

[ST_JC_Platform] Security Target for SECORA™ ID v2.01 (SLJ38Gxymm1ap) - NSCIB-CC-2400062-01

[TR_03110_1] Federal Office for Information Security (BSI) Technical Guideline TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 1 - eMRTDs with BAC/PACEv2 and EACv1 Version 2.20, 26. February 2015

[TR_03110_2] Federal Office for Information Security (BSI) Technical Guideline TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS) Version 2.21, 21 December 2016

[TR_03110_3] Federal Office for Information Security (BSI) Technical Guideline TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 3 - Common Specifications Version 2.21, 21 December 2016

[PKCS #3] Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, November 1, 1993

[PP0059]	BSI-CC-PP-0059-2009-MA-02, Version 1.03
[PP_0084]	Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014, BSI-CC-PP-0084-2014
[FIPS_197]	Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. Department of Commerce/National Institute of Standards and Technology, November 26, 2001
[PKCS v2.2]	PKCS v2.2
[X9.62]	ANSI X9.62-2005
[ISO14888-3]	ISO/IEC 14888-3:2006
[IEEE P1363]	IEEE Std 1363-2000
[FIPS186-3]	FIPS 186-3
[RFC5639]	RFC 5639
[SEC1]	Certicom SEC1
[Directive]	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
[SOC]	Statement of Compatibility for Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection - eSign V1.0

Revision history

Reference	Description
Revision 0.9, 2025-06-05	
Chapter 1.3	TOE identification corrected for applet version 1.3.0.0
Chapter 1.5	Guidance version updated.
Revision 0.8, 2025-05-19	
Chapter 1.3	TOE identification updated for applet version 1.3.0.0
Chapter 1.5	Guidance version updated.
Revision 0.7, 2025-04-02	
Chapter 6.2	Assurance components *.COMP are are added to the SARs.
Revision 0.6, 2025-03-25	
Chapter 1.3	TOE identification updated for applet version 1.2.0.0
Chapter 1.5	Guidance version updated. Also added the OS platform guidance for the Java Card with open mode.
References	ICAO specification is updated to Eighth edition.
Revision 0.5, 2025-03-03	
Chapter 6.1.2.1	FCS_CKM.5 added as a dependency to FCS_CKM.6 as per CC:2022-Errata-V1.1.
Chapter 6.1.6.5	Refined the FPT_TST.1 SFR as per CC:2022.
Revision 0.4, 2025-02-12	
Chapter 1.3	Added more clarity for the OS product configurations.
Chapter 6.1.2.8	FCS_RNG SFR description is updated as per the format of [AIS 31].
Revision 0.3, 2025-01-10	
all	CC Conformance claim is updated to include Part 4 and 5. Mappings are corrected in section 6.3.1 Security requirement coverage. New SFR FCS_COP.1/TA added for Terminal authentication.
Revision 0.2, 2024-12-06	
Chapter 1.6.6	Additional details added for Lifecycle and Delivery
Chapter 7	Content added for TOE Summary Specification
Revision 0.1, 2024-11-28	
all	Initial version - draft

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2025-06-05

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email:
csscustomerservice@infineon.com