MASKTECH

SECURITY TARGET

COMMON CRITERIA DOCUMENTS | Version 1.2

MaskTech eSign Applet on Secora™ ID S v1.1

Java Card applet providing Secure Signature Creation Device with key generation and key import

Certification-ID: NSCIB-CC-299278

Public Version

MaskTech International GmbH | Nordostpark 45 | Nuernberg | www.masktech.com | +49 (0)911 95 51 49-0

Contents

1 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- prEN 419211-1, Protection profiles for secure signature creation device – Part 1: Overview[1]
- ISO/IEC 15408-1:2009[2] Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
- ISO/IEC 15408-2[2], Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components
- ISO/IEC 15408-3[2], Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components

[1] To be published. This document was submitted to the Enquiry procedure under reference prEN 14169-1.

[2] ISO/IEC 15408-1, -2 and -3 respectively correspond to Common Criteria for Information Technology Security Evaluation, Parts 1, 2 and 3.

2 Conventions and Terminology

2.1 Conventions

The content and structure of this document follow the rules and conventions laid out in ISO/IEC 15408-1.

Normative aspects of content in this European Standard are specified according to the Common Criteria rules and not specifically identified by “shall”.

2.2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.2.1 Legislative references

The European standard prEN 14169 reflects the requirement of a European directive in the technical terms of a protection profile. The following terms are used in the text to reference this directive:

2.2.1.1 The Directive

Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on “a Community framework for electronic signatures” [DIR_1999/93/EC] Note: References in this document to a specific article and paragraph of Directive 1999/93/ec are of the form “(**the directive**: n.m)”.

2.2.1.2 Annex

one of the annexes, Annex I, Annex II or Annex III of **the directive**

2.2.2 Technical Terms

2.2.2.1 Administrator

user who performs administrative functions. In the context of this Security Target the role is split into two roles borrowed from ePassport procedures in order to distinguish different tasks:

- **Pre-personalization agent**: Loading of the eSign package.
- **Personalization agent**: Installation of the eSign applet(s) and writing of user data.

2.2.2.2 Advanced electronic signature

digital signature which meets specific requirements in **(the directive: 2.2)**

Note 1 to entry: according to **the directive** a digital signature qualifies as an advanced electronic signature if it:

- is uniquely linked to the signatory;
- is capable of identifying the signatory;
- is created using means that the signatory can maintain under their sole control; and
- is linked to the data to which it relates in such a manner that any subsequent change of the data are detectable.

2.2.2.3 Authentication data

information used to verify the claimed identity of a user

2.2.2.4 Certificate

digital signature used as electronic attestation binding signature verification data to a person confirming the identity of that person as legitimate signer **(the directive: 2.9)**

2.2.2.5 Certificate info

information associated with an SCD/SVD pair that may be stored in a secure signature creation device

Note 1 to entry: Certificate info may include:

- 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, or
- a public key certificate as defined in X.509.

Note 2 to entry: Certificate info may contain information to allow the user to distinguish between several certificates.

2.2.2.6 Certificate generation application

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

2.2.2.7 Certification service provider

CSP entity that issues certificates or provides other services related to electronic signature **(the directive: 2.11)**

2.2.2.8 Data to be signed

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

2.2.2.9 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 1 to entry: Examples of DTBS/R are:

- 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.

2.2.2.10 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

2.2.2.11 Qualified certificate

public key certificate that meets the requirements laid down in **Annex I** and that is provided by a CSP that fulfills the requirements laid down in **Annex II (the directive: 2.10)**

2.2.2.12 Qualified electronic signature

an advanced electronic signature which is based on a qualified certificate and which is created by an SSCD

2.2.2.13 Reference authentication data

RAD data persistently stored by the TOE for authentication of the signatory

2.2.2.14 Secure signature-creation device

SSCD a signature-creation device which meets the requirements laid down in *Annex III*

Note 1 to entry: An SSCD may be evaluated according to this security target conforming to *PP SSCD KG* and *PP SSCD KI* as defined in the series of European Standards prEN 14169

2.2.2.15 Signatory

a person who holds (and is a legitimate user) of an SSCD and acts either on their own behalf or on behalf of the natural or legal person or entity they represent

2.2.2.16 Signature creation application

SCA application complementing an SSCD with a user interface with the purpose to create an electronic signature

2.2.2.17 Signature creation data

SCD unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature

Note 1 to entry: For the PPs of this standard the SCD is held in the SSCD.

2.2.2.18 Signature creation system

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

2.2.2.19 Signature verification data

SVD data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature

2.2.2.20 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

2.2.2.21 User

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

2.2.2.22 User message

data determined by the signatory as the correct input for signing

2.2.2.23 Verification authentication data

VAD data input to an SSCD for authentication of the signatory

2.3 Abbreviated Terms

CA	Chip Authentication
CC	Common Criteria[1]
CGA	certificate generation application
CSP	certification service provider
DTBS	data to be signed
DTBS/R	data to be signed or its unique representation
EAL	evaluation assurance level[1]
ePP	electronic passport
eSign	electronic signature card
HID	human interface device
IT	information technology
MRTD	Machine Readable Travel Document
PP	protection profile[1]
RAD	reference authentication data
SCA	signature creation application
SCD	signature creation data
SCS	signature creation system
SDO	signed data object
SFP	security function policy
SSCD	Secure Signature Creation Device
ST	security target[1]
SVD	signature verification data
TOE	target of evaluation[1]
TSF	TOE security functionality[1]
VAD	verification authentication data

[1] See [CC_Part1, CC_Part2, CC_Part3] for details on the specification of Common Criteria.

3 Security Target Introduction (ASE_INT.1)

3.1 ST Reference

Title	Security Target – MaskTech eSign Applet on Secora™ ID S v1.1
Version	1.2, 2022-09-09
Editors	Thomas Rölz
Compliant to	Protection profiles for Secure signature creation device Part 2: Device with key generation, version 2.0.1, BSI-CC-PP-0059 [CC_PP-0059] (***PP SSCD KG***) Part 3: Device with key import, version 1.0.2, BSI-CC-PP-0075 [CC_PP-0075] (***PP SSCD KI***) Part 4: Extension for device with key generation and trusted communication with certificate generation application, version 1.0.1, BSI-CC-PP-0071 [CC_PP-0071] (***PP SSCD KG TCCGA***) Part 5: Extension for device with key generation and trusted communication with signature creation application, version 1.0.1, BSI-CC-PP-0072 [CC_PP-0072] (***PP SSCD KG TCSCA***) Part 6: Extension for device with key import and trusted communication with signature creation application, version 1.0.4, BSI-CC-PP-0076 [CC_PP-0076] (***PP SSCD KI TCSCA***)
CC Version	3.1 (Revision 5)
Assurance Level	The assurance level for this ST is EAL5 augmented
Keywords	secure signature creation device, electronic signature, digital signature, key generation, trusted communication with certificate generation application, trusted communication with signature creation application, key import

3.2 TOE reference

TOE name	MaskTech eSign Applet on Secora™ ID S v1.1
TOE version	1.0
Applet ID	0x0013
TOE hardware	IFX_CCI_000005 by Infineon Technologies AG
Javacard OS platform	Secora™ ID S v1.1 by Infineon Technologies AG
Javacard OS certification	CC-22-175887

3.3 TOE Identification

It is possible to receive the applet ID of the MaskTech eSign Applet on Secora™ ID S v1.1 by personalizing the Helper applet according to [AGD_eSign] Section “Applet ID” in the Helper chapter. The platform can be identified according to section “Platform Information”[1].

3.4 Security Target Overview

This security target defines the security objectives and requirements for the contactless/contact-based[2] chip of a secure signature creation device (SSCD). The application’s file system follows the PKCS #15 structure [PKCS_15]. The assurance level for the TOE is CC EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

This Security Target claims conformance on the following protection profiles covering a number of requirements for a secure signature creation device:

Protection profiles *PP SSCD KG*, *PP SSCD KG TCCGA* and *PP SSCD KG TCSCA* as well as *PP SSCD KI* and *PP SSCD KI TCSCA* are established by CEN as a European standard for products to create electronic signatures. They fulfill requirements of directive[3] 1999/93/ec of the European parliament and of the council of 13 December 1999 on a community framework for electronic signatures.

In accordance with article 9 of this European directive this standard can be indicated by the European commission in the Official Journal of the European Communities as generally recognized standard for electronic signature products.

The core protection profiles *PP SSCD KG* and *PP SSCD KI* define security functional requirements and security assurance requirements that comply with those defined in Annex III of **the directive** for a secure signature creation device (SSCD). This secure signature creation device is the target of evaluation (TOE) for protection profiles *PP SSCD KG* and *PP SSCD KI*.

European Union Member States may presume that there is compliance with the requirements laid down in Annex III of **the directive** when an electronic signature product is eval-

[1] Both queries are possible only in the personalization phase.

[2] Both interfaces provide similar functionality and are thus taken as one single product in this ST. If the Personalization Agent configures the TOE with contact-only interface trusted channels are optional for communication with the TOE aside from key import (easy access).

[3] This European directive is referred to in the ST as “the directive”.

uated to a Security Target (ST) that is compliant with protection profiles *PP SSCD KG* and *PP SSCD KI*.

PP SSCD KG describes core security requirements for a secure device that can **generate** a signing key[4] (signature creation data, SCD) and operates to create electronic signatures with the generated key. *PP SSCD KI* describes core security requirements for a secure device that can **import** a signing key[5] (signature creation data, SCD) and operates to create electronic signatures with the imported key. A device evaluated according to *PP SSCD KG* and/or *PP SSCD KI* and used in the specified environments can be trusted to create any type of digital signature. As such *PP SSCD KG* and/or *PP SSCD KI* can be used for any device that has been configured to create a digital signature. Specifically *PP SSCD KG* and/or *PP SSCD KI* allows the qualification of a product as a device for creating a qualified electronic signature as defined in **the directive**.

When operated in a secure environment for signature creation a signer may use an SSCD that fulfills only these core security requirements to create a qualified electronic signature.[6]

PP SSCD KG TCCGA is an extension and conforms[7] to the core *PP SSCD KG*. It defines the security requirements for a trusted communication to a certificate generation application (CGA). These security features allow a changed life cycle of the TOE, i.e. the signatory may generate an SCD/SVD key pair suitable to create qualified electronic signatures and transfer the corresponding public key (signature verification data, SVD) as input to the CGA **after** the delivery of the SSCD. The TOE supports its authentication as SSCD by the CGA of the Certification service provider (CSP) and a trusted communication with this CGA for protection of the SVD.

PP SSCD KG TCSCA is an extension and conforms[7] to the core *PP SSCD KG*. It defines the security requirements for an SSCD used in environments, where the communication between SSCD and the signature creation application (SCA) is assumed to be protected by the SSCD and the SCA. These security features allow using the TOE in a more complex operational environment. The TOE supports a trusted communication with an SCA for protection of authentication data and data to be signed.

PP SSCD KI TCSCA is an extension and conforms[7] to the core *PP SSCD KI*. It defines the security requirements for an SSCD used in environments, where the communication between SSCD and the signature creation application (SCA) is assumed to be protected by the SSCD and the SCA. These security features allow using the TOE in a more complex operational environment. The TOE supports a trusted communication with an SCA for protection of authentication data and data to be signed. *PP SSCD KI TCSCA* is equivalent to *PP SSCD KG TCSCA*, but refers to a different core PP.

For convenience, extensive parts that refer mainly to only one PP are marked as:

PP SSCD KG is marginalized with **KG**

[4] An SSCD that can generate its own SCD/SVD was defined in the previous version of *PP SSCD KG* (CWA 14169) as a Type 3 SSCD. The notion of types does not exist anymore in this series of ENs.

[5] An SSCD that can import SCD/SVD was defined in the previous version of PP *PP SSCD KI* (CWA 14169) as a Type 2 SSCD. The notion of types does not exist anymore in this series of ENs. In order to refer to the same functionality, a reference to EN 419211-3 (i.e. Part 3) should be used.

[6] An advanced electronic signature is defined as an electronic signature created by an SSCD using a public key with a public key certificate created as specified in **the directive**.

[7] See [CC_Part1] for the usage of multiple protection profiles.

PP SSCD KI is marginalized with **KI**

PP SSCD KG TCSCA* or *PP SSCD KI TCSCA is marginalized with **SCA**

PP SSCD KG TCCGA is marginalized with **CGA**

In addition, margins **PACE** or **EAC**, respectively, are applied, when large text passages concern the PACE or EAC functionality.

3.5 TOE Overview

This security target defines the security objectives and requirements for the MaskTech eSign Applet on Secora™ ID S v1.1 as secure signature creation device (SSCD). The MaskTech eSign Applet on Secora™ ID S v1.1 actually comprises several applets mentioned in 3.6.1 that together with the platform components yield the TOE.

3.5.1 TOE Definition

In the context of this Security Target the SSCD functionality is provided by the MaskTech eSign Applet on Secora™ ID S v1.1 to be used exclusively on the Secora™ ID S v1.1 Java Card Platform Implementation for Infineon on IFX_CCI_000005 (SLJ52GxxyyyzS) which is certified CC EAL6 augmented (CC-22-175887). The Java Card platform is provided in the FLASH of a smart card based on the IFX_CCI_000005 chip of Infineon Technologies AG which is itself also certified CC EAL6 augmented.

The TOE is a combination of hardware and software configured to securely create or import, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole life cycle beginning with import 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 SCD and the correspondent signature verification data (SVD),
b) to import SCD and, optionally, the corresponding SVD through a trusted channel[8],
c) to export the SVD for certification through a trusted channel[9] to the CGA,
d) to prove the identity as SSCD to external entities,
e) to, optionally, receive and store certificate info,
f) to switch the TOE from a non-operational state to an operational state, and
g) if in an operational state, to create digital signatures for data with the following steps:
    1) select a set of SCD,
    2) authenticate the signatory and determine its intent to sign,
    3) receive data to be signed or a unique representation thereof (DTBS/R) through a trusted channel[10] from SCA,

[8] For contact-only based SSCDs key import is only possible after Chip Authentication has been accomplished.

[9] For contact-only based SSCDs trusted channel is only used if the CGA requests Chip Authentication.

[10] Trusted channel is optional with cards configured for contact-only interface (easy access).

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

The TOE is prepared for the signatory's use by

a) importing at least one set of SCD, and/or

b) optionally, generating at least one SCD/SVD pair, and

c) personalizing for the signatory by storing in the TOE:

1) authentication data (i.e. PUK) for the signatory to be able to activate the RAD
2) optionally, certificate info for at least one SCD in the TOE.

After preparation 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 by activating the RAD.

As the initial value of the RAD is set by the legitimate user, the verification authentication data (VAD) required for use of the TOE in signing is implicitly known only by the legitimate user. After preparation he must be informed of the PUK value enabling him to activate (and set) the RAD. The means of providing this information is expected to protect the confidentiality and the integrity of the PUK.

If the use of an SCD is no longer required, then it shall be destroyed by erasing the SCD data as well as the associated certificate info, if any exists.

3.5.2 TOE Operational Usage

3.5.2.1 General Operation

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. The electronic signature created with the TOE is a *qualified electronic signature* as defined in the Directive if the certificate for the SVD is a qualified certificate (Annex I).

The signature creation application is assumed to protect the integrity of the input it provides to the TOE signature creation function as being consistent with the user data 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. Optionally, the TOE and the SCA communicate through a trusted channel[11] in order to protect the integrity of the DTBS/R.

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

[11] Trusted channel is optional with cards configured for contact-only interface (easy access).

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:

- initializing 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.

3.5.2.2 Operation of the TOE

This section presents a functional overview of the TOE and its distinct operational environments (Fig. 3.1). Depending on the TOE interface configured by the Personalization Agent during personalization trusted channels may be established for communication with the TOE in the usage phase.

Contact-only interface The Personalization Agent configures the TOE **solely** for use with the contact interface. Because contact based communication is by definition considered secure in the preparation environment, the signing environment and the management environment trusted channel communication is optional (aside from key import) in this case. This allows for easy access without PACE authentication in most cases.

Contactless or dual interface The Personalization Agent configures the TOE for use with contactless interface or dual interface. In this case each interaction with the TOE requires user authentication using the PACE protocol. A Secure Messaging session is started providing a trusted channel for communication.

N Personalization is performed in the Global Platform environment making use of secure communication via SCP03.

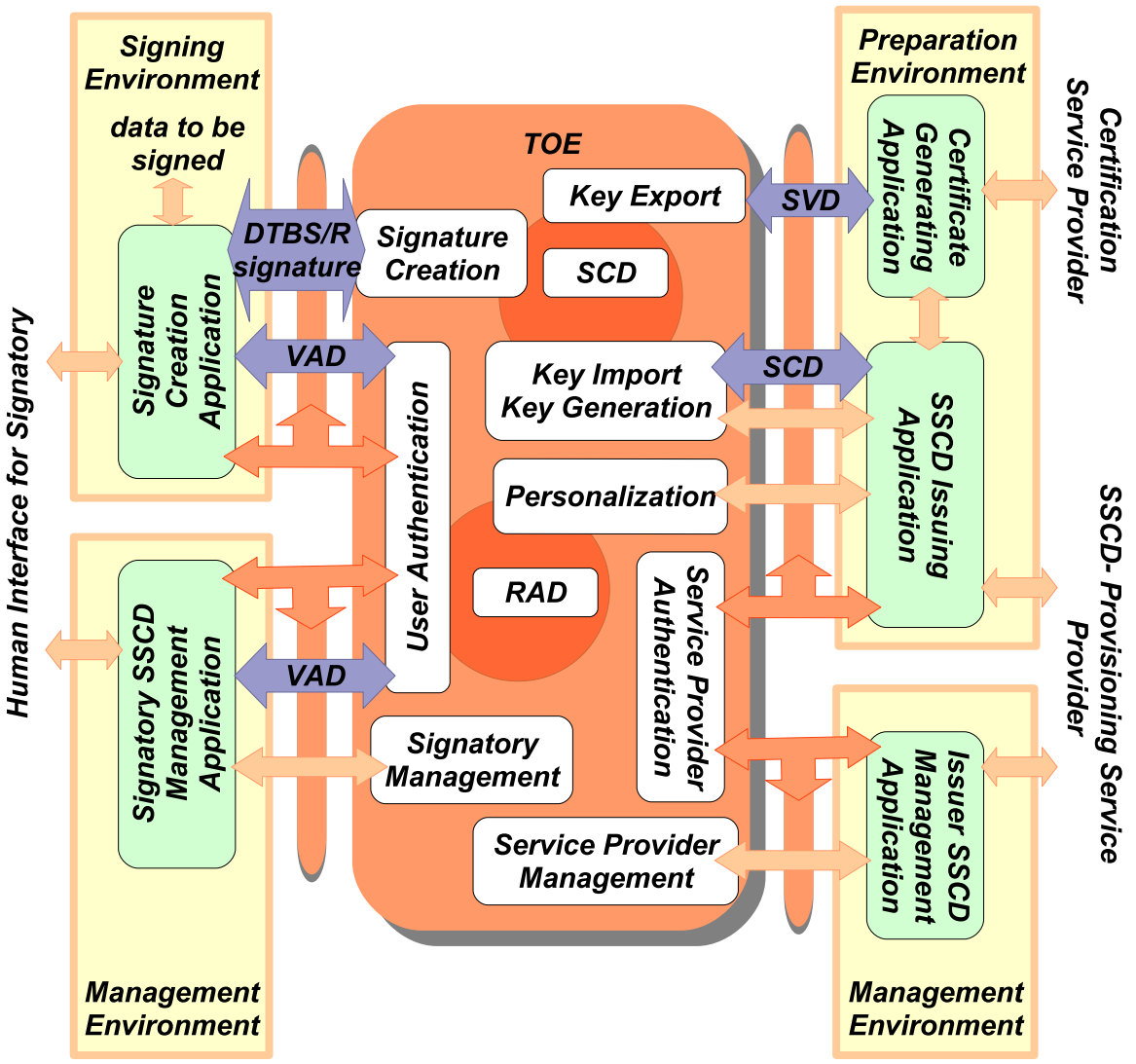

Figure 3.1: SSCD functions and operational environments including trusted channels for communication with CGA and SCA.

The TOEs interactions comprise of:

Preparation environment

- Interaction with an SCD/SVD generation application to **import** the signature creation data (SCD) via trusted channel. The SCD/SVD generation application transmits the SVD to the CGA.
- Interaction with a *certificate generation application* (CGA) to obtain a certificate for the signature validation data (SVD) corresponding to the SCD the TOE has **generated**. The trusted channel[12] allows the CGA to check the authenticity of the SVD.
- Interaction with an *SSCD issuing application* to personalize the TOE with personal information of the legitimate user. Optionally one or more signature key pairs can be generated on the card or written to the card.

[12] For contact-only based SSCDs trusted channel is only used if the CGA requests Chip Authentication.

Signing environment

- Interaction with a signer through a *signature creation application* (SCA) to sign data after authenticating the signer as its signatory. The SCA 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[13]. The communication through a trusted channel[14] ensures the integrity of the DTBS respective DTBS/R.

Management environment

- Interaction with a *signatory SSCD management application* to activate the RAD or change its reference data.
- Interaction with a *issuer SSCD management application* to reset a blocked RAD or terminate a signature key.

The TOE stores reference authentication data (RAD, i.e. PIN, CAN and PIN_{QES}) and multiple instances of signature creation data (SCD). It provides a function to identify each SCD and the signature creation application (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 in Article 5.1 of **the directive**[15]. Determining the state of the certificate as qualified is beyond the scope of prEN 14169. However, key #1 of the signature key set meets the requirements for the generation of qualified electronic signatures.

The SCA is assumed to protect the integrity of the input it provides to the TOE signature creation function as being consistent with the user data authorized for signing by the signatory. Unless implicitly known to the TOE, the SCA indicates the kind of the signing input (as DTBS/R) it provides and computes any hash 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. The TOE and the SCA communicate through a trusted channel[15] in order to protect the integrity of the DTBS/R.

The TOE stores signatory RAD to authenticate a user as its signatory (see Table 3.2). The TOE protects the confidentiality and integrity of the RAD. The TOE receives the VAD from the 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.

Note 1: Within the PACE protocol, not the VAD (i.e. the password for PIN or CAN, respectively) is transmitted from the terminal to the card, but a nonce encrypted with the VAD (zero-knowledge protocol).

[13] At a pure functional level the SSCD creates a digital signature; for an implementation of the SSCD, in that meeting the requirements of *PP SSCD KG* and/or *PP SSCD KI* 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.

[14] Trusted channel is optional with cards configured for contact-only interface (easy access).

[15] Note that this Security Target takes all requirements of the eIDAS regulation [REG_910/2014] and the commission implementing regulation [CID_2016/650] into account.

3.5.3 TOE major security features

Security features of the platform

The TOE relies on the following security features of the Java Card platform Secora™ ID S v1.1.

- Cryptographic ciphers (AES, TDES)
- Signature algorithms (ECDSA, RSA)
- Key agreement algorithms (ECDH, PACE)
- Key pair generation (EC, RSA)
- Message digest algorithms (SHA-1, SHA-2 family)
- Random number generation (PTG.3 according to [BSI_AIS31])
- Secure channel SCP03 from [GP_SCP03]
- Content management provided by [GP]
- LDS-API according to [ICAO_9303]
- PACE API, a proprietary API for the PACE cryptographic protocol which is especially hardened against side channel attacks.

Security Features and Access Control

MaskTech eSign Applet on Secora™ ID S v1.1 supports the following methods:

PACE according to [BSI_TR-03110-1, BSI_TR-03110-2, ICAO_SAC][16] for

- the identification and authentication of the user as the legitimate card holder
- the establishment of a trusted channel between the terminal and the card
- the protection against tracking and eavesdropping
- proof the authenticity of the chip to the terminal (*Chip Authentication*)

The TOE provides the following secrets to be used within the PACE protocol (PIN_{QES} assigns an additional password for authentication to create qualified electronic signatures):

[16] PACE authentication is not used with cards configured for contact-only interface (easy access).

Secret	Minimum length	Initial value set by	Used to authenticate for
PIN	6 digits	Signatory on first usage	Advanced signature creation, verification of PIN_{QES}, change reference data of PIN_{QES}‡ change reference data of PIN and Select or Read Binary of protected files
PUK	8 digits	Administrator on personalization	Signature key generation, certificate import, key termination, activation of PIN, activation of PIN_{QES}, reset retry counter of PIN, reset retry counter of PIN_{QES} change reference data of PIN and Update Binary of protected files
CAN	6 digits	Administrator on personalization	Verification of PIN_{QES}, change reference data of PIN_{QES}‡ and unblock PIN and PUK

‡ *Additionally requires authentication against PIN_{QES}.*

Table 3.1: Secrets used within the PACE protocol.

PIN and **PUK** are protected against denial-of-service attacks by setting the chip into a **suspended state**, before the retry counter of the secret in question is exhausted after consecutive failed authentication attempts. Before the very last retry to authenticate against PIN or PUK, respectively, can be done, an authentication against **CAN** must be performed.

Chip Authentication Version 1 according to [BSI_TR-03110-1][17] to

- proof the authenticity of the chip to the terminal
- establish a trusted channel between the terminal and the card

Terminal Authentication Version 1 according to [BSI_TR-03110-1][18] to restrict the service provisions to authorized SCAs and CGAs.

The number and type of keys (QES/NonQES) is limited only by space. The key sizes are specified during personalization according to [AGD_eSign].

To create an electronic signature, the legitimate user must authenticate himself against the **RAD**, which consists of one or more secrets stored on the chip. The RAD also ensures that the SSCD is in an non-operational state when delivered to the signatory. In the *preparation phase* (see also section 3.6.4) CAN and PUK are set in the personalization step and delivered to the signatory. The creation of a qualified electronic signature is additionally protected by the secret **PIN_{QES}**, which is a password with a minimum length of 6 digits stored on the chip in the OwnerPIN object. For PIN and PIN_{QES} no initial values are set in the personalization step.

[17] Chip Authentication may be configured by the Personalization Agent and is used only if the application requests it. For contact-only SSCDs it is mandatory for key import.

[18] Terminal Authentication is not used with cards configured for contact-only interface.

The secrets must be activated by the signatory on first usage. For this, the authentication against PUK is required. Table 3.2 lists the keys and the corresponding RADs:

Key #	To be used for	Corresponding RAD	Remarks
1	qualified signature	PIN **and** PIN_{QES} **or** CAN **and** PIN_{QES}	After each qualified signature creation, the authentication state of PIN_{QES} is reset to 'not verified'.
2	advanced signature	PIN	–
3	advanced signature	PIN	–

Table 3.2: Available signature keys and corresponding RADs.

To use the decryption key #4, authentication against PIN is required. Note that this functionality is not within the scope of this certification. Also note that some security requirements (see chapter 8) only apply to configurations requiring Terminal Authentication for the communication with the SCA and CGA.

Configuration of Security Features

Configuration of the security features is accomplished during personalization by the SSCD-provisioning service provider. Details are given in the *User Guidance* [AGD_eSign].

3.6 TOE Description

3.6.1 Component Overview

The TOE is the MaskTech eSign Applet on Secora™ ID S v1.1 installed on the Java Card Secora™ ID S v1.1 which is based on the Smart Card IC IFX_CCI_000005.

The TOE comprises

- the circuitry of the travel document's chip (IFX_CCI_000005),
- the IC Dedicated Software provided by Infineon Technologies AG,
- the IC Embedded Software, the Java Card Platform (Secora™ ID S v1.1) for Infineon Technologies AG on IFX_CCI_000005.
- the eSign Applet provided by MaskTech International GmbH
- the Helper Applet provided by MaskTech International GmbH
- the PACE Applet provided by MaskTech International GmbH
- the TLV-Library provided by MaskTech International GmbH and
- the associated guidance documentation[19] [AGD_eSign]

[19]The User Manual (Administration Guide) provides guidance to perform installation/personalization and maintain the targeted security level during Personalization and Operation phase.

Figure 3.2 shows the components of the TOE in a layered structure. The blue outline encloses all components being part of the composite TOE covered in this Security Target.

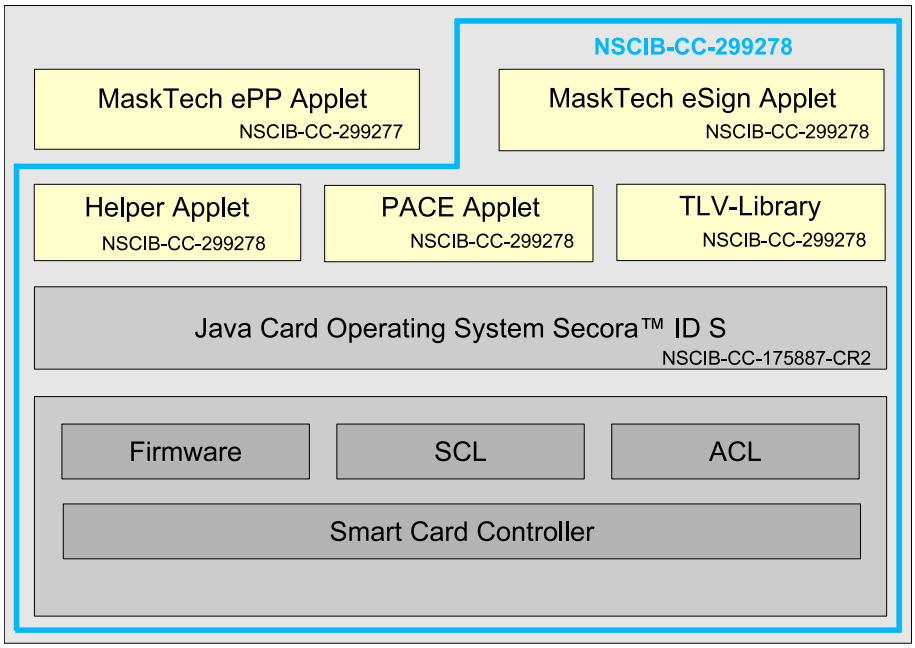

Figure 3.2: Components of the MaskTech eSign Applet on Secora™ ID S v1.1

The bottom layer represents the hardware consisting of

- Smart Card Controller (IFX_CCI_000005)
- Firmware
- Symmetric Crypto Library (SCL)
- Asymmetric Cryptographic Library (ACL)

The hardware is CC certified and provides protection against fault attacks and side channel attacks. It also provides hardware co-processors supporting cryptographic standards AES, RSA, EC, and 3DES.

The layer above the hardware represents the JavaCard Operating System Secora™ ID S v1.1. It is CC certified as CC-22-175887 and provides security services for

- Cryptographic ciphers (AES, TDES)
- Signature algorithms (ECDSA, RSA)
- Key agreement algorithms (ECDH, PACE)
- Key pair generation (EC, RSA)
- Message digest algorithms (SHA-1, SHA-2 family)
- Random number generation (PTG.3 according to [BSI_AIS31])
- Secure channel SCP03 from [GP_SCP03]
- Content management provided by [GP]

- LDS-API according to [ICAO_9303]
- PACE API, a proprietary API for the PACE cryptographic protocol which is especially hardened against side channel attacks.

The light yellow blocks represent the the applets provided by MaskTech International GmbH that together yield the MaskTech eSign Applet on Secora™ ID S v1.1. Only the components surrounded by the blue outline are part of TOE and responsible for the following tasks:

- MaskTech eSign Applet provides the SSCD functionality.
- MaskTech Helper Applet provides functionality for Secure Messaging as well as buffer handling.
- MaskTech PACE Applet provides functionality for the PACE protocol.
- MaskTech TLV-Library provides functionality for TLV-handling during communication with the TOE.

N The MaskTech ePP applet also shown in figure 3.2 is not part of the TOE but may co-exist with MaskTech eSign Applet on Secora™ ID S v1.1 on the same card. It is covered by another certification (NSCIB-CC-299277). Other (third-party) applets are not allowed by the side of MaskTech eSign Applet on Secora™ ID S v1.1 according to [AGD_eSign]

3.6.2 TOE Interfaces

The physical and logical interfaces of the TOE are as follows:

- The physical interface of the TOE is the entire surface of the IC.
- The contact based interface according to [ISO_7816-3].
- The RF interface for contactless communication according to [ISO_14443] Type B.
- The command interface for communication with the TOE provided by the SSCD Application.

3.6.3 Packaging

The applets provided by MaskTech International GmbH are packaged in cap-files to be used on modules according to [SECORA_ST-SLJ52], section '1.4.3 TOE package types'. The cap files can be delivered to the customer in three ways:

- The cap-files are pre-loaded onto the chips by the IC manufacturer Infineon Technologies AG. In this case the cap-files are transferred to Infineon Technologies AG using their proprietary certified delivery procedures.
- The cap-files are loaded onto the chips by MaskTech International GmbH.
- The cap-files are loaded onto the chips by the customer. In this case cap-files are transfered to the customer electronically using the certified delivery procedures of MaskTech International GmbH (encrypted, signed). Cap-file installation is explained in [AGD_eSign], chapter "Applet Installation". The guidance in PDF-format can be downloaded by the customer from the MaskTech web site.

3.6.4 TOE Life Cycle

3.6.4.1 General

The TOE life cycle distinguishes stages for development, production, preparation and operational use.

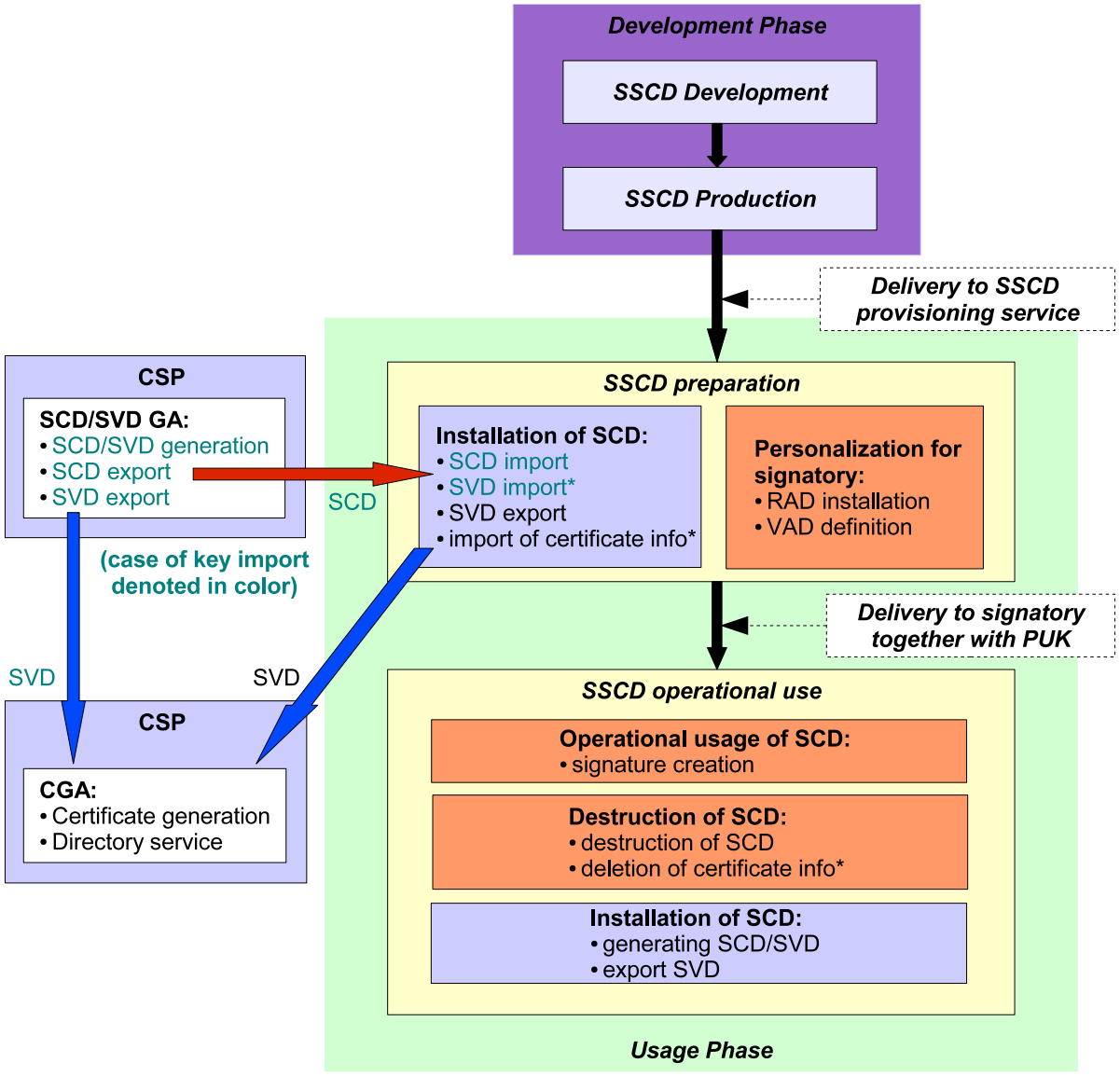

Figure 3.3: TOE life cycle; the asterisks * marks the optional import of the SVD and certificate info during TOE preparation and certificate info deletion when SCD is destroyed.

The development phase comprises the development and production of the TOE. The steps are in detail:

Development

- Infineon Technologies AG develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

- Infineon Technologies AG in the role of the software developer [20] uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (Secora™ ID S v1.1 Java Card operating system).
- MaskTech International GmbH in the role of the software developer develops the SSCD applet (MaskTech eSign Applet on Secora™ ID S v1.1) and the guidance documentation associated with this TOE component.

Production

- Manufacturing of the chip (IC/dedicated software/embedded software) by Infineon Technologies AG.
- Pre-personalization (loading of the eSign package) by Infineon Technologies AG, MaskTech International GmbH, Linxens (Thailand) Co Ltd. (former SMARTRAC TECHNOLOGY Ltd., see [SC_Linxens]), HID Global Ireland (see [SC_HID]) or HID Global Malaysia (see [SC_HID_MY]).

The steps of the development phase performed by MaskTech International GmbH, i.e. the development of the SSCD applet and the Pre-personalization (loading of the eSign package) are subject of the evaluation according to the assurance life cycle (ALC) class. The steps performed by Infineon Technologies AG are evaluated within the certification of the platform ([SECORA_ST-SLJ52]). The development phase ends with the delivery of the TOE to the SSCD-provisioning service.

The operational usage of the TOE comprises the preparation stage and the operational use stage. In the preparation stage the personal information of the legitimate user is written and, optionally, one or more SCD/SVD pairs are generated and the according certificates stored on the card. In the preparation stage SCD/SVD pairs may also be imported to the card by the SSCD-provisioning service. The TOE operational use stage begins when the signatory has obtained both the PUK value and the TOE. Enabling the TOE for signing requires at least one set of SCD stored in its memory.[21]

The life cycle (Fig. 3.3) allows the generation of an SCD/SVD pair before as well as after the delivery to the signatory.

3.6.4.2 Preparation Stage

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.

[20] Note that in this ST the role software developer of the protection profile is subdivided into two separate roles: The operating system is developed by the OS software developer (Java Card, Infineon Technologies AG), and the application by the Java Card applet developer (SSCD, MaskTech International GmbH).

[21] Note that according to *PP SSCD KG* the operational use stage begins before the preparation stage ends, because the signatory must enable the SCD for use (by setting the VAD) after receiving the TOE and the PUK.

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

CGA a) Initialize the security functions in the TOE for the identification as SSCD, for the proof of this SSCD identity to external entities, and for the protected export of the SVD (required by *PP SSCD KG TCCGA*).

CGA b) Links the identity of the TOE as SSCD and the identity of the legitimate user as potential applicant for certificates for SVD generated by the TOE (required by *PP SSCD KG TCCGA*).

c) 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.

d) Set a PUK to enable the legitimate user to activate the RAD and prepare information about the PUK value for delivery to the legitimate user.

KI e) In the case of **key import**: The initialization of the TOE, i.e. the CSP generates the SCD/SVD pair by means of a SCD/SVD generation device, loads the SCD to the TOE, and sends the SVD to the CGA. The TOE may import and store the SCD/SVD pair. The CSP ensures

   1) the correspondence between SCD and SVD,
   2) 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.

f) Optionally, generate a certificate for at least one SCD by (more details about the **SVD certification task** are given below):

   1) initializing security functions in the TOE for protected export of the SVD and obtaining a certificate for the SVD after receiving a protected request from the TOE.
   2) In the case of **key import**, the CSP is expected to first store the SCD in a SSCD before generating a (qualified) certificate. A secure channel with the TOE may be used to support this, by ensuring integrity of the SCD during transmission to the TOE.

g) Optionally, present certificate info to the SSCD.

h) Deliver the TOE and the accompanying PUK value info to the legitimate user.

The **SVD certification task** of an SSCD-provisioning service provider as specified in *PP SSCD KG* may support a centralized, 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 (cf. [DIR_1999/93/EC], 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 personalization.

Before initiating the actual certificate signature the CGA 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 personalized 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.

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

If the TOE is used for creation of qualified or 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. [DIR_1999/93/EC], article 2, clause 9).

N Preparation includes the installation of the applet loaded in the production phase. After the preparation of the product has been done, the Secora™ ID S v1.1 operating system is switched to its proprietary native mode which disables GP and identification commands to avoid tracking as well as loading/installation of 3rd party applets.

3.6.4.3 Operational Use Stage

In this life cycle stage the signatory can use the TOE to create qualified or advanced electronic signatures.

The TOE operational use stage begins when the signatory has obtained both the PUK and the TOE or, in the case of **key import**, when at least one SCD/SVD pair is generated by the CSP and the SCD is imported into the SSCD and the signatory takes control over the TOE and makes the SCD operational. Enabling the TOE for signing requires at least one set of SCD stored in its memory.

The signatory can also interact with the SSCD through a trusted channel[22] to perform management tasks, e.g. reset a RAD value or use counter if the PIN in the reference data has been lost or blocked.

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.

CGA In the usage phase, SCD/SVD generation by the TOE and SVD export from the TOE may take place in the preparation stage (by the SSCD-provisioning service provider) and/or in the operational use stage (usually by the signatory). The TOE provides a trusted channel[23] to the

[22] Trusted channel is optional with cards configured for contact-only interface (easy access).
[23] For contact-only based SSCDs trusted channel is only used if the CGA requests Chip Authentication.

CGA protecting the integrity of the SVD. The signatory may be allowed to choose some of the data in the certificate request for instance to use a pseudonym instead of the legal name in the certificate[24]. 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 in the operational use stage require additional security functions in the TOE and an interaction with the SSCD-provisioning service provider through a trusted channel[25]. Before generating the certificate including the SVD exported from the TOE, the CGA additionally establishes

a) the identity of the TOE as SSCD,
b) that the originating SSCD has been personalized for the applicant for the certificate as legitimate user, and
c) the correspondence between SCD stored in the SSCD and the received SVD.

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

[24] The certificate request in this case will contain the name of the signatory as the requester, as for instance it may be signed by the signatory's existing SCD.

[25] Trusted channel is optional with cards configured for contact-only interface (easy access).

4 Conformance Claims (ASE_CCL.1)

4.1 CC Conformance Claim

This ST is conforming to the Common Criteria version 3.1 Revision 5:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 [CC_Part1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 [CC_Part2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1 Revision 5, April 2017 [CC_Part3]

as follows

- Part 2 extended
- Part 3 conformant

The

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

has to be taken into account.

4.2 PP Claim, Package Claim

Strict conformance of this ST to the following Common Criteria protection profiles is claimed:

KG
- "Protection profiles for secure signature creation device – Part 2: Device with key generation", BSI-CC-PP-0059-2009-MA-02 [CC_PP-0059]

CGA
- "Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application", BSI-CC-PP-0071-2012-MA-01 [CC_PP-0071]

SCA
- "Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application", BSI-CC-PP-0072-2012-MA-01 [CC_PP-0072]

KI
- "Protection profiles for secure signature creation device – Part 3:Device with key import", BSI-CC-PP-0075-MA-01 [CC_PP-0075]

KI SCA
- "Protection profiles for secure signature creation device – Part 6:Extension for device with key import and trusted communication with signature creation application", BSI-CC-PP-0076-MA-01 [CC_PP-0076]

N There are various interface options of the TOE (contact, contactless, dual interface) that are decided and configured by the Personalization Agent during personalization. For contact-only TOEs (without contactless interface support) communication can be realized without establishment of trusted channels (aside from key import) covering only protection profiles *PP SSCD KG* and *PP SSCD KI*. Any configuration with contactless interface supports trusted channels covering all mentioned protection profiles (*PP SSCD KG*, *PP SSCD KG TCSCA*, *PP SSCD KG TCCGA*, *PP SSCD KI*, and *PP SSCD KI TCSCA*.

This ST is conforming to assurance package EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [CC_Part3].

4.3 Conformance Rationale

KI This ST claims strict conformance to *PP SSCD KG* and *PP SSCD KI*. This implies for this ST:

a) The security problem definition (SPD) of this ST is described by the threats, organizational security policies and assumptions as for the TOE in both *PP SSCD KG* and *PP SSCD KI*. With the exception of assumption **A.CSP** specified in *PP SSCD KI* only, the threats, organizational security policies and assumptions are the same in both PPs.

b) The security objectives for the TOE include all security objectives of both *PP SSCD KG* and *PP SSCD KI*. The security objectives that are generated by the TOE itself or imported from the operational environment are identical in both PPs (i.e. OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_ Design, OT.Tamper_ID and OT.Tamper_Resistance). *PP SSCD KG* defines the security objectives for the TOE:
   1) OT.SCD/SVD_Auth_gen
   2) OT.SCD_Unique
   3) OT.SCD_SVD_Corresp

   PP SSCD KI defines the analogous security objectives for the operational environment:
   1) OE.SCD/SVD_Auth_gen
   2) OE.SCD_Unique
   3) OE.SCD_SVD_Corresp

   Furthermore, *PP SSCD KI* defines OT.SCD_Auth_Imp that is related to SCD import only.

c) The security functional requirements (SFRs) for the TOE include all SFRs of both *PP SSCD KG* and *PP SSCD KI*. The SFRs that are not defined in both PPs, but only in *PP SSCD KG* are:
   1) FCS_CKM.1 (Cryptographic key generation)

2) FDP_ACC.1/SCD/SVD_Generation (Subset access control)
3) FDP_AFC.1/SCD/SVD_Generation (Security attribute based access control)
4) FDP_ACC.1/SVD_Transfer (Subset access control)
5) FDP_AFC.1/SVD_Transfer (Security attribute based access control)

The SFRs that are defined only in *PP SSCD KI* are:

1) FDP_ACC.1/SCD_Import (Subset access control)
2) FDP_AFC.1/SCD_Import (Security attribute based access control)
3) FDP_UCT.1/SCD (Basic data exchange confidentiality)
4) FTP_ITC.1/SCD (Inter-TSF trusted channel)
5) FDP_ITC.1/SCD (Import of user data without security attributes)

The SFR FMT_MSA.3 (Static attribute initialization) is defined in both *PP SSCD KG* and *PP SSCD KI*, but differ in the scope of FMT_MSA.3.1 (*PP SSCD KG* requires the enforcement of SCD/SVD_Generation_SFP, SVD_Transfer_SFP and Signature_Creation_SFP; *PP SSCD KI* requires the enforcement of SCD_Import_SFP and Signature_Creation_SFP). In this ST FMT_MSA.3 has been **refined** to cover the scope of both *PP SSCD KG* and *PP SSCD KI*. The SFR FMT_MSA.4 (Security attribute value inheritance) is defined in both *PP SSCD KG* and *PP SSCD KI*, but differ in the definition of the rules. FMT_MSA.4 as defined in *PP SSCD KI* is therefore included in this ST as iteration FMT_MSA.4/KI.

d) The SARs specified in *PP SSCD KG* and *PP SSCD KI* are identical.

This ST claims conformance to *PP SSCD KG*, *PP SSCD KG TCCGA* and *PP SSCD KG TCSCA*.

CGA

This implies for this ST:

SCA

a) The security problem definition (SPD) for *PP SSCD KG*, *PP SSCD KG TCCGA* and *PP SSCD KG TCSCA* are described by the same threats, organizational security policies and assumptions.

b) The security objectives for the TOE include all the security objectives for the TOE of *PP SSCD KG* and in addition:

1) OT.TOE_SSCD_Auth (Authentication proof as SSCD) defined in *PP SSCD KG TCCGA*
2) OT.TOE_TC_SVD_Exp (Trusted channel for SVD) defined in *PP SSCD KG TCCGA*
3) OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import) defined in *PP SSCD KG TCSCA*
4) OT.TOE_TC_DTBS_Imp (Trusted channel for DTBS) defined in *PP SSCD KG TCSCA*

c) The security objectives for the operational environment include all the security objectives for the TOE of *PP SSCD KG* and in addition:

1) OE.CGA_SSCD_Auth (Pre-initialization of the TOE for SSCD authentication) defined in *PP SSCD KG TCCGA*
2) OE.CGA_TC_SVD_Imp (CGA trusted channel for SVD import) defined in *PP SSCD KG TCCGA*

Furthermore, the following modifications are performed:

1) *PP SSCD KG TCCGA* substitutes OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD-provisioning service) by OE.Dev_Prov_Service.
2) *PP SSCD KG TCSCA* substitutes OE.HID_VAD by OE.HID_TC_VAD_Exp (to support the security objective for the TOE OT.TOE_TC_VAD_Imp)

3) *PP SSCD KG TCSCA* substitutes OE.DTBS_Protect by OE.SCA_TC_DTBS_Exp (to support the security objective for the TOE OT.TOE_TC_DTBS_Imp)

d) The security functional requirements (SFRs) for the TOE include all SFRs of *PP SSCD KG* and in addition:
   1) FIA_API.1 (Authentication Proof of Identity) specified in *PP SSCD KG TCCGA*
   2) FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor) specified in *PP SSCD KG TCCGA*
   3) FTP_ITC.1/SVD (Inter-TSF trusted channel) specified in *PP SSCD KG TCCGA*
   4) FDP_UIT.1/DTBS (Data exchange integrity) specified in *PP SSCD KG TCSCA*
   5) FTP_ITC.1/VAD (Inter-TSF trusted channel – TC Human Interface Device) specified in *PP SSCD KG TCSCA*
   6) FTP_ITC.1/DTBS (Inter-TSF trusted channel – Signature creation Application) specified in *PP SSCD KG TCSCA*

e) *PP SSCD KG TCCGA* provides operation of the SFR FIA_UAU.1 of *PP SSCD KG*.

f) *PP SSCD KG TCSCA* provides refinements for the SFR FIA_UAU.1 of *PP SSCD KG*.

g) The SARs specified in *PP SSCD KG*, *PP SSCD KG TCCGA* and *PP SSCD KG TCSCA* are identical.

KI SCA

This ST claims conformanceto *PP SSCD KI* and *PP SSCD KI TCSCA*. This implies for this ST[1]:

a) The security problem definition (SPD) for *PP SSCD KI* and *PP SSCD KI TCSCA* are described by the same threats, organizational security policies and assumptions.

b) The security objectives for the TOE include all the security objectives for the TOE of *PP SSCD KI* and in addition:
   1) OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import)
   2) OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import)
   3) OT.TOE_TC_DTBS_Imp (Trusted channel for DTBS)

c) The security objectives for the operational environment include all the security objectives for the TOE of *PP SSCD KI* except the following modifications: Furthermore, the following modifications are performed:
   1) OE.HID_VAD is substituted by OE.HID_TC_VAD_Exp (to support the security objective for the TOE OT.TOE_TC_VAD_Imp)
   2) OE.DTBS_Protect is substituted by OE.SCA_TC_DTBS_Exp (to support the security objective for the TOE OT.TOE_TC_DTBS_Imp)

d) The security functional requirements (SFRs) for the TOE include all SFRs of *PP SSCD KI* and in addition:
   1) FDP_UIT.1/DTBS (Data exchange integrity)
   2) FTP_ITC.1/VAD (Inter-TSF trusted channel – TC Human Interface Device)
   3) FTP_ITC.1/DTBS (Inter-TSF trusted channel – Signature creation Application)

e) *PP SSCD KI TCSCA* provides refinements for the SFR FIA_UAU.1 of *PP SSCD KI*.

f) The SARs specified in *PP SSCD KI* and *PP SSCD KI TCSCA* are identical.

[1]These implications are analogous to the implications resulting from the conformance of *PP SSCD KG TCSCA* to *PP SSCD KG*. Therefore, the security objectives and security functional requirement specified in *PP SSCD KI TCSCA* and *PP SSCD KG TCSCA* are identical and valid for both **key generation** and **key import**.

4.4 PP Additions

Password Authenticated Connection Establishment (PACE) and *Extended Access Control Version 1* (EACv1) (i.e. *Chip Authentication Version 1* (CAv1) and *Terminal Authentication Version 1* (TAv1)) functionality to provide a secure authentication protocol and a secure channel for the communication with authorized terminals in phase *usage/operational* has been added. This implies the following augmentations, which are adapted from protection profiles [CC_PP-0056-V2] and [CC_PP-0068-V2]:

1) FCS_CKM.1/DH_PACE
2) FCS_CKM.1/CA
3) FCS_COP.1/CA_ENC
4) FCS_COP.1/CA_MAC
5) FCS_COP.1/SIG_VER
6) FCS_COP.1/PACE_ENC
7) FCS_COP.1/PACE_MAC
8) FCS_RND.1
9) FDP_ACC.1/TRM
10) FDP_ACF.1/TRM
11) FIA_UID.1 (the existing SFR has been extended)
12) FIA_UAU.4/PACE
13) FIA_UAU.5/PACE
14) FIA_UAU.6
15) FMT_MTD.1/CVCA_UPD
16) FMT_MTD.1/DATE
17) FMT_MTD.1/KEY_READ
18) FPT_EMS.1/KEYS

ECC key generation in order to create the Chip Authentication key pair has been taken into account by adding the SFR:

19) FCS_CKM.1/CA_STATIC

Additional protection against attacks against the RAD is addressed by

21) FIA_AFL.1/Suspend_PIN
22) FIA_AFL.1/Block_PIN

taken from protection profile [CC_PP-0086].

The SFRs

23) FDP_ACC.1/Signature_Creation/N-QES
24) FDP_ACF.1/Signature_Creation/N-QES

are added as iterations of the SFRs FDP_ACC.1/Signature_Creation and FDP_ACF.1/ Signature_Creation to address the different authentication requirement for non-qualified electronic signature creation.

The SFRs

24) FMT_MSA.1/Admin_KG
25) FMT_MSA.1/Admin_KI

are added as refinements of the SFRs FMT_MSA.1/Admin from *PP SSCD KG* and *PP SSCD KI* respectively to avoid naming collision.

Table 9.2 takes the dependencies of the SFRs into account.

Some SFRs as defined in *PP SSCD KG* have been renamed to avoid mistakes with the newly added SFRs listed above. These are:

SFR in *PP SSCD KG*	**SFR in this ST**
FCS_CKM.1	FCS_CKM.1/SCD
FCS_COP.1	FCS_COP.1/SCD
FIA_AFL.1	FIA_AFL.1/RAD
FPT_EMS.1	FPT_EMS.1/SSCD

5 Security Problem Definition (ASE_SPD.1)

5.1 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

a) SCD: private key used to perform an electronic signature operation. The confidentiality, integrity and signatory’s sole control over the use of the SCD shall be maintained.
b) SVD: public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported shall be maintained.
c) DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature shall be maintained.

PACE
EAC

Secondary assets taken from [CC_PP-0056-V2] respectively [CC_PP-0068-V2]

a) Accessibility to the TOE functions and data only for authorized subjects: property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorized subjects only.
b) TOE internal secret cryptographic keys: permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality. The confidentiality and integrity of the cryptographic keys must be maintained.
c) TOE internal non-secret cryptographic material: permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SO_D containing digital signature) used by the TOE in order to enforce its security functionality. The integrity and authenticity of the non-secret cryptographic material must be maintained.

Users and subjects acting for users

a) 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.

b) Administrator: user who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.
c) 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.

EAC **Subject referring the EACv1 functionality adapted from [CC_PP-0056-V2]**

1. Certification Service Provider (corresponding to “Country Verifying Certification Authority” in [CC_PP-0056-V2], which does not exist within the SSCD-context)
2. Document Verifier
3. Legitimate Terminal (CGA and SCA) (corresponding to “Domestic Extended Inspection System” in [CC_PP-0056-V2], which does not exist within the SSCD-context)

Threat agents

a) 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 a high attack potential and knows no secret.

5.2 Threats

5.2.1 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.

5.2.2 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.

5.2.3 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.

5.2.4 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.

5.2.5 T.SigF_Misuse *Misuse of the signature creation function of the TOE*

An attacker misuses the signature creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

5.2.6 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.

5.2.7 T.Sig_Forgery *Forgery of the electronic signature*

An attacker forges a signed data object, maybe using an electronic signature that has been created by the TOE, and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

5.3 Organizational Security Policies

5.3.1 P.CSP_QCert *Qualified certificate*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. **the directive**, article 2, clause 9, and Annex I) for the SVD generated by the SSCD. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

5.3.2 P.QSign *Qualified electronic signatures*

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. **the directive**, article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to **the directive** Annex I)[1]. 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 an 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.

[1] It is a non-qualified advanced electronic signature if it is based on a non-qualified certificate for the SVD.

5.3.3 P.Sigy_SSCD *TOE as secure signature creation device*

The TOE meets the requirements for an SSCD laid down in Annex III of **the directive** [DIR_1999/93/EC]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

5.3.4 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.

5.4 Assumptions

5.4.1 A.CGA *Trustworthy certification generation application*

The CGA protects the authenticity of the signatory's name or pseudonym and the SVD in the (qualified) certificate by a qualified electronic signature of the CSP.

5.4.2 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.

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

KI

The CSP uses only a trustworthy SCD/SVD generation device and ensures that this device can be used by authorized 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.

6 Security Objectives (ASE_OBJ.2)

6.1 Security Objectives for the TOE

6.1.1 Relation between the Claimed PPs

For relation between *PP SSCD KG*, *PP SSCD KG TCCGA* and *PP SSCD KG TCSCA* as well as *PP SSCD KI* and *PP SSCD KI TCSCA* see section Conformance rationale on page 28.

6.1.2 OT.Lifecycle_Security *Life cycle security*

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

Note 2: The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation or repeated 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.

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

KG

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

6.1.4 OT.SCD_Auth_Imp *Authorized SCD import*

KI

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

6.1.5 OT.SCD_Unique *Uniqueness of the signature creation data*

KG

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation shall practically occur only once and shall not be reconstructable from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible.

6.1.6 OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*

KG

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD.

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

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

Note 3: The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation or SCD import signature creation operation, storage and secure destruction.

6.1.8 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.

6.1.9 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.

6.1.10 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.

6.1.11 OT.EMSEC_Design *Provide physical emanation security*

The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

6.1.12 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.

6.1.13 OT.Tamper_Resistance *Tamper resistance*

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

6.1.14 OT.TOE_SSCD_Auth *Authentication proof as SSCD*

CGA

The TOE shall hold unique identity and authentication data as SSCD and provide security mechanisms to identify and to authenticate itself as SSCD.

6.1.15 OT.TOE_TC_SVD_Exp *TOE trusted channel for SVD export*

CGA

The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the TOE.

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

SCA

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

Note 4: This security objective for the TOE is partly covering OE.HID_VAD from the core *PP SSCD KG*. While OE.HID_VAD in *PP SSCD KG* requires only the operational environment to protect VAD, *PP SSCD KG TCSCA* requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore *PP SSCD KG TCSCA* re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

6.1.17 OT.TOE_TC_DTBS_Imp *Trusted channel for DTBS*

SCA

The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE shall not generate electronic signatures with the SCD for altered DTBS.

Note 5: This security objective for the TOE is partly covering OE.DTBS_Protect from the core *PP SSCD KG*. While OE.DTBS_Protect in *PP SSCD KG* requires only the operational environment to protect DTBS, *PP SSCD KG TCSCA* requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore *PP SSCD KG TCSCA* re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

6.2 Security Objectives for the Operational Environment

6.2.1 Relation between the Claimed PPs

For relation between *PP SSCD KG*, *PP SSCD KG TCCGA* and *PP SSCD KG TCSCA* as well as *PP SSCD KI* and *PP SSCD KI TCSCA* see section Conformance rationale on page 28.

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

KI

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

6.2.3 OE.SCD_Secrecy *SCD Secrecy*

KI

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.

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

KI

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.

6.2.5 OE.SCD_SVD_Corresp *Correspondence between SVD and SCD*

KI

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.

6.2.6 OE.SVD_Auth *Authenticity of the SVD*

The operational environment shall ensure the integrity or, in the case of **key import**, 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.

6.2.7 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 qualified 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.

6.2.8 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.

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

The signatory shall use a trustworthy SCA that

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

Note 6: The SCA should be able to support advanced electronic signatures. Currently, there are three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CAdES, XAdES and PAdES. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.

6.2.10 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.

6.2.11 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.

6.2.12 OE.SSCD_Prov_Service *Authentic SSCD provided by SSCD-provisioning service*

CGA

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.

6.2.13 OE.Dev_Prov_Service *Authentic SSCD provided by SSCD-Provisioning Service*

CGA

The SSCD-Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, personalizes the TOE for the legitimate user as signatory, links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the signatory.

Note 7: This objective replaces OE.SSCD_Prov_Service from *PP SSCD KG*, which is possible as it does not imply any additional requirements for the operational environment when compared to OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_ Service).

6.2.14 OE.CGA_SSCD_Auth *Pre-initialization of the TOE for SSCD authentication*

CGA

The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSCD, successfully proved this identity as SSCD to the CGA, and whether this identity is linked to the legitimate holder of the device as applicant for the certificate.

6.2.15 OE.CGA_TC_SVD_Imp *CGA trusted channel for SVD import*

CGA

The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the SSCD.

The developer prepares the TOE by pre-initialization for the delivery to the customer (i.e. the SSCD-Provisioning Service) in the development phase not addressed by a security objective for the operational environment. The SSCD-Provisioning Service performs initialization and personalization as TOE for the legitimate user (i.e. the Device Holder). If the TOE is delivered to the Device Holder with SCD the TOE is an SSCD. This situation is addressed by OE.SSCD_Prov_Service except the additional initialization of the TOE for proof as SSCD and trusted channel to the CGA. If the TOE is delivered to the Device Holder without an SCD the TOE will be an SSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the Signatory in the operational use stage the TOE provides additional security functionality addressed by OT.TOE_SSCD_Auth and OT.TOE_TC_ SVD_Exp. But this security functionality shall be initialized by the SSCD-Provisioning Service as described in OE.Dev_Prov_Service. Therefore *PP SSCD KG TCCGA* substitutes OE.SSCD_Prov_Service by OE.Dev_Prov_Service allowing generation of the first SCD/SVD pair after delivery of the TOE to the Device Holder and requiring initialization of security functionality of the TOE. Nevertheless the additional security functionality shall be used by the operational environment as described in OE.CGA_SSCD_Auth and OE.CGA_TC_ SVD_Imp. This approach does not weaken the security objectives of and requirements to the TOE but enforce more security functionality of the TOE for additional method of use. Therefore it does not conflict with the CC conformance claim to the core *PP SSCD KG*.

6.2.16 OE.HID_TC_VAD_Exp *Trusted channel of HID for VAD export*

SCA

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

Note 8: This security objective for the TOE is partly covering OE.HID_VAD from the core *PP SSCD KG* or *PP SSCD KI*. While OE.HID_VAD in *PP SSCD KG* or *PP SSCD KI* require only the operational environment to protect VAD, *PP SSCD KG TCSCA* and *PP SSCD KI TCSCA* require the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore *PP SSCD KG TCSCA* and *PP SSCD KI TCSCA* re-assign partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

6.2.17 OE.SCA_TC_DTBS_Exp *Trusted channel of SCA for DTBS export*

SCA

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

Note 9: This security objective for the TOE is partly covering OE.DTBS_Protect from the core *PP SSCD KG*. While OE.DTBS_Protect in *PP SSCD KG* or *PP SSCD KI* requires only the operational environment to protect DTBS, *PP SSCD KG TCSCA* and *PP SSCD KI TCSCA* require the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore *PP SSCD KG TCSCA* and *PP SSCD KI TCSCA* re-assign partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

6.3 Security Objective Rationale

6.3.1 Security Objectives Backtracking

The following tables show how the security objectives for the TOE (table 6.1) and the security objectives for the operational environment(table 6.2) cover the threats, organizational security policies and assumptions.

Security objectives that are added by *PP SSCD KI*, *PP SSCD KI TCSCA*, *PP SSCD KG TCCGA* or *PP SSCD KG TCSCA*, as well as assumption A.CSP added by *PP SSCD KI*, are color coded for better readability.

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

Table 6.1: Mapping of security problem definition to security objectives of the TOE (assumptions are mapped in table 6.2)

	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.Dev_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.CGA_SSCD_Auth	OE.CGA_TC_SVD_Imp	OE.HID_TC_VAD_Exp	OE.SCA_TC_DTBS_Exp
T.SCD_Divulg	x	x														
T.SCD_Derive			x													
T.Hack_Phys																
T.SVD_Forgery				x		x								x		
T.SigF_Misuse									x	x	x	x			x	x
T.DTBS_Forgery										x	x					x
T.Sig_Forgery			x		x											
P.CSP_QCert	x			x	x								x			
P.QSign					x					x						
P.Sigy_SSCD	x	x	x				x	x					x	x		
P.Sig_Non-Repud		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 6.2: Mapping of security problem definition to security objectives

6.3.2 Security Objectives Sufficiency

Countering of threats by security objectives:

T.SCD_Divulg *(Storing, copying and releasing of the signature creation data)* addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in **the directive** [DIR_1999/93/EC], recital (18). This threat is countered by

KI
- 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

KI
- OE.SCD/SVD_Auth_Gen, which ensures that only authorized SCD generation in the environment is possible, and

KI
- OT.SCD_Auth_Imp, which ensures that only authorized 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.

KG
- OT.SCD/SVD_Auth_Gen and/or
- OE.SCD_Unique counters this threat by implementing cryptographically secure gen-

KI eration of the SCD/SVD pair.
- OT.Sig_Secure ensures cryptographically secure electronic signatures.

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

- OT.SCD_Secrecy preserves the secrecy of the SCD.
- OT.EMSEC_Design counters physical attacks through the TOE interfaces and observation of TOE emanations.
- OT.Tamper_ID and
- OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tampering attacks.

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

KI
- OE.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD in the case of **key import**, or

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

- OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA (in the case of **key generation**) or ensures the authenticity of the SVD given to the CGA of the CSP in the case of **key import**. It ensures verification of the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

CGA Additionally T.SVD_Forgery is addressed by

- OT.TOE_TC_SVD_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by
- OE.CGA_TC_SVD_Imp, which provides verification of SVD authenticity by the CGA.

T.SigF_Misuse *(Misuse of the signature creation function of the TOE)* addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create SDO for data for which the signatory has not decided to sign, as required by **the directive** [DIR_1999/93/EC], Annex III, paragraph 1, literal (c).

- OT.Lifecycle_Security requires the TOE to detect flaws during the initialization, personalization and operational usage including secure destruction of the SCD on demand of the signatory.
- OT.Sigy_SigF ensures that the TOE provides the signature creation function for the legitimate signatory only.
- OE.DTBS_Intend 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 prevents the DTBS/R from alteration inside the TOE.
- OE.Signatory ensures that the signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD and also ensures that the signatory keeps their VAD confidential.

SCA The combination of

- OT.TOE_TC_DTBS_Imp and
- OE.SCA_TC_DTBS_Exp counters the undetected manipulation of the DTBS during the transmission form the SCA to the TOE.

If the SCA provides a human interface for user authentication, OE.HID_TC_VAD_Exp requires the HID to protect the confidentiality and the integrity of the VAD as needed by the authentication method employed. The HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to

- OE.HID_TC_VAD_Exp and
- OT.TOE_TC_VAD_Imp.

T.DTBS_Forgery *(Forgery of the DTBS/R)* addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signatory has expressed its intent to sign.

The TOE IT environment addresses T.DTBS_Forgery by the means of

- OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and
- 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.

SCA The threat T.DTBS_Forgery is addressed by the security objectives

- OT.TOE_TC_DTBS_Imp and
- OE.SCA_TC_DTBS_Exp that ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE.

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

- OT.Sig_Secure,
- OT.SCD_Unique and
- OE.CGA_QCert address this threat in general.

KG
- OT.Sig_Secure ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together.

KG
- OT.SCD_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance.
- OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

KI In the case of **key import** the following objectives for the operational environment replace the corresponding objectives for the TOE:

- OE.Sig_Secure replaces OT.Sig_Secure and ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together.
- OE.SCD_Unique replaces OT.SCD_Unique and ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance.

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 initialization, personalization and operational usage,
- OT.SCD_SVD_Corresp, which requires 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.

KI In the case of **key import** P.CSP_QCert is also addressed by:

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

CGA According to:

- OT.TOE_SSCD_Auth the copies of the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD to prove this identity as SSCD to the CGA.
- OE.CGA_SSCD_Auth ensures that the CSP checks the proof of the device presented of the applicant that it is an SSCD.

P.QSign *(Qualified electronic signatures)* provides that the TOE and the SCA may be employed to sign data with a qualified 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 III of **the directive** [DIR_1999/93/EC]. This is ensured as follows:

Paragraph 1(a) of the directive, Annex III requires that the SCD used for signature creation can practically occur only once; this is ensured by:

KG
- OT.SCD_Unique or

KI
- OE.SCD_Unique in the case of **key import**

Paragraph 1(a) of the directive, Annex III requires to ensure the secrecy of the SCD; this is ensured by:

KG
- OT.SCD_Unique or

KI
- OE.SCD_Unique in the case of **key import**,
- OT.SCD_Secrecy and

KG
- OT.Sig_Secure or

KI
- OE.SCD_Secrecy in the case of **key import**
- OT.EMSEC_ Design and
- OT.Tamper_Resistance address specific objectives to ensure secrecy of the SCD against specific attacks.

Paragraph 1(b) of the directive, Annex III requires to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE; this is ensured by:

- OT.SCD_Secrecy and
- OT.Sig_Secure.

Paragraph 1(c) of the directive, Annex III requires to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others; this is ensured by:

- OT.Sigy_SigF and

KI
- OE.SCD_Secrecy in the case of **key import**

Paragraph 2 of the directive, Annex III requires that the TOE shall not alter the DTBS/R; this is ensured by:

- OT.DTBS_Integrity_TOE.

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

- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialization, personalization and operational usage,

KG
- OT.SCD/SVD_Auth_Gen or

KI
- OE.SCD/SVD_Auth_Gen in the case of **key import**, which limits invocation of the generation of the SCD and the SVD to authorized users only

KI
- OT.SCD_Auth_Imp, which limits SCD import to authorized users only (**key import**),

KI
- 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 (**key import**). 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, initialized and personalized as SSCD from the SSCD-provisioning service.

CGA
- OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialized and personalized TOE from an SSCD-Provisioning Service through the TOE delivery procedure.

If the TOE implements SCD generated under control of the SSCD-Provisioning Service the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD in the operational phase he or she applies for the (qualified) certificate as the Device Holder and legitimate user of the TOE. The CSP will use the TOE security features to check whether the following requirements are fulfilled:

CGA • OE.CGA_SSCD_Auth (the device presented is an SSCD linked to the applicant) and

CGA • OE.CGA_TC_SVD_Imp (the received SVD is sent by this SSCD).

This is addressed by the TOE security features:

CGA • OT.TOE_SSCD_Auth and

CGA • OT.TOE_TC_SVD_Exp.

Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

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

- OE.SSCD_Prov_Service ensures that the signatory uses an authentic copy of the TOE, initialized and personalized for the signatory.

KI In the case of **key import** the following security objectives for the operational environment ensure the security of the SCD in the CSP environment:

- OE.SCD/SVD_Auth_Gen 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.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.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory.
- OE.SVD_Auth and
- OE.CGA_QCert require the environment to ensure the authenticity of the SVD as being exported by the TOE and used under sole control of the signatory.
- OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE.
- OT.SCD_Unique provides that the signatory's SCD can practically occur just once.

CGA • OE.CGA_SSCD_Auth requires that the verification whether the device presented by the applicant is an SSCD and

CGA • OE.CGA_TC_SVD_Imp requires that the received SVD is sent by the device holding the corresponding SCD.

This is addressed by the TOE security objectives

CGA • OT.TOE_SSCD_Auth and

CGA • OT.TOE_TC_SVD_Exp supported by

CGA
- OE.Dev_Prov_Service.
- OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD-Provisioning Service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD).
- OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory ensures that the signatory keeps their VAD confidential.

SCA
- OE.HID_TC_VAD_Exp and

SCA
- OT.TOE_TC_VAD_Imp protect the confidentiality of VAD during the transmission between the HID and TOE.

The following security objectives ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS.

- OE.DTBS_Intend,
- OT.DTBS_Integrity_TOE,
- OE.DTBS_Protect, or respectively

SCA
- OE.SCA_TC_DTBS_Exp and

SCA
- OT.TOE_TC_DTBS_Imp.
- OT.Sig_Secure requires robust cryptographic techniques to ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification.
- OT.Lifecycle_Security,
- OT.SCD_Secrecy,
- OT.EMSEC_Design,
- OT.Tamper_ID and
- OT.Tamper_Resistance protect the SCD against any compromise.

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 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 certification 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, which ensures the generation of qualified certificates, and by
- OE.SVD_Auth, which ensures the protection of the integrity and the verification of the authenticity in the case of **key import** of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

A.CSP *(Secure SCD/SVD management by CSP)* establishes several security aspects concerning handling of SCD and SVD by the CSP.

- OE.SCD/SVD_Auth_Gen addresses that the SCD/SVD generation device can only be used by authorized users.
- OE.SCD_Unique (addresses that the generated SCD is unique and cannot be derived by the SVD.
- OE.SCD_SVD_Corresp addresses that SCD and SVD correspond to each other.
- OE.SCD_Secrecy addresses 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.

7 Extended Components Definition (ASE_ECD.1)

This Security Target uses the following extended components:

FPT_EMS as defined in [CC_PP-0059],

FIA_API as defined in [CC_PP-0071] and

FCS_RND as defined in [CC_PP-0068-V2] (see also note 31).

No other components are used.

8 Security Requirements (ASE_REQ.2)

8.1 Security Functional Requirements

8.1.1 Use of Requirement Specifications

Common Criteria allow several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration*. Each of these operations is used in this ST.

A **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is either (i) denoted by the word "refinement" in **bold** text and the added or changed words are in bold text or (ii) included in text as **bold** text and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed or the removed words are simply striked through (e.g., like in ~~removed words~~).

A **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections filled in by the ST author are denoted as double-underlined text.

An **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing as underlined text denotes assignments, which have been made by the PP authors, and the original text of the component is given by a footnote. Assignments filled in by the ST author are denoted as double-underlined text.

An **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

8.1.2 Cryptographic Support (FCS)

KG

FCS_CKM.1/SCD	Cryptographic key generation – SCD
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/SCD	The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm RSA and specified cryptographic key sizes up to 2048 bit[1] that meet the following: [RFC_8017] **and** ECDSA and specified cryptographic key sizes 224/256/384/512(BP)/521(NIST) bit that meet the following: [BSI_TR-03111].

Note 10: The SFR also covers the generation of asymmetric key pairs to be used for decryption.

PACE

FCS_CKM.1/DH_PACE	**Cryptographic key generation – Diffie-Hellman for PACE session keys**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case. FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/ DH_PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to [BSI_TR-03111] and specified cryptographic key sizes 192/224/256/384/512(BP)/521(NIST) bits (ECDH), 112 bits (TDES) and 128/192/256 bits (AES) that meet the following: [ICAO_SAC].

Note 11: The TOE generates a shared secret value K with the terminal during the PACE protocol, see [ICAO_SAC]. The shared secret value K is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{Enc}) according to [ICAO_SAC] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Note 12: FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO_SAC].

Note 13: This SFR has been adapted from [CC_PP-0068-V2].

EAC

FCS_CKM.1/CA_STATIC	**Cryptographic key generation – ECC key pair generation for Chip Authentication**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/CA_STATIC	The TSF shall generate **cryptographic keys** in accordance with a specified cryptographic key generation algorithm ECC key pair and specified cryptographic key sizes 224 bit - 521 bit that meet the following: [BSI_TR-03111].

[1] Depending on the card configuration there may also be key sizes of 3072/4096 bit (CRT).

Note 14: This SFR has been added in order to create an ECC key pair to be used for Chip Authentication. It follows the SFR FCS_CKM.1/SCD (FCS_CKM.1 in BSI-CC-PP-0059), but revokes the refinement 'SCD/SVD pair'.

EAC

FCS_CKM.1/CA	Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH and specified cryptographic key sizes 112 bits (TDES) and 128/192/256 bits (AES) that meet the following: based on an ECDH protocol compliant to [BSI_TR-03111]

Note 15: FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [BSI_TR-03110-1].

Note 16: The TOE shall destroy any session keys in accordance with FCS_CKM.4 after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE session keys after generation of a Chip Authentication session keys and changing the Secure Messaging to the Chip Authentication session keys. (iv) The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.

Note 17: This SFR has been adapted from [CC_PP-0056-V2].

FCS_CKM.4	Cryptographic key destruction
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys with random values that meets the following: none.

Note 18: The cryptographic key SCD will be destroyed on demand of the signatory. The signatory may want to destruct the SCD stored in the SSCD e.g. after the qualified certificate for the corresponding SVD is not valid any more.

PACE
EAC

Note 19: The TOE shall destroy the PACE or CA session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any ses-

sion keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.

FCS_COP.1/SCD	Cryptographic operation – SCD
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/SCD	The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm RSASSA-PSS **and** raw RSA and cryptographic key sizes up to 2048 bit[2] that meet the following: [RFC_8017] **and** in accordance with a specified cryptographic algorithm RSA-PKCS1-v1_5 and cryptographic key sizes up to 2048 bit[3] that meet the following: [RFC_8017] **and** in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes 224/256/384/512/521 bit that meet the following: [BSI_TR-03111].

Note 20: The operations in the element FCS_COP.1.1 shall be appropriate for the SCD imported according to FTP_ICT.1/SCD.

EAC

FCS_COP.1/CA_ENC	Cryptographic operation – Symmetric encryption / decryption
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/CA_ENC	The TSF shall perform Secure Messaging - encryption and decryption in accordance with a specified cryptographic algorithm AES in CBC mode and cryptographic key sizes 128 bit, 192 bit and 256 bit **and** 3DES in CBC mode and cryptographic key sizes 112 bit that meet the following: compliant to [BSI_TR-03110-1].

Note 21: This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or AES) for Secure Messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA.

Note 22: This SFR has been adapted from [CC_PP-0056-V2].

[2]Depending on the card configuration there may also be key sizes of 3072/4096 bit (CRT).
[3]Depending on the card configuration there may also be key sizes of 3072/4096 bit (CRT).

N For personalization of the TOE the Secure Channel Protocol SCP03 specified in [GP_SCP03] of Global Platform ([GP]) is used with AES 256 bits key length and encryption compliant to [NIST_SP800-38A].

EAC

FCS_COP.1/CA_MAC	**Cryptographic operation – MAC**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/CA_MAC	The TSF shall perform secure messaging - message authentication code in accordance with a specified cryptographic algorithm CMAC-AES and cryptographic key sizes 128/192/256 bit **and** Retail-MAC and cryptographic key sizes 112 bit that meet the following: compliant to [ICAO_SAC].

Note 23: This SFR requires the TOE to implement the cryptographic primitive for Secure Messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication protocol version 1 according to the FCS_CKM.1/CA. Furthermore the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the authentication mechanism.

Note 24: This SFR has been adapted from [CC_PP-0056-V2].

N For personalization of the TOE the Secure Channel Protocol SCP03 specified in [GP_SCP03] of Global Platform ([GP]) is used with AES 256 bits key length and encryption compliant to [NIST_SP800-38A].

EAC

FCS_COP.1/SIG_VER	Cryptographic operation – Signature verification
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/SIG_VER	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm ECDSA with SHA-1/SHA-224/SHA-256/SHA-384/SHA-512 and cryptographic key sizes 192/224/256/384/512 bits that meet the following: compliant to [BSI_TR-03110-1].

Note 25: This SFR has been adapted from [CC_PP-0056-V2]. It applies only to configurations with Terminal Authentication (TA).

PACE

FCS_COP.1/PACE_ENC	Cryptographic operation – Encryption / decryption AES/3DES
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_ENC	The TSF shall perform Secure Messaging - encryption and decryption in accordance with the cryptographic algorithm AES in CBC mode and cryptographic key sizes 128, 192 and 256 bits **and** 3DES in CBC mode and cryptographic key sizes 112 bits that meet the following: compliant to [ICAO_SAC].

Note 26: This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for Secure Messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{Enc}).

Note 27: This SFR has been adapted from [CC_PP-0068-V2].

PACE

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

FCS_COP.1.1/PACE_MAC	The TSF shall perform Secure Messaging - message authentication code in accordance with a specified cryptographic algorithm CMAC and cryptographic key sizes 128/192/256 bit **and** Retail-MAC and cryptographic key sizes 112 bit that meet the following: compliant to [ICAO_SAC].

Note 28: This SFR requires the TOE to implement the cryptographic primitive for Secure Messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}).

Note 29: This SFR has been adapted from [CC_PP-0068-V2].

PACE
EAC

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 Class PTG.3 quality metric according to [BSI_AIS31].

Note 30: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

Note 31: This SFR has been adapted from [CC_PP-0068-V2] and changed according to [CC_PP-0084] (FCS_RNG.1) to meet [BSI_AIS31]. The naming 'FCS_RND.1' has been kept for consistence with the certification procedure for the MRTD application (BSI-DSZ-CC-NSCIB-CC-299277).

8.1.3 User Data Protection (FDP)

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

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	authorized not authorized
SCD	SCD Operational	no yes
SCD	SCD Identifier	arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

Table 8.1: Subjects and security attributes for access control

PACE

FDP_ACC.1/TRM	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/TRM	The TSF shall enforce the Access Control SFP on terminals gaining access to the User Data **and data stored in EF.SOD of the electronic document** and none.

Note 32: This SFR has been adapted from [CC_PP-0068-V2]. The term *logical travel document* has been changed to *electronic document*.

PACE

FDP_ACF.1/TRM	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/TRM	The TSF shall enforce the Access Control SFP to objects based on the following: 1) Subjects: a) **Legitimate Terminal** 2) Objects: a) **data stored in EF.DG14 and EF.SOD of the TOE**, b) **all TOE intrinsic secret cryptographic keys stored in the electronic document**. 3) Security attributes: a) **authorization of the Legitimate Terminal** 4) none
FDP_ACF.1.2/TRM	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 1) A **Legitimate Terminal** is allowed to read data objects from FDP_ACF.1/TRM according to [ICAO_SAC] after a successful PACE authentication as required by **FIA_UAU.1**.
FDP_ACF.1.3/TRM	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none

FDP_ACF.1.4/TRM	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: 1) Any terminal being not authenticated as **Legitimate Terminal** is not allowed to read, to write, to modify, to use any User Data stored on the electronic document. 2) Terminals not using Secure Messaging are not allowed to read, to write, to modify, to use any data stored on the electronic document. 3) none

Note 33: This SFR has been adapted from [CC_PP-0068-V2]. The term *travel document* has been changed to *electronic document*, *BIS-PACE* has been changed to *Legitimate Terminal*.

KG

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.

KG

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 "authorized" is allowed to generate SCD/SVD pair. **Refinement: S.User is allowed to generate SCD/SVD pair after a successful PACE authentication using the PUK as the shared password.**
FDP_ACF.1.3/ SCD/SVD_Generation	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

KG

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.

KG

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 initialization
FDP_ACF.1.1/ SVD_Transfer	The TSF shall enforce the SVD_Transfer_SFP to objects based on the following: 1) the S.User is associated with the security attribute Role, 2) the SVD.
FDP_ACF.1.2/ SVD_Transfer	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Admin and R.Sigy **are** allowed to export SVD.
FDP_ACF.1.3/ SVD_Transfer	The TSF shall explicitly authorize 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

KI

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, SVD, 3) operations: import of SCD.

KI

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 initialization
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 "authorized" is allowed to import SCD. **Refinement for the configurations with Terminal Authentication (TA): S.User with security attribute "SCD/SVD Management" set to "authorized" (PACE PUK) is allowed to import SCD after a successful Terminal Authentication.**[4]
FDP_ACF.1.3/ SCD_Import	The TSF shall explicitly authorize 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 authorized" is not allowed to import SCD.

FDP_ACC.1/ Signature_Creation	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ Signature_Creation	The TSF shall enforce the Signature_Creation_SFP on 1) subjects: S.User, 2) objects: DTBS/R, SCD, 3) operations: signature creation.

FDP_ACF.1/ Signature_Creation	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

[4] Contact-only based SSCDs do not support Terminal Authentication and PACE. In this case Global PUK and Chip Authentication are used.

FDP_ACF.1.1/ Signature_Creation	The TSF shall enforce the Signature_Creation_SFP to objects based on the following: 1) the 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" . **Refinement for the configurations with Terminal Authentication (TA): R.Sigy is allowed to create qualified electronic signatures for DTBS/R with SCD after successful Terminal Authentication and successful authentication against RAD[5].**
FDP_ACF.1.3/ Signature_Creation	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ Signature_Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no" .

FDP_ACC.1/ Signature_Creation/ N-QES	**Subset access control – Non-qualified electronic signature**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ Signature_Creation/ N-QES	The TSF shall enforce the Signature_Creation_SFP on 1) subjects: S.User, 2) objects: DTBS/R, SCD, 3) operations: signature creation.

FDP_ACF.1/ Signature_Creation/ N-QES	**Security attribute based access control – Non-qualified electronic signature**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

[5] Contact-only based SSCDs do not support Terminal Authentication.

FDP_ACF.1.1/ Signature_Creation/ N-QES	The TSF shall enforce the Signature_Creation_SFP to objects based on the following: 1) the 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/ N-QES	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/ N-QES	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ Signature_Creation/ N-QES	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" .

KI

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 initialization
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 ~~user data~~ **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.

KI

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 ~~user data~~ **SCD** in a manner protected from unauthorized disclosure.

SCA

FDP_UIT.1/DTBS	Data exchange integrity
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FDP_UIT.1.1/DTBS	The TSF shall enforce the Signature_Creation_SFP to receive user data in a manner protected from modification and insertion errors.
FDP_UIT.1.2/DTBS	The TSF shall be able to determine on receipt of user data, whether modification and insertion has occurred.

FDP_RIP.1	Subset residual information protection
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from the following objects: SCD.

The following data persistently stored by the TOE shall have the user data attribute “integrity checked persistent stored data”:

1) SCD
2) SVD (if persistently stored by the TOE).

The DTBS/R temporarily stored by the TOE has the user data attribute “integrity checked stored data”:

FDP_SDI.2/Persistent	Stored data integrity monitoring and action
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
Dependencies:	No dependencies.
FDP_SDI.2.1/Persistent	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored data.
FDP_SDI.2.2/Persistent	Upon detection of a data integrity error, the TSF shall 1) prohibit the use of the altered data, 2) inform the S.Sigy about integrity error.

FDP_SDI.2/DTBS	Stored data integrity monitoring and action
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
Dependencies:	No dependencies.
FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored DTBS.
FDP_SDI.2.2/DTBS	Upon detection of a data integrity error, the TSF shall 1) prohibit the use of the altered data, 2) inform the S.Sigy about integrity error.

Note 34: 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).

CGA

FDP_DAU.2/SVD	Data authentication with identity of guarantor
Hierarchical to:	FDP_DAU.1 Basic data authentication.
Dependencies:	FIA_UID.1 Timing of identification.
FDP_DAU.2.1/SVD	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of SVD.
FDP_DAU.2.2/SVD	The TSF shall provide CGA with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

8.1.4 Identification and Authentication (FIA)

PACE
EAC

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) to establish the communication channel 3) carrying out the PACE Protocol according to [ICAO_SAC] 4) to read the initialization data in phase “Usage/Preparation” 5) to read the random identifier in phase “Usage/Preparation” 6) to carry out the Chip Authentication protocol v.1 according to [BSI_TR-03110-1] 7) to carry out the Terminal Authentication protocol v.1 according to [BSI_TR-03110-1] 8) none on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Note 35: This SFR has been amended with items from [CC_PP-0056-V2]. Item (7) of FIA_UID.1.1 applies only to configurations with Terminal Authentication (TA).

CGA
SCA

FIA_UAU.1	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1	The TSF shall allow: 1) self-test according to FPT_TST.1 2) identification of the user by means of TSF required by FIA_UID.1 3) establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD, 4) establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD, 5) none on behalf of the user to be performed before the user is identified.
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.

PACE
EAC

FIA_UAU.4/PACE	**Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FIA_UAU.4.1/PACE	The TSF shall prevent reuse of authentication data related to 1) PACE protocol according to [ICAO_SAC], 2) authentication mechanism based on Triple-DES **or** AES, 3) Terminal Authentication protocol v.1 according to [BSI_TR-03110-1].

Note 36: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Administrator may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

Note 37: This SFR has been adapted from [CC_PP-0056-V2]. Item (3) of FIA_UAU.4.1 applies only to configurations with Terminal Authentication (TA).

PACE EAC

FIA_UAU.5/PACE	**Multiple authentication mechanisms**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1/PACE	The TSF shall provide: 1) PACE protocol according to [ICAO_SAC], 2) Passive Authentication according to [ICAO_9303_11], 3) Secure Messaging in MAC-ENC mode according to [ICAO_SAC], 4) Symmetric authentication mechanism based on Triple-DES **or** AES, 5) **Secure Channel Protocol SCP03 specified in [GP_SCP03] with *Personalization Agent* Keys**, 6) **Chip Authentication protocol v.1 according to [BSI_TR-03110-1]**, 7) Terminal Authentication protocol v.1 according to [BSI_TR-03110-1]. to support user authentication.

FIA_UAU.5.2/PACE	The TSF shall authenticate any user's claimed identity according to the following rules: 1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of Secure Messaging with the key agreed with the terminal by means of the PACE protocol. 2. The TOE accepts the authentication attempt as *Personalization Agent* by the Secure Channel Protocol SCP03 of Global Platform with *Personalization Agent* Keys. 3. After run of the Chip Authentication protocol version 1 the TOE accepts only received commands with correct message authentication code sent by means of Secure Messaging with key agreed with the terminal by means of the Chip Authentication mechanism v.1. 4. The TOE accepts the authentication attempt by means of the Terminal Authentication protocol v.1 only if the terminal uses the public key presented during the Chip Authentication protocol v.1 and the Secure Messaging established by the Chip Authentication mechanism v.1. 5. The TOE accepts the authentication attempt by means of the Chip Authentication protocol v.1 only if Secure Messaging is established by PACE. 6. none

Note 38: This SFR has been adapted from [CC_PP-0056-V2]. Item (6) of FIA_UAU.5.1 and item (3) of FIA_UAU.5.2 apply only to configurations with Terminal Authentication (TA).

N Item 2 of FIA_UAU.5.2/PACE above defines the authentication of the Personalization Agent during personalization by means of Secure Channel Protocol SCP03 specified in [GP_SCP03] of Global Platform ([GP]).

PACE EAC

FIA_UAU.6	**Re-authenticating – Re-authenticating of Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE protocol or the Chip Authentication protocol version 1 shall be verified as being sent by the **Legitimate Terminal**.

Note 39: This SFR has been adapted from [CC_PP-0068-V2] or [CC_PP-0056-V2], respectively.

FIA_AFL.1/RAD	Authentication failure handling
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1/RAD	The TSF shall detect when an administrator configurable positive integer within the range 1 to 5 unsuccessful authentication attempt occur related to consecutive failed authentication attempts.
FIA_AFL.1.2/RAD	When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD.

FIA_AFL.1/Suspend_PIN	Authentication failure handling – Suspending PIN
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1/Suspend_PIN	The TSF shall detect when an administrator configurable number of unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the PIN as the shared password for PACE.
FIA_AFL.1.2/Suspend_PIN	When the defined number of unsuccessful authentication attempts has been met, the TSF shall suspend the reference value of the PIN according to [BSI_TR-03110-2].

Note 40: This SFR has been adapted from [CC_PP-0086].

FIA_AFL.1/Block_PIN	Authentication failure handling – Blocking PIN
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1/Block_PIN	The TSF shall detect when 1 unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the suspended PIN as the shared password for PACE.
FIA_AFL.1.2/Block_PIN	When the defined number of unsuccessful authentication attempts has been met, the TSF shall block the reference value of PIN according to [BSI_TR-03110-2].

Note 41: This SFR has been adapted from [CC_PP-0086].

CGA

FIA_API.1	Authentication proof of identity
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a Chip Authentication protocol version 1 according to [BSI_TR-03110-1] to prove the identity of the SSCD.

8.1.5 Security Management (FMT)

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 **and Certification Service Provider and Document Verifier and Legitimate Terminal**
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

FMT_SMF.1	Specification of management functions
Hierarchical to:	No other components.
Dependencies:	No dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: 1) creation and modification of RAD, 2) enabling the signature creation function, 3) modification of the security attribute SCD/SVD management, SCD operational, 4) change the default value of the security attribute SCD Identifier, 5) none.

FMT_MOF.1	Management of security functions behavior
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.

KG

FMT_MSA.1/Admin_KG	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_KG	The TSF shall enforce the SCD/SVD_Generation_SFP to restrict the ability to modify and none the security attributes SCD/SVD management to R.Admin.

KI

FMT_MSA.1/Admin_KI	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_KI	The TSF shall enforce the SCD_Import_SFP to restrict the ability to modify the security attributes SCD/SVD management to R.Admin.

FMT_MSA.1/Signatory	Management of security attributes
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions.
FMT_MSA.1.1/Signatory	The TSF shall enforce the Signature_Creation_SFP to restrict the ability to modify the security attributes SCD operational to R.Sigy.

FMT_MSA.2	Secure security attributes
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles.
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for SCD/SVD Management and SCD operational.

KG

FMT_MSA.3/KG	Static attribute initialization
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles.
FMT_MSA.3.1/KG	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/KG	TSF shall allow the R.Admin to specify alternative initial values to override the default values when an object or information is created.

KI

FMT_MSA.3/KI	Static attribute initialization
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles.
FMT_MSA.3.1/KI	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/KI	TSF shall allow the R.Admin to specify alternative initial values to override the default values when an object or information is created.

KG

FMT_MSA.4/KG	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/KG	The TSF shall use the following rules to set the value of security attributes: 1) 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.

Note 42: The TOE may not support generating an SVD/SCD pair by the signatory alone, in which case rule (2) is not relevant.

KI

FMT_MSA.4/KI	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/KI	The TSF shall use the following rules to set the value of security attributes: (1) If S.Admin imports SCD while S.Sigy is currently authenticated, the security attribute “SCD operational” of the SCD shall be set to “yes” after import of the SCD as a single operation.

EAC

FMT_MTD.1/CVCA_UPD	Management of TSF data – Country Verifier Certification Authority
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_UPD	The TSF shall restrict the ability to update the 1) **Certification Authority Public Key**, 2) **Certification Authority Certificate**, to **Certification Service Provider**

Note 43: The Certification Service Provider updates its asymmetric key pair and distributes the public key be means of the CA link-certificates (cf. [BSI_TR-03110-1]). The TOE updates its internal trust-point if a valid CA link-certificates is provided by the terminal (cf. [BSI_TR-03110-1]).

Note 44: This SFR has been adapted from [CC_PP-0056-V2]. The objects *Country Verifying Certification Authority Public Key* and *Country Verifier Certification Authority Certificate* have been changed to *Certification Authority Public Key* and *Certification Authority Certificate*, respectively. The role *Country Verifying Certification Authority*, which does not exist in this context, has been changed to *Certification Service Provider*. This SFR applies only to configurations with Terminal Authentication (TA).

EAC

FMT_MTD.1/DATE	**Management of TSF data – Current date**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/DATE	The TSF shall restrict the ability to modify the current date to 1) **Certification Service Provider**, 2) Document Verifier, 3) **Legitimate Terminal**.

Note 45: The authorized roles are identified in their certificate (cf. [BSI_TR-03110-1]) and authorized by validation of the certificate chain. The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication v.1 (cf. to [BSI_TR-03110-1]).

Note 46: This SFR has been adapted from [CC_PP-0056-V2]. The role *Country Verifying Certification Authority*, which does not exist in this context, has been changed to *Certification Service Provider*. The role *Domestic Extended Inspection System*, which does not exist in this context, has been changed to *Legitimate Terminal*. This SFR applies only to configurations with Terminal Authentication (TA).

PACE
EAC

FMT_MTD.1/KEY_READ	**Management of TSF data – Key read**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_READ	The TSF shall restrict the ability to read the 1) PACE passwords, 2) Chip Authentication private key, 3) Personalization keys 4) **Electronic signature private keys** to none

Note 47: This SFR has been adapted from [CC_PP-0056-V2]. The object *electronic signature keys* has been added.

FMT_MTD.1/Admin	**Management of TSF data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MTD.1.1/Admin	The TSF shall restrict the ability to create the RAD to R.Admin

FMT_MTD.1/Signatory	**Management of TSF data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MTD.1.1/Signatory	The TSF shall restrict the ability to modify and none the RAD to R.Sigy

8.1.6 Protection of the TSF (FPT)

FPT_EMS.1/SSCD	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1/SSCD	The TOE shall not emit information about IC power consumption and command execution time in excess of non-useful information enabling access to RAD and SCD.
FPT_EMS.1.2/SSCD	The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to RAD and SCD.

PACE
EAC

FPT_EMS.1/KEYS	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_EMS.1.1/KEYS	The TOE shall not emit information about IC power consumption and command execution time in excess of non-useful information enabling access to 1) Chip Authentication session keys, 2) PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}), 3) the ephemeral private key ephem-SK_{PICC}-PACE, 4) Manufacturer authentication key, 5) Personalization Agent keys, 6) Chip Authentication private keys, and 7) decryption keys.
FPT_EMS.1.2/KEYS	The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to 1) Chip Authentication session keys, 2) PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}), 3) the ephemeral private key ephem-SK_{PICC}-PACE, 4) Manufacturer authentication key, 5) Personalization Agent Keys, 6) Chip Authentication private keys, and 7) decryption keys.

Note 48: This SFR has been adapted from [CC_PP-0056-V2].

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) exposure to out-of-range operating conditions where therefore a malfunction could occur

FPT_PHP.1	**Passive detection of physical attack**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

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

FPT_TST.1	TSF testing
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self-tests during initial start-up to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

KI

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.

N This TSF requires a trusted channel for key import from the CGA in the field. This is fullfilled in any case, even for the contact-only configuration because in this case Chip Authentication is mandatory in order to establish a trusted channel.

CGA

FTP_ITC.1/SVD	Inter-TSF trusted channel
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FTP_ITC.1.1/SVD	The TSF shall provide a communication channel between itself and another trusted IT product **CGA** that is logically distinct from other communication channels and provides ensured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/SVD	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/SVD	The TSF **or the CGA** shall initiate communication via the trusted channel for 1) data authentication with identity of guarantor according to FIA_API.1 and FDP_DAU.2/SVD, 2) none.

SCA

FTP_ITC.1/VAD	**Inter-TSF trusted channel – TC Human Interface Device**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/VAD	The TSF shall provide a communication channel between itself and another trusted IT product **HID** that is logically distinct from other communication channels and provides ensured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/VAD	The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/VAD	The TSF **or the HID** shall initiate communication via the trusted channel for 1) user authentication according to FIA_UAU.1, 2) none.

Note 49: The PACE protocol used for authentication is a zero-knowledge protocol and thus protects the confidentiality of the VAD implicitly.

SCA

FTP_ITC.1/DTBS	**Inter-TSF trusted channel**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/DTBS	The TSF shall provide a communication channel between itself and another trusted IT product **SCA** that is logically distinct from other communication channels and provides ensured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/DTBS	The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.

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

8.2 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
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semiformal modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.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

Assurance class	Assurance components	
AVA: Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

Table 8.3: Assurance Requirements: EAL5 augmented with ALC_DVS.2 and AVA_VAN.5

9 Rationale

9.1 Security Requirements Rationale

9.1.1 Security Requirements Coverage

Security objectives and security functional requirements that are added by *PP SSCD KI*, *PP SSCD KI TCSCA*, *PP SSCD KG TCCGA* or *PP SSCD KG TCSCA* are color coded for better readability. Security functional requirements taken from [CC_PP-0056-V2] or [CC_PP-0068-V2] or modified to meet those PPs, respectively, are given in *italics*, security functional requirements taken from [CC_PP-0086] are given in **bold face**.

9.1.2 Security Functional Requirements Sufficiency

OT.Lifecycle_Security *(Life cycle security)* is provided by the SFRs

- FCS_CKM.1/SCD (for SCD/SVD generation),
- FCS_COP.1/SCD (for SCD usage) and
- FCS_CKM.4 (for SCD destruction)

ensuring cryptographically secure life cycle 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.

KI 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 SCD usage is ensured by access control

- FDP_ACC.1/Signature_Creation,
- FDP_AFC.1/Signature_Creation,
- FDP_ACC.1/Signature_Creation/N-QES,
- FDP_AFC.1/Signature_Creation/N-QES which is based on the security attribute secure TSF management according to
- FMT_MOF.1,
- FMT_MSA.1/Admin_KG,
- FMT_MSA.1/Admin_KI,
- FMT_MSA.1/Signatory,
- FMT_MSA.2,
- FMT_MSA.3_KG,
- FMT_MSA.3_KI,
- FMT_MSA.4_KG,
- FMT_MSA.4_KI,
- 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 life cycle.

(Life cycle security) in the phase “usage/preparation” is provided by the SFRs

- FCS_CKM.1/DH_PACE,
- FCS_CKM.1/CA_STATIC,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RND.1,
- FIA_UID.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6 and
- FMT_MTD.1/KEY_READ.

(Life cycle security) in the phase “usage/operational” is provided by the SFRs

- FCS_CKM.1/DH_PACE,
- FCS_CKM.1/CA,
- FCS_COP.1/CA_ENC,

- FCS_COP.1/CA_MAC,
- FCS_COP.1/SIG_VER,
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RND.1,
- FDP_ACC.1/TRM,
- FDP_AFC.1/TRM,
- FIA_API.1,
- FIA_UID.1,
- FIA_UAU.4/PACE,
- FIA_UAU.6,
- FMT_MTD.1/CVCA_UPD,
- FMT_MTD.1/DATE and
- FMT_MTD.1/KEY_READ.

KG **OT.SCD/SVD_Auth_Gen** *(Authorized SCD/SVD generation)* addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by

- FIA_UID.1 and
- FIA_UAU.1

provide user identification and user authentication prior to enabling access to authorized 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_KG,
- FMT_MSA.1/Admin_KI,
- FMT_MSA.2 ,
- FMT_MSA.3/KG and
- FMT_MSA.3/KI

for static attribute initialization. The SFR

- FMT_MSA.4/KG and
- FMT_MSA.4/KI

defines rules for inheritance of the security attribute “SCD operational” of the SCD.

KI **OT.SCD_Auth_Imp** *(Authorized SCD import)* is provided by the security functions specified by the following SFRs.

- 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 authorized users can import SCD.

KG **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/SCD.

KG **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/SCD

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/KG

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 SFRs.

KG
- FCS_CKM.1/SCD 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.

KI
- FDP_UCT.1/SCD and
- FTP_ICT.1/SCD ensures the confidentiality for SCD import.
- FDP_RIP.1 and
- FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been used for signature creation and that destruction of SCD leaves no residual information.
- FDP_SDI.2/Persistent ensures 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).
- FPT_EMS.1/SSCD 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/SCD, 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.
- FMT_MTD.1/Admin and
- FMT_MTD.1/Signatory manage the authentication function.
- FIA_AFL.1/RAD provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.
- FIA_AFL.1/Suspend_PIN provides protection against denial-of-service attacks.
- FIA_AFL.1/Block_PIN provides protection against brute force attacks against authentication.
- 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).
- FDP_ACC.1/Signature_Creation,
- FDP_ACF.1/Signature_Creation,
- FDP_ACC.1/Signature_Creation/N-QES and
- FDP_ACF.1/Signature_Creation/N-QES provide access control based on the security attributes managed according to the SFRs
- FMT_MTD.1/Signatory,
- FMT_MSA.2,
- FMT_MSA.3/KG,

- FMT_MSA.3/KI,
- FMT_MSA.4/KG and
- FMT_MSA.4/KI.
- 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.

In the phase “usage/operational” *Signature creation function for the legitimate signatory only* is additionally provided by the SFRs

- FCS_CKM.1/DH_PACE,
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RND.1,
- FIA_UID.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6 and
- FIA_API.1.

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/SSCD and
- FPT_EMS.1.1/KEYS.

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_EMS.1.1/KEYS and
- FPT_PHP.3

to resist physical attacks.

CGA **OT.TOE_SSCD_Auth** *(Authentication proof as SSCD)* requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by

- FIA_API.1.
- FIA_UAU.1 allows (additionally to *PP SSCD KG*) establishment of the trusted channel before (human) user is authenticated.

Furthermore

- FCS_CKM.1/CA_STATIC provides the keys for the Chip Authentication protocol.

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

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

The functionality for integrity and confidentiality is provided by

- FCS_CKM.1/DH_PACE,
- FCS_CKM.1/CA_STATIC,
- FCS_CKM.1/CA,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/CA_ENC,
- FCS_COP.1/CA_MAC,
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RND.1,
- FDP_ACC.1/TRM,
- FDP_AFC.1/TRM,
- FIA_UID.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6,
- FMT_MTD.1/CVCA_DIS,
- FMT_MTD.1/DATE and
- FMT_MTD.1/KEY_READ.

SCA **OT.TOE_TC_VAD_Imp** *(Trusted channel of TOE for VAD import)* is provided by

- FTP_ITC.1/VAD

to provide a trusted channel to protect the VAD provided by the HID to the TOE.

The functionality for integrity and confidentiality is provided by

- FCS_CKM.1/DH_PACE,
- FCS_CKM.1/CA_STATIC,
- FCS_CKM.1/CA,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/CA_ENC,
- FCS_COP.1/CA_MAC,
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RND.1,
- FIA_UID.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6,
- FMT_MTD.1/CVCA_DIS,
- FMT_MTD.1/DATE and
- FMT_MTD.1/KEY_READ.

SCA **OT.TOE_TC_DTBS_Imp** *(Trusted channel of TOE for DTBS)* is provided by

- FTP_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by
- FDP_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS.

The functionality for integrity and confidentiality is provided by

- FCS_CKM.1/DH_PACE,
- FCS_CKM.1/CA_STATIC,
- FCS_CKM.1/CA,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/CA_ENC,
- FCS_COP.1/CA_MAC,
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RND.1,
- FIA_UID.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,

- FIA_UAU.6,
- FMT_MTD.1/CVCA_DIS,
- FMT_MTD.1/DATE and
- FMT_MTD.1/KEY_READ.

9.1.3 Satisfaction of Dependencies of Security Requirements

Functional requirements	Dependencies	Satisfied by
FCS_CKM.1/SCD	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/SCD, FCS_CKM.4
FCS_CKM.1/DH_PACE	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_CKM.4
FCS_CKM.1/CA_STATIC	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_CKM.4
FCS_CKM.1/CA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/SCD, FCS_CKM.1/DH_PACE, FCS_CKM.1/CA
FCS_COP.1/SCD	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/SCD, FCS_CKM.4
FCS_COP.1/CA_ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/CA_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/SIG_VER	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/PACE_ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_COP.1/PACE_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_RND.1	No dependencies	n/a
FDP_ACC.1/TRM	FDP_ACF.1	FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/TRM, FMT_MSA.3/KG
FDP_ACC.1/ SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/ SCD/SVD_Generation

Functional requirements	Dependencies	Satisfied by
FDP_ACF.1/ SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/ SCD/SVD_Generation, FMT_MSA.3/KG
FDP_ACC.1/SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3/KG
FDP_ACC.1/SCD_Import	FDP_ACF.1	FDP_ACF.1/SCD_Import
FDP_ACF.1/SCD_Import	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3/KI
FDP_ACC.1/ Signature_Creation	FDP_ACF.1	FDP_ACF.1/ Signature_Creation
FDP_ACF.1/ Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/ Signature_Creation, FMT_MSA.3/KG, FMT_MSA.3/KI
FDP_ACC.1/Signature_ Creation/N-QES	FDP_ACF.1	FDP_ACF.1/Signature_ Creation/N-QES
FDP_ACF.1/Signature_ Creation/N-QES	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_ Creation/N-QES, FMT_MSA.3/KG, FMT_MSA.3/KI
FDP_ITC.1/SCD	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3/KI
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
FDP_UIT.1/DTBS	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1/ Signature_Creation, FDP_ACC.1/Signature_ Creation/N-QES, FTP_ITC.1/DTBS
FDP_RIP.1	No dependencies	n/a
FDP_SDI.2/Persistent	No dependencies	n/a
FDP_SDI.2/DTBS	No dependencies	n/a
FDP_DAU.2/SVD	FIA_UID.1	FIA_UID.1
FIA_UID.1	No dependencies	n/a
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.4/PACE	No dependencies	n.a.
FIA_UAU.5/PACE	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FIA_AFL.1/RAD	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/Suspend_PIN	FIA_UAU.1	FIA_UAU.1

Functional requirements	Dependencies	Satisfied by
FIA_AFL.1/Block_PIN	FIA_UAU.1	FIA_UAU.1
FIA_API.1	No dependencies	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_SMF.1	No dependencies	n/a.
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin_KG	[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/Admin_KI	[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, FDP_ACC.1/ Signature_Creation/N-QES, FDP_ACC.1/SCD_Import, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/ SCD/SVD_Generation, FDP_ACC.1/SCD_Import, FDP_ACC.1/ Signature_Creation, FDP_ACC.1/ Signature_Creation/N-QES, FMT_SMR.1, FMT_MSA.1/Admin_KG, FMT_MSA.1/Admin_KI, FMT_MSA.1/Signatory
FMT_MSA.3/KG	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin_KG, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.3/KI	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin_KI, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4/KG	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/ SCD/SVD_Generation, FDP_ACC.1/ Signature_Creation, FDP_ACC.1/Signature_ Creation/N-QES

Functional requirements	Dependencies	Satisfied by
FMT_MSA.4/KI	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/ FDP_ACC.1/SCD_Import, FDP_ACC.1/ Signature_Creation, FDP_ACC.1/ Signature_Creation/N-QES
FMT_MTD.1/CVCA_UPD	FMT_SMR.1, FMT_SMF.1,	FMT_SMR.1. FMT_SMF.1
FMT_MTD.1/DATE	FMT_SMR.1, FMT_SMF.1,	FMT_SMR.1. FMT_SMF.1
FMT_MTD.1/KEY_READ	FMT_SMR.1, FMT_SMF.1,	FMT_SMR.1. FMT_SMF.1
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
FPT_EMS.1/SSCD	No dependencies	n/a
FPT_EMS.1/KEYS	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
FTP_ITC.1/SVD	No dependencies	n/a
FTP_ITC.1/VAD	No dependencies	n/a
FTP_ITC.1/DTBS	No dependencies	n/a

Table 9.2: Satisfaction of dependencies of security functional requirements

Assurance requirement(s)	Dependencies	Satisfied by
EAL5 package	(dependencies of EAL5 package are not reproduced here)	By construction, all dependencies are satisfied in a CC EAL package
ALC_DVS.2	no dependencies	
AVA_VAN.5	ADV_ARC.1 ADV_FSP.4 ADV_TDS.3 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1	ADV_ARC.1 ADV_FSP.5 ADV_TDS.4 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.3 (all are included or exceeded in EAL5 package)

Table 9.3: Satisfaction of dependencies of security assurance requirements

9.1.4 Rationale for Chosen Security Assurance Requirements

The assurance level for *PP SSCD KG*, *PP SSCD KG TCCGA* and *PP SSCD KG TCSCA* as well as *PP SSCD KI* and *PP SSCD KI TCSCA* is EAL5 augmented by

AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, i.e. the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure.

This ST chooses the higher assurance level EAL5 augmented by

AVA_VAN.5 Advanced methodical vulnerability analysis

ALC_DVS.2 Sufficiency of security measures

The requirements of the claimed protection profiles are met or exceeded and the dependencies are fulfilled as shown in table 9.3. The augmentation ALC_DVS.2 is chosen in addition to the requirements of the protection profiles and the EAL5 package. It provides higher assurance of the security of the TOEs development and manufacturing.

10 TOE Summary Specification (ASE_TSS.1)

This chapter describes the TOE security functions and the assurance measures covering the requirements of the previous chapter.

10.1 TOE Security Functions

This chapter gives the overview description of the different TOE security functions composing the TSF.

10.1.1 F.Access_Control

This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access. This function consists of following elements:

1. Access to objects is controlled based on subjects, objects (any file) and security attributes.
2. No access control policy allows reading of any key.
3. Any access not explicitly allowed is denied.
4. Access Control in **development phase** enforces development policy: Configuration of the TOE, configuring of access control policy and doing key management (PACE and EACv1) only by the *Manufacturer* or on behalf of him (see F.Management).
5. Access Control in **usage/preparation phase** enforces personalization policy: Writing of user data, authentication data and SCD/SVD only by the *Administrator* identified with its authentication key (see F.Management).
6. Access Control in **usage/operational phase** enforces operational use policy: Operation of the signature creation function only by the *Signatory* who must activate the SSCD application before first usage; generation and writing of SCD/SVD only by the *Signatory* identified with its authentication key (see F.Management). For Personalization in the Preparation Phase the Secure Channel Protocol SCP03 of Global Platform with Personalization Agent keys is used.

10.1.2 F.Identification_Authentication

This function provides identification/authentication of the user roles

- Administrator
- Signatory
- Certificate Service Provider
- Document Verifier
- Legitimate Terminal

by the methods:

- PACE authentication method according to [BSI_TR-03110-1, BSI_TR-03110-2] with the following properties:
  - It uses PIN, PUK or CAN.
  - The method sets the card to a **suspended state** before the secret is finally blocked (only PIN and PUK) or to delay the processing of the authentication command after a failed authentication (CAN).
  - The cryptographic method for confidentiality is AES/CBC or 3DES/CBC provided by F.Crypto.
  - The cryptographic method for authenticity is CMAC or Retail-MAC provided by F.Crypto.
  - On error (wrong MAC, wrong challenge) the user role is not identified/authenticated.
  - On success the session keys are created and stored for Secure Messaging.
  - Keys and data in transient memory are overwritten after usage.
- Chip Authentication with the following properties:
  - According to [BSI_TR-03110-1] using ECDH from F.Crypto.
  - Session keys are created and stored for Secure Messaging replacing existing session keys.
- Terminal Authentication with the following properties:
  - According to [BSI_TR-03110-1] checking certificates with ECDSA from F.Crypto.
  - It uses a challenge from the card.
  - Usable only in a Secure Messaging session with Chip Authentication key.
  - It distinguishes between the roles:
    * Certificate Service Provider
    * Document Verifier
    * Legitimate Terminal
  - Update of CVCA certificate is allowed for Certificate Service Provider.
  - Update of current date is allowed for Certificate Service Provider, Document Verifier and Legitimate Terminal.
  - The challenge-response authentication is only performed with a public key from an IS certificate.
  - Verifying validity of certificate chain:
    * Certificates must be in the sequence: known CVCA [> CVCA...]> DV > IS.
    * Expiration dates must not be before the current date with the exception of CVCA.
- Secure Messaging with the following properties:
  - The cryptographic method for confidentiality is AES/CBC or 3DES/CBC provided by F.Crypto.

  - The cryptographic method for authenticity is CMAC or Retail-MAC provided by F.Crypto.
  - In a Secure Messaging protected command the method for confidentiality and the method for authenticity must be present.
  - The initialization vector is a zero-IV for 3DES encryption and an encrypted Send Sequence Counter (SSC) for AES encryption, CMAC and Retail-MAC.
  - A session key is used.
  - On any command that is not protected correctly with the session keys these are overwritten according to FIPS 140-2 [FIPS_140-3] (or better) and a new PACE authentication or (in phase usage/operational) CA authentication, is required.
  - Keys and data in transient memory are overwritten after usage.
- Verification of the PIN for qualified signature with a minimum length of 6 bytes for *authentication data* that is blocked after three failed authentications, the reset of the retry counter is limited to 10. The transmission of the PIN must be protected by Secure Messaging with PACE.
- RSA with 2048 bit - 4096 bit key length or ECDSA with 224 bit - 521 bit key length for both qualified and advanced signature; the qualified signature creation requires authentication before each signature creation (i.e. the authentication state is reset immediately after usage).

N For personalization of the TOE the Secure Channel Protocol SCP03 specified in [GP_SCP03] of Global Platform ([GP]) is used with AES 256 bits key length and encryption compliant to [NIST_SP800-38A].

10.1.3 F.Management

Note 50: Some configurations require Terminal Authentication (TA) for the communication between the TOE and the SCA or CGA. Those configurations have to provide the **data structures necessary to perform TA**. As this feature is provided in addition to the requirements of *PP SSCD KG*, *PP SSCD KG TCCGA* and *PP SSCD KG TCSCA*, also the configurations that do not require TA do not conflict the strict conformance claim given in chapter 4.

Key management (PACE and EACv1) and other administrative tasks can be performed.

In preparation phase the *Administrator* performs the following steps:

- configuring the card for usage as SSCD (loading of the eSign package),
- writing of all the required user data to the appropriate files (PUK and CAN),
- optionally, generating an SCD/SVD key pair, exporting the SVD and writing the certificate to the card and
- delivering the SSCD and the PUK to the user.
- Changing the TOE into the end-usage mode for **usage/operational phase**.

In operational use phase the *Signatory* may perform the following steps:

- activating the SSCD functionality by activating the RAD,
- changing the RAD value,
- generation of SCD/SVD and exporting of SVD using a trusted channel and
- destruction of the a signature key by deleting and overwriting the key value.

10.1.4 F.Crypto

This function provides a high level interface to

- DES
- Triple-DES/CBC
- AES
- DES/Retail MAC
- CMAC
- ECC
- RSA
- Random number generation

N For personalization of the TOE the Secure Channel Protocol SCP03 specified in [GP_SCP03] of Global Platform ([GP]) is used with AES 256 bits key length and encryption compliant to [NIST_SP800-38A].

10.1.5 F.Integrity

F.Integrity assures the integrity of internal applet data. It is based on the platform service SF.Physical provided by Secora™ ID S v1.1 (cf. the security target [SECORA_ST-SLJ52]).

F.Integrity provides the following properties:

- Preserve a secure state when the following types of failures occur:
  - Exposure to operating conditions causing a TOE malfunction.
  - Failure detected by TSF according to FPT_TST.1.
- Run a suite of self tests during initial start-up to demonstrate the correct operation of the TSF. The TOE makes use of the User Mode Security Life Control selftest provided by the platform during startup. The self test functionality is therefore realized by Secora™ ID S v1.1 and the hardware.
- Resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.
- Provide unambiguous detection of physical tampering that might compromise the TSF.

- Provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

10.2 Assurance Measures

The assurance measures fulfilling the requirements of EAL5 augmented by ALC_DVS.2 and AVA_VAN.5 are given in table 10.2.

Measure	Description
ADV_ARC.1	Security architecture description
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	Semiformal modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures, 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
ATE_COV.2	Analysis of coverage
ATE_DPT.3	Testing: modular design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.5	Advanced methodical vulnerability analysis

Table 10.2: Assurance Measures

10.2.1 TOE Summary Specification Rationale

Table 10.4 shows the coverage of the SFRs by TSFs.

SFR	TSFs
FCS_CKM.1/SCD	F.Crypto
FCS_CKM.1/DH_PACE	F.Crypto
FCS_CKM.1/CA_STATIC	F.Crypto

SFR	TSFs
FCS_CKM.1/CA	F.Crypto
FCS_CKM.4	F.Management, F.Identification_Authentication
FCS_COP.1/SCD	F.Crypto
FCS_COP.1/CA_ENC	F.Crypto
FCS_COP.1/CA_MAC	F.Crypto
FCS_COP.1/SIG_VER	F.Crypto
FCS_COP.1/PACE_ENC	F.Crypto
FCS_COP.1/PACE_MAC	F.Crypto
FCS_RND.1	F.Crypto
FDP_ACC.1/TRM	F.Access_Control
FDP_AFC.1/TRM	F.Access_Control
FDP_ACC.1/SCD/SVD_Generation	F.Access_Control, F.Identification_Authentication, F.Management
FDP_AFC.1/SCD/SVD_Generation	F.Access_Control, F.Identification_Authentication, F.Management
FDP_ACC.1/SVD_Transfer	F.Access_Control, F.Identification_Authentication
FDP_AFC.1/SVD_Transfer	F.Access_Control, F.Identification_Authentication
FDP_ACC.1/SCD_Import	F.Access_Control, F.Identification_Authentication, F.Management
FDP_AFC.1/SCD_Import	F.Access_Control, F.Identification_Authentication, F.Management
FDP_ACC.1/Signature_Creation	F.Access_Control, F.Identification_Authentication
FDP_AFC.1/Signature_Creation	F.Access_Control, F.Identification_Authentication
FDP_ACC.1/Signature_Creation/ N-QES	F.Access_Control, F.Identification_Authentication
FDP_AFC.1/Signature_Creation/ N-QES	F.Access_Control, F.Identification_Authentication
FDP_ITC.1/SCD	F.Access_Control, F.Identification_Authentication, F.Management
FDP_UCT.1/SCD	F.Access_Control, F.Identification_Authentication, F.Management
FDP_UIT.1/DTBS	F.Access_Control, F.Identification_Authentication
FDP_RIP.1	F.Identification_Authentication, F.Management
FDP_SDI.2/Persistent	F.Management, F.Integrity
FDP_SDI.2/DTBS	F.Management, F.Integrity
FDP_DAU.2/SVD	F.Crypto, F.Identification_Authentication
FIA_UID.1	F.Identification_Authentication

SFR	TSFs
FIA_UAU.1	F.Identification_Authentication
FIA_UAU.4/PACE	F.Identification_Authentication
FIA_UAU.5/PACE	F.Access_Control, F.Identification_Authentication
FIA_UAU.6	F.Identification_Authentication
FIA_AFL.1/RAD	F.Access_Control, F.Identification_Authentication
FIA_AFL.1/Suspend_PIN	F.Access_Control
FIA_AFL.1/Block_PIN	F.Access_Control
FIA_API.1	F.Identification_Authentication
FMT_SMR.1	F.Identification_Authentication
FMT_SMF.1	F.Identification_Authentication, F.Management
FMT_MOF.1	F.Access_Control, F.Identification_Authentication, F.Management
FMT_MSA.1/Admin_KG	F.Identification_Authentication, F.Management
FMT_MSA.1/Admin_KI	F.Identification_Authentication, F.Management
FMT_MSA.1/Signatory	F.Access_Control, F.Identification_Authentication
FMT_MSA.2	F.Identification_Authentication, F.Management
FMT_MSA.3/KG	F.Identification_Authentication, F.Management
FMT_MSA.3/KI	F.Identification_Authentication, F.Management
FMT_MSA.4/KG	F.Identification_Authentication, F.Management
FMT_MSA.4/KI	F.Identification_Authentication, F.Management
FMT_MTD.1/CVCA_UPD	F.Identification_Authentication
FMT_MTD.1/DATE	F.Identification_Authentication
FMT_MTD.1/KEY_READ	F.Access_Control
FMT_MTD.1/Admin	F.Identification_Authentication, F.Management
FMT_MTD.1/Signatory	F.Identification_Authentication, F.Management
FPT_EMS.1/SSCD	F.Identification_Authentication
FPT_EMS.1/KEYS	F.Identification_Authentication
FPT_FLS.1	F.Integrity
FPT_PHP.1	F.Integrity
FPT_PHP.3	F.Integrity
FPT_TST.1	F.Integrity
FTP_ITC.1/SCD	F.Access_Control
FTP_ITC.1/SVD	F.Access_Control, F.Identification_Authentication
FTP_ITC.1/VAD	F.Access_Control, F.Identification_Authentication
FTP_ITC.1/DTBS	F.Access_Control

Table 10.4: Coverage of SFRs for the TOE by TSFs.

10.3 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target and the Security Target of the platform [SECORA_ST-SLJ52].

10.3.1 Mapping of the Platform TSFs

For every platform TSF the following Table 10.5 maps the corresponding TSFs of this Composite ST or shows that they are not relevant.

Platform TSF	Corresponding TSF	Remarks
SF.Firewall	N/A (used implicitly)	Java Card applet management
SF.RIP	F.Administration, F.Integrity	Java Card TOE
SF.Rollback	F.Integrity	Java Card TOE
SF.SCP	F.Access_Control	GlobalPlatform secure channel
SF.CM	F.Access_Control	GlobalPlatform card management
SF.Physical	F.Integrity, F.Administration, F.Access_Control	Java Card TOE
SF.CS	F.Crypto, F.Access_Control, F.Administration	Java Card TOE
SF.PIN	F.Administration, F.Integrity	Java Card TOE

Table 10.5: Correspondence and Relevance of Platform and Composite TSFs

10.3.2 Mapping of the Platform Objectives

Some of the security objectives of the TOE and the platform can be mapped directly (see Table 10.6). None of them show any conflicts between each other.

Platform Objective	Corresponding Objective	Remarks
O.SID	N/A (used implicitly)	No conflict with this ST.
O.FIREWALL	N/A (used implicitly)	No conflict with this ST.
O.GLOBAL_ARRAYS_CONFID	OT.SCD_Secrecy	No conflict with this ST.
O.GLOBAL_ARRAYS_INTEG	OT.DTBS_Integrity_TOE	No conflict with this ST.
O.NATIVE	N/A (used implicitly)	No conflict with this ST.
O.OPERATE	N/A (used implicitly)	No conflict with this ST.
O.REALLOCATION	N/A (used implicitly)	No conflict with this ST.
O.RESOURCES	N/A (used implicitly)	No conflict with this ST.
O.ALARM	Relevant	This platform objective is relevant for the correct function of the TOE. However, there is no directly corresponding objective for the TOE. No conflict with this ST.
O.CIPHER	Relevant	This platform objective is relevant for the correct function of the TOE because it makes use of cryptographic algorithms provided by the platform. However, there is no directly corresponding objective for the TOE. No conflict with this ST.

Platform Objective	Corresponding Objective	Remarks
O.KEY-MNGT	OT.SCD_Unique OT.SCD_SVD_Corresp OT.Sig_Secure	No conflict with this ST.
O.PIN-MNGT	OT.SCD_Auth_Imp OT.SCD/SVD_Auth_Gen OT.Sigy_SigF	No conflict with this ST.
O.TRANSACTION	Relevant	This platform objective is relevant for the correct function of the TOE. However, there is no directly corresponding objective for the TOE. No conflict with this ST.
O.OBJ-DELETION	Relevant	This platform objective is relevant for the correct function of the TOE. However, there is no directly corresponding objective for the TOE. No conflict with this ST.
O.DELETION	N/A (used implicitly)	No conflict with this ST.
O.LOAD	N/A (used implicitly)	No conflict with this ST.
O.INSTALL	N/A (used implicitly)	No conflict with this ST.
O.COMMUNICATION	N/A (used implicitly)	No conflict with this ST.
O.CARD-MANAGEMENT	N/A (used implicitly)	No conflict with this ST.
O.SCP.IC	OT.EMSEC_Design OT.Tamper_ID OT.Tamper_Resistance	No conflict with this ST.
O.SCP.RECOVERY	OT.Tamper_ID OT.Tamper_Resistance	No conflict with this ST.
O.SCP.SUPPORT	Relevant	This platform objective is relevant for the correct function of the TOE because it makes use of cryptographic algorithms provided by the platform. However, there is no directly corresponding objective for the TOE. No conflict with this ST.
O.SCP.RNG	Relevant	This platform objective is relevant for the correct function of the TOE because it makes use of random numbers provided by the platform. However, there is no directly corresponding objective for the TOE. No conflict with this ST.

Table 10.6: Correspondence and Relevance of Platform and Composite Objectives

10.3.3 Mapping of the Platform SFRs

The relevant Security Requirements of the TOE and the platform can be mapped directly (see Table 10.7). None of them show any conflicts between each other.

Platform SFR	Corresponding SFR	Remarks
FDP_ACC.2/FIREWALL	N/A (used implicitly)	Java Card Firewall. Applet requirements are mentioned in the User Guidance. No conflict.
FDP_ACF.1/FIREWALL	N/A (used implicitly)	Java Card Firewall. Applet requirements are mentioned in the User Guidance. No conflict.
FDP_IFC.1/JCVM	N/A (used implicitly)	Java Virtual Machine. No conflict.
FDP_IFF.1/JCVM	N/A (used implicitly)	Java Virtual Machine. No conflict.
FDP_RIP.1/OBJECTS	N/A (used implicitly).	Java Card Firewall. No conflict.
FMT_MSA.1/JCRE	N/A (used implicitly)	Java Card Firewall. No conflict.
FMT_MSA.1/JCVM	N/A (used implicitly)	Java Virtual Machine. No conflict.
FMT_MSA.2/ FIREWALL_JCVM	N/A (used implicitly)	Java Card Firewall. Applet requirements are mentioned in the User Guidance. No conflict.
FMT_MSA.3/FIREWALL	N/A (used implicitly)	Java Card Firewall. Applet requirements are mentioned in the User Guidance. No conflict.
FMT_MSA.3/JCVM	N/A (used implicitly)	Java Virtual Machine. No conflict.
FMT_SMF.1	N/A (used implicitly)	Used implicitly. No conflict.
FMT_SMR.1	N/A (used implicitly)	Java Card Firewall. No conflict.
FCS_CKM.1	FCS_CKM.1/SCD FCS_CKM.1/CA_STATIC FCS_CKM.1/CA FCS_CKM.1/DH_PACE	TOE SFRs based on platform SFR.
FCS_CKM.2	N/A (used implicitly)	Java Card internal. No conflict.
FCS_CKM.3	N/A (used implicitly)	Java Card internal. No conflict.
FCS_CKM.4	FCS_CKM.4	TOE SFR based on platform SFR.

Platform SFR	Corresponding SFR	Remarks
FCS_COP.1 with iterations **JCAPI:** FCS_COP.1.1/JCAPI/* **Global Platform SCP:** FCS_COP.1.1/SCP/* **Secure Messaging:** FCS_COP.1.1/SM/*	FCS_COP.1/SCD FCS_COP.1/PACE_ENC FCS_COP.1/PACE_MAC FCS_COP.1/CA_ENC FCS_COP.1/CA_MAC FCS_COP.1/SIG_VER	FCS_COP.1/SCD is covered by FCS_COP.1.1/JCAPI/RSA-DEC[1] and FCS_COP.1.1/JCAPI/ECDSA-SIG. FCS_COP.1/PACE_ENC is covered by FCS_COP.1.1/SM/PACE. FCS_COP.1/PACE_MAC is covered by FCS_COP.1.1/SM/PACE. FCS_COP.1/CA_ENC is covered by FCS_COP.1.1/JCAPI/ECDH. FCS_COP.1/CA_MAC is covered by FCS_COP.1.1/JCAPI/ECDH. FCS_COP.1/SIG_VER is covered by FCS_COP.1.1/JCAPI/ECDSA-VER.
FDP_RIP.1/ABORT	FDP_RIP.1	TOE SFR based on platform SFR.
FDP_RIP.1/APDU	N/A (used implicitly).	Java Card internal. No conflict.
FDP_RIP.1/bArray	FDP_RIP.1	TOE SFR based on platform SFR.
FDP_RIP.1/KEYS	FDP_RIP.1	TOE SFR based on platform SFR.
FDP_RIP.1/TRANSIENT	N/A (used implicitly).	Java Card internal. No conflict.
FDP_ROL.1/FIREWALL	N/A (used implicitly).	Java Card Firewall. Applet requirements are mentioned in the User Guidance. No conflict.
FAU_ARP.1	FPT_FLS.1	TOE SFR based on platform SFR.
FDP_SDI.2	FPT_FLS.1	TOE SFR based on platform SFR.
FPR_UNO.1	N/A (used implicitly)	Java Card internal. No conflict.
FPT_FLS.1	FPT_FLS.1	TOE SFR based on platform SFR.
FPT_TDC.1	N/A (used implicitly)	Java Card internal. No conflict.
FIA_ATD.1/AID	N/A (used implicitly).	Java Card internal. No conflict.
FIA_UID.2/AID	N/A (used implicitly).	Java Card internal. No conflict.
FIA_USB.1/AID	N/A (used implicitly).	Java Card internal. No conflict.
FMT_MTD.1/JCRE	N/A (used implicitly).	Java Card internal. No conflict.
FMT_MTD.3/JCRE	N/A (used implicitly).	Java Card internal. No conflict.
FDP_ITC.2/Installer	N/A (used implicitly).	Java Card internal. No conflict.
FMT_SMR.1/Installer	N/A (used implicitly).	Java Card internal. No conflict.
FPT_RCV.3/Installer	N/A (used implicitly).	Java Card internal. No conflict.
FPT_FLS.1/Installer	N/A (used implicitly).	Java Card internal. No conflict.

[1]Because FCS_COP.1.1/JCAPI/RSA-SIG supports only SHA-1 for ISO 9796-2 the TOE instead makes use of FCS_COP.1.1/JCAPI/RSA-DEC for signature generation (SHA-2 family also supported).

Platform SFR	Corresponding SFR	Remarks
FDP_ACC.2/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FDP_ACF.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FDP_RIP.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FMT_MSA.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FMT_MSA.3/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FMT_SMF.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FMT_SMR.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FPT_FLS.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FDP_RIP.1/ODEL	FDP_RIP.1	TOE SFR based on platform SFR.
FPT_FLS.1/ODEL	FPT_FLS.1	TOE SFR based on platform SFR.
FDP_UIT.1/CCM	N/A (used implicitly)	Java Card internal. No conflict.
FDP_ROL.1/CCM	N/A (used implicitly)	Java Card internal. No conflict.
FDP_ITC.2/CCM	N/A (used implicitly)	Java Card internal. No conflict.
FPT_FLS.1/CCM	N/A (used implicitly)	Java Card internal. No conflict.
FCS_COP.1/DAP	N/A (used implicitly)	Java Card internal. No conflict.
FDP_ACC.1/SD	N/A (used implicitly)	Java Card internal. No conflict.
FDP_ACF.1/SD	N/A (used implicitly)	Java Card internal. No conflict.
FMT_MSA.1/SD	N/A (used implicitly)	Java Card internal. No conflict.
FMT_MSA.3/SD	N/A (used implicitly)	Java Card internal. No conflict.
FMT_SMF.1/SD	N/A (used implicitly)	Java Card internal. No conflict.
FMT_SMR.1/SD	N/A (used implicitly)	Java Card internal. No conflict.
FTP_ITC.1/SC	N/A (used implicitly)	Java Card internal. No conflict.
FCO_NRO.2/SC	N/A (used implicitly)	Java Card internal. No conflict.
FDP_IFC.2/SC	N/A (used implicitly)	Java Card internal. No conflict.
FDP_IFF.1/SC	N/A (used implicitly)	GlobalPlatform. No conflict.
FMT_MSA.1/SC	N/A (used implicitly)	GlobalPlatform. No conflict.
FMT_MSA.3/SC	N/A (used implicitly)	GlobalPlatform. No conflict.
FMT_SMF.1/SC	N/A (used implicitly)	GlobalPlatform. No conflict.
FIA_UID.1/SC	N/A (used implicitly)	Java Card internal. No conflict.
FIA_UAU.1/SC	N/A (used implicitly)	Java Card internal. No conflict.
FIA_UAU.4/SC	N/A (used implicitly)	Java Card internal. No conflict.
FPT_PHP.3	FPT_PHP.3	TOE SFR based on platform SFR.
FPT_TST.1	FPT_TST.1	TOE SFR based on platform SFR.
FCS_RNG.1	FCS_RND.1	The TOE makes use of random numbers according to AIS 31 Class PTG.3. The platform provides random numbers with the defined quality metric to be used directly.

Table 10.7: Correspondence and Relevance of Platform and Composite SFRs

10.3.4 TOE Security Environment

This Security Target considers the assumptions and objectives for the operational environment of the protection profiles [CC_PP-0059], [CC_PP-0071], [CC_PP-0072], [CC_PP-0075], [CC_PP-0076], and the Security Target of the platform [SECORA_ST-SLJ52].

10.3.4.1 Relevance of Platform Security Objectives for the Operational Environment

Significant Platform Security Objectives for the Operational Environment must be considered.

Platform Objective for the Environment	Relevance for Composite ST
OE.APPLET	According to OE.APPLET applets loaded post-issuance must not contain native methods. The user guidance contains respective directives.
OE.VERIFICATION	According to OE.VERIFICATION all the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. Additionally, the applet shall follow all the recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform. The user guidance contains respective directives.
OE.CODE-EVIDENCE	According to OE.CODE-EVIDENCE for application code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that loaded application has not been changed since the code verifications required in OE.VERIFICATION. For application code loaded post-issuance and verified off-card according to the requirements of OE.VERIFICATION, the verification authority shall provide digital evidence to the TOE that the application code has not been modified after the code verification and that he is the actor who performed code verification. For application code loaded post-issuance and partially or entirely verified on-card, technical measures must ensure that the verification required in OE.VERIFICATION are performed. On-card bytecode verifier is out of the scope of this Security Target. All this is achieved by making use of a checksum along with respective instructions in the user guidance.

Table 10.8: Platform Security Objectives for the Operational Environment

10.3.4.2 Assurance Requirements

The level of assurance of the

- MaskTech eSign Applet on Secora™ ID S v1.1 is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5
- JavaCard platform is EAL6 augmented with ALC_FLR.1
- Hardware (Infineon Technologies AG, IFX_CCI_000005) is EAL6 augmented

This shows that the Assurance Requirements of the TOE is matched or exceeded by the Assurance Requirements of the platform and hardware. There are no conflicts.

10.3.5 Conclusion

Overall no contradictions between the Security Targets of the TOE, the JavaCard platform and the hardware can be found.

11 Bibliography

[AGD_eSign] MaskTech eSign Applet on Secora™ ID S v1.1 User Manual, MaskTech International GmbH, Version 1.08, 2022-09-08.

[BSI_AIS31] Anwendungshinweise und Interpretationen zum Schema – Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, BSI, AIS 31, Version 3, 2013-05-15.

[BSI_TR-03110-1] TR-03110-1, Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.20, 2015-02-26.

[BSI_TR-03110-2] TR-03110-2, 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), BSI, Version 2.21, 2016-12-21.

[BSI_TR-03111] TR-03111, Technical Guideline TR-03111: Elliptic Curve Cryptography, BSI, Version 2.1, 2018-06-01.

[CC_Part1] CCMB-2017-04-001, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Common Criteria Maintenance Board, 2017-04.

[CC_Part2] CCMB-2017-04-002, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Common Criteria Maintenance Board, 2017-04.

[CC_Part3] CCMB-2017-04-003, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Common Criteria Maintenance Board, 2017-04.

[CC_PartEM] CCMB-2017-04-004, Version 3.1, Revision 5, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CC_PP-0056-V2] BSI-CC-PP-0056-V2-2012-MA-02, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application', Extended Access Control with PACE, BSI, Version 1.3.2, 2012-12-05.

[CC_PP-0059] BSI-CC-PP-0059-2009-MA-02, Protection profiles for Secure signature creation device – Part 2: Device with key generation, Information Society Standardization System CEN/ISSS, EN 419211-2:2013, 2016-06-30.

[CC_PP-0068-V2] BSI-CC-PP-0068-V2-2011-MA-01, Common Criteria Protection Profile / Machine Readable Travel Document using Standard Inspection Procedure with PACE (ePass_PACE PP), BSI, Version 1.01, 2014-07-22.

[CC_PP-0071] BSI-CC-PP-0071-2012-MA-01, Protection profiles for Secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, Information Society Standardization System CEN/ISSS, EN 419211-4:2013, 2016-06-30.

[CC_PP-0072] BSI-CC-PP-0072-2012-MA-01, Protection profiles for Secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, Information Society Standardization System CEN/ISSS, EN 419211-5:2013, 2016-06-30.

[CC_PP-0075] BSI-CC-PP-0075-2012-MA-01, Protection profiles for Secure signature creation device – Part 3: Device with key import, Information Society Standardization System CEN/ISSS, EN 419211-3:2013, 2016-06-30.

[CC_PP-0076] BSI-CC-PP-0076-2013-MA-01, Protection profiles for Secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application, Information Society Standardization System CEN/ISSS, EN 419211-6:2014, 2016-06-30.

[CC_PP-0084] BSI-CC-PP-0084-2014, Security IC Platform Protection Profile with Augmentation Packages, EUROSMART, Version 1.0, 2014-01-13.

[CC_PP-0086] BSI-CC-PP-0086-2015, Common Criteria Protection Profile / Electronic document implementing Extended Access Control Version 2 (EAC2) based on BSI TR-03110 (EAC2_PP), BSI, Version 1.01, 2015-05-20.

[CID_2016/650] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, European Commission, 2016.

[DIR_1999/93/EC] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures, European Parliament, 2000.

[FIPS_140-3] FIPS PUB 140-3, Security Requirements for Cryprographic Modules, National Institute of Standards and Technology, 2019-03.

[GP] GPC_SPE_034, GlobalPlatform Card - Card specification Version 2.3.1, GlobalPlatform, March 2018.

[GP_SCP03] GPC_SPE_014, GlobalPlatform Technology - Secure Channel Protocol '03' - Card Specification v2.3 - Amendment D - Version 1.2, GlobalPlatform, April 2020.

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, ICAO, 2021.

[ICAO_9303_11] ICAO Doc 9303, Machine Readable Travel Documents: Part 11 – Security Mechanisms for MRTDs, ICAO, 2021.

[ICAO_SAC] Technical Report: Supplemental Access Control for Machine Readable Travel Documents, ICAO, TR-SAC V1.1, 2014-04-15.

[ISO_14443] ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Multipart Standard, ISO/IEC, 2016-2018.

[ISO_7816-3] ISO/IEC 7816-3:2006, Identification cards – Integrated circuit cards – Part 3: Cards with contacts – Electrical interface and transmission protocols, ISO/IEC, 2006-10.

[NIST_SP800-38A] NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, National Institute of Standards and Technology, 2001-12.

[PKCS_15] PKCS #15: Cryptographic Token Information Syntax Standard, Version 1.1, 2000-06-06.

[REG_910/2014] 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, European Parliament, 2014.

[RFC_8017] RFC 8017, PKCS #1: RSA Cryptography Specifications Version 2.2, K. Moriarty (Ed.), B. Kaliski, J. Johnson, and A. Rusch, 2016-11.

[SC_HID] BSI-DSZ-CC-S-0183-2021, HID Global GmbH, Site Security Target Lite of HID Global Ireland Teoranta in Galway, Ireland, Doc. No: F-10-138d, Rev. B, 2018-09-13.

[SC_HID_MY] BSI-DSZ-CC-S-0189-2021, HID Global GmbH, Site Security Target Lite for HID Global Malaysia, PRO-01286 Rev D2, 2020-04-17.

[SC_Linxens] BSI-DSZ-CC-S-0207-2021, Linxens (Thailand) Co Ltd., Site Security Target LITE for Linxens Thailand, Version 2.4, 2021-11-24.

[SECORA_ST-SLJ52] Infineon Technologies AG, Secora™ ID S v1.1 (SLJ52GxxyyyzS) Security Target.

12 Revision History

Version	Date	Author	Changes
1.0	2022-06-07	Thomas Rölz	Initial version
1.1	2022-08-24	Thomas Rölz	Updated bibliography
1.2	2022-09-09	Thomas Rölz	Updated bibliography

13 Contact

MaskTech GmbH – **Headquarters**

Nordostpark 45	Phone	+49 911 955149 0
D-90411 Nuernberg	Fax	+49 911 955149 7
Germany	Email	info@masktech.de

MaskTech GmbH – **Support**

Bahnhofstr. 13	Phone	+49 911 955149 0
D-87435 Kempten	Fax	+49 831 5121077 5
Germany	Email	support@masktech.de

MaskTech GmbH – **Sales**

Lauenburger Str. 15	Phone	+49 4151 8990858
D-21493 Schwarzenbek	Fax	+49 4151 8995462
Germany	Email	stimm@masktech.de