Security Target
ACOS-IDv2.0 SSCD (A) CL-TC-Comm

Qualified Signature Creation Device and Qualified Seal Creation Device

according Art. 29 and Art. 39, Regulation (EU) No 910/2014

Document Information

Author: Austria Card Ges.m.b.H. - Thomas Aichinger

Title: Security Target

Version: 1.01 public

Date: 2021-11-16

Company: AUSTRIA CARD-Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Lamezanstraße 4-8, 1230 Vienna, Austria

Classification: **Public**

Document History

Version	Date	Author	Changes
V1.0 public	2021-11-09	AC	References updated; public version
v1.01 public	2021-11-16	AC	References updated

1 Contents

2 Security Target Introduction (ASE_INT)

2.1 ST Reference

Title	Security Target - ACOS-IDv2.0 SSCD (A) CL-TC-Comm
Version	1.01 public
Author	Austria Card Ges.m.b.H.
Compliant to	Common Criteria Protection Profiles: "Protection profiles for secure signature creation device - • Part 2: Device with key generation, Version 2.0.1, BSI-CC-PP-0059-2009-MA-01" [1] ("PP SSCD KG" or "PP-Part 2") • Part 3: Device with key import, Version 1.0.2, BSI-CC-PP-0075" [2] ("PP SSCD KI" or "PP-Part 3") • Part 4: Extension for device with key generation and trusted channel to certificate generation application, Version 1.01, BSI-CC-PP-0071" [3] ("PP SSCD KG TCCGA" or "PP-Part 4") • Part 5: Extension for device with key generation and trusted channel to signature creation application, Version 1.01, BSI-CC-PP-0072" [4] ("PP SSCD KG TCSCA" or "PP-Part 5") • Part 6: Extension for device with key import and trusted channel to signature creation application, Version 1.0.4, BSI-CC-PP-0076" [5] ("PP SSCD KI TCSCA" or "PP-Part 6")
CC Version	3.1 Revision 5
Certification ID	ACOS-IDv2.0 SSCD
Assurance Level	EAL4+
Keywords	secure signature creation device, electronic signature, digital signature, key import, trusted communication with signature creation application

The term "CL-TC-COMM" means that this security target is applicable when the TOE is operated via contactless interface. The use of a trusted channel for communication between the SCA/HID and the TOE to protect the DTBS/R and VAD is provided and required by the TOE.

Note that the Protection Profiles mentioned above are referencing "*Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures*" [6] with the term "the directive". The directive was repealed by "*Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic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*" [31] begin of 2016 (called "eIDAS regulation" in the following). References to the repealed Directive shall be construed as references to eIDAS regulation.

2.2 TOE Reference

TOE Name	ACOS-IDv2.0 SSCD (A) CL-TC-Comm
TOE Developer	Austria Card Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Lamezanstraße 4-8, 1230 Wien, Austria
IC Developer	Infineon Technologies AG

TOE Hardware	Infineon Security Controller IFX_CCI_000005h H13 and IFX_CCI_000008h H13, BSI-DSZ-CC-1110-V4-2021
TOE Version	v2.0 SSSD (A)
TOE Configurations	"Configuration A" and "Configuration B" are covered by this Security Target. The configuration[1] is defined once in the Preparation Stage by an Administrator. Note that there is also a "Configuration C" which is not covered by this security Target.

This Security Target is applicable when the TOE is operated via contactless interface. Please note that for use via contact based interface another Security Target is valid [7].

2.3 TOE Overview

This Security Target defines security requirements for secure signature and seal creation devices (SSCD, QSCD) with the following functionality

- key (SCD) generation and core requirements as described in [1] (PP SSCD KG)
- key (SCD) import and core requirements as described in [2] (PP SSCD KI)
- trusted communication with certificate generation application (TCCGA), as described in [3] (PP SSCD KG TCCGA)
- creation of any type of digital signature and specifically digital signature to be used for (qualified or advanced) electronic signatures, as described in [1] (PP SSCD KG) and in [2] (PP SSCD KI)
- trusted communication with signature creation application (TCSCA), as described in [4] (PP SSCD KG TCSCA) and [5] (PP SSCD KI TCSCA) to protect authentication data and data to be signed

These security features allow using the TOE in a complex operational environment.

This Security Target is applicable when the TOE is operated via contactless interface only. Please note that for use via contact based interface another Security Target is valid [7].

The TOE is designed and implemented to fulfil "*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*" [31] ("eIDAS regulation"), in particular the TOE fulfils the requirements and is certified as

- a qualified signature creation device according Article 29 and
- a qualified seal creation device according Article 39.

Notes: this includes also the creation of advanced signatures.

The cryptographic algorithms and cryptographic key sizes and other cryptographic parameters are chosen in accordance with ANSSI-PG-083 [8] and SOGIS Agreed Cryptographic Mechanisms [9].

2.3.1 Operation of the TOE

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

[1] Configurations are explained further in chapter: 2.3.4 and 3.2

- The preparation environment, where it interacts with a certification service provider through a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with the SCD the TOE has generated. The initialisation environment interacts further with the TOE to personalise it with the initial value[2] of the reference authentication data (RAD).
- The signing environment where it interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation application provides the data to be signed (DTBS), or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting digital signature[3]).
- The management environments where it interacts with the user or an SSCD-provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

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

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case, the TOE provides a function to identify each SCD and the SCA can provide an interface to the signer to select an SCD for use in the signature creation function of the SSCD. The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. The digital signature created by the TOE may be used to create an advanced electronic signature as defined in Article 5.1 of the directive. Determining the state of the certificate as qualified is beyond the scope of this Security Target.

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.

Protection of the VAD and DTBS/R: the TOE provides trusted channel capabilities for further protection of the VAD and DTBS/R, which are PACE authentication and Secure Messaging as described below.

Secure Transfer of VAD and DTBS/R: in Configuration A and B the TOE provides trusted channel capabilities, which are PACE authentication and Secure Messaging, for protection of the VAD and DTBS/R when they are transferred over the contactless interface.

The TOE requires the SCA or HID to make use of trusted channel capabilities for transfer of the VAD and DTBS/R when the contactless interface is used.

[2] Note that the term “initial value of the RAD” stored during preparation refers to the value of the “transport pin” (T-PIN) and includes value of the PUK as well. Those are described further in chapter 2.3.4.2

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

Since Configuration B is also conformant to the ACOS-ID eMRTD certification (see Security Target [10]) it requires in addition PACE and Secure Messaging to be used for selection of the SSCD application. This secure channel is conformant to both the eMRTD and the SSCD certification.

Note: this ST does not cover Configuration C of the TOE, since the SSCD application cannot be used via the contactless interface in Configuration C.

The TOE stores signatory reference authentication data to authenticate a user as its signatory. The RAD is a password, e.g. PIN. The TOE protects the confidentiality and integrity of the RAD. The TOE provides a user interface to either directly receive verification authentication data (VAD) from the user or alternatively 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 include:

- initialising the RAD;
- generating or importing at least one key pair
- (optional) storing personal information of the legitimate user.

The TOE may be in any form factor, 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.

2.3.2 TOE Definition

The TOE ACOS-IDv2.0 SSCD is a chip operating system including applications (software) compliant to ISO 7816-3 [11], ISO 7816-4 [12], ISO 7816-8 [13], ISO 7816-9 [14], ISO 14443 [15] [16] [17] , BSI TR-03110 [18] and EN 419212 [19] and [20], ICAO Doc 9303 [21] and [18]. It provides multi-application support (e.g. Signature application, ePassport / ID Card application, access control- and health-applications). The operating system and applications run on Infineon Security Controller IFX_CCI_000005h H13 and IFX_CCI_000008h H13 including software packages [22].

The TOE is a composition of ACOS-IDv2.0 operating system and applications (software) and a secure chip (hardware) including its associated software packages (software).

The secure chip and software packages (e.g. libraries) are certified according to CC EAL 6+ according to the Protection Profile BSI-CC-PP-0084-2014 [23] (see [24]).

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

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

The TOE provides the following functions:

a) to generate signature creation data (SCD) and the correspondent signature-verification data (SVD);
b) to export the SVD for certification through a trusted channel to the CGA;
c) to prove the identity as SSCD to external entities;
d) to import signature creation data (SCD) and, optionally, the correspondent signature verification data (SVD);
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 an SCD if multiple are present in the SSCD;
    2) authenticate the signatory and determine its intent to sign;
    3) receive data to be signed or a unique representation thereof (DTBS/R) and VAD optionally through a trusted channel with SCA;
    4) apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R.
h) to, optionally receive, store and send any other data (stored in additional EFs) in any state

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

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

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

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

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

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

The TOE provides multi-application support, i.e., installation of one or more additional multi-purpose applications (MPA) on one chip is possible. MPA applications might be – but not limited to – eMRTD, eDL, Access or eHealth applications. Installation of additional SSCD applications in certified configuration or non-certified IAS applications (identification, authentication and signature) is also possible.

To ensure that the security objectives of the SSCD application still hold, restrictions and minimum requirements for the MPA applications (e.g. necessary access conditions for contained files, keys) are defined and evaluated to prove their correctness as a part of the evaluation. The application separation (access control / access conditions) provided by the OS ensures that no inference with the SSCD application is possible.

In case of Configuration B the MPA application might be an eMRTD application in a certified configuration, which is additionally supported by the composite product. The eMRTD application is evaluated and certified in another parallel process using a separate Security Target [10].

The TOE supports contact based T=1 (according ISO/IEC7816-3) and contactless T=CL Type A (according to ISO/IEC14443) communication protocols.

The following “Figure 1: TOE Block Diagram” gives an overview of the TOE and its borders and the scope of the evaluation.

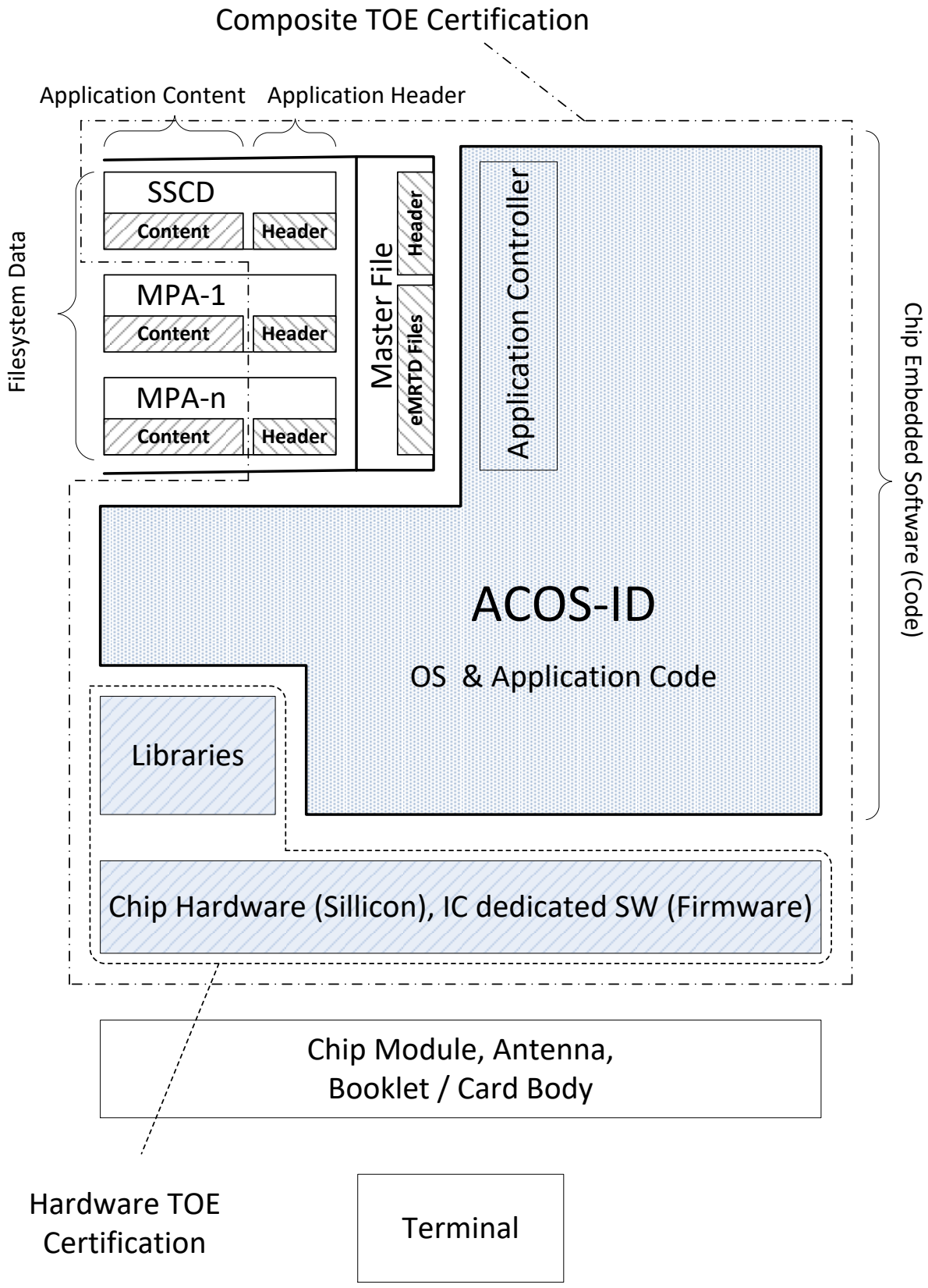


Figure 1: TOE Block Diagram

2.3.3 Scope

"Figure *1: TOE Block Diagram*" together with "*Table 1:* Components and Scope" define the scope of the TOE. The latter gives more details and also divided the physical versus the logical scope.

Component	**In Scope of TOE (physical / logical)**	**Covered by**
Chip Hardware (Silicon) and IC dedicated Software (Firmware)	Yes (physical)	Chip hardware certification
Libraries (from secure chip hardware vendor)	Yes (logical)	Chip hardware certification
ACOS-ID Operation System and Application Code (IC Embedded Software) including Application Controller	Yes (logical)	Composite certification
Master File, application header and SSCD related files / keys	Yes (logical)	Composite certification
SSCD, MPA-1 … MPA-n Application Header	Yes (logical)	Composite certification
SSCD Application Content, including SSCD file/key headers	Yes (logical)	Composite certification
Guidance Documentation	Yes (physical)	Composite certification
MPA-1 … MPA-n Application Content	No	n/a
Chip Module, Bonding Wires, Antenna, Booklet / Card Body (all optional)	No	n/a
Terminal	No	n/a

Table 1: Components and Scope

From the communication (Operating System to Terminal) perspective the logical scope ends at the input / output interface of the Operating System, which is the APDU-Interface (Application Protocol Data Unit) consisting of all commands supported by the operating system. Any APDU command is received by the input interface and any response APDU is sent via the output interface.

In the scope of this ST all APDUs (commands and responses) are physically transmitted over the contactless interface, represented by connections on the Chip Hardware (pads on silicon).

2.3.4 TOE Life-Cycle

This Life-Cycle (LC) description takes into account the description in the five underlying PPs.
Overview

The following LC description is mainly taken from PP SSCD KG and combined with the relevant parts taken from the description in PP SSCD KI and additionally all modifications from PP SSCD KG TCCGA. PP SSCD KG TCSCA and PP SSCD KI TCSCA just refer to the former ones, but make no modifications regarding life-cycle.

Further additions / modifications of the LC are written in "black" colour.

The TOE lifecycle distinguishes (“Development Phase”), “Usage” as well as a “Termination” phase.

The “Development Phase” is further separated into

- “SSCD Development”
- “SSCD Production”

The “Usage” Phase is further separated into

- “SSCD preparation”
- “SSCD operational use”

The following Figures (Figure 2 and Figure 3) give an overview of the LC in case of key generating (PP SSCD KG) or key import (PP SSCD KI) respectively.

Note: Figure 2 and Figure 3 show examples of the lifecycle where an SCD or SCD/SVD pair is generated/imported from SSCD- provisioning service before delivery to the signatory. The lifecycle also allows generation/import of SCD or SCD/SVD key pairs after delivery to the signatory as well. Note that it is not required to generate / import SCD/SVD pair or SCD before delivery to the signatory.

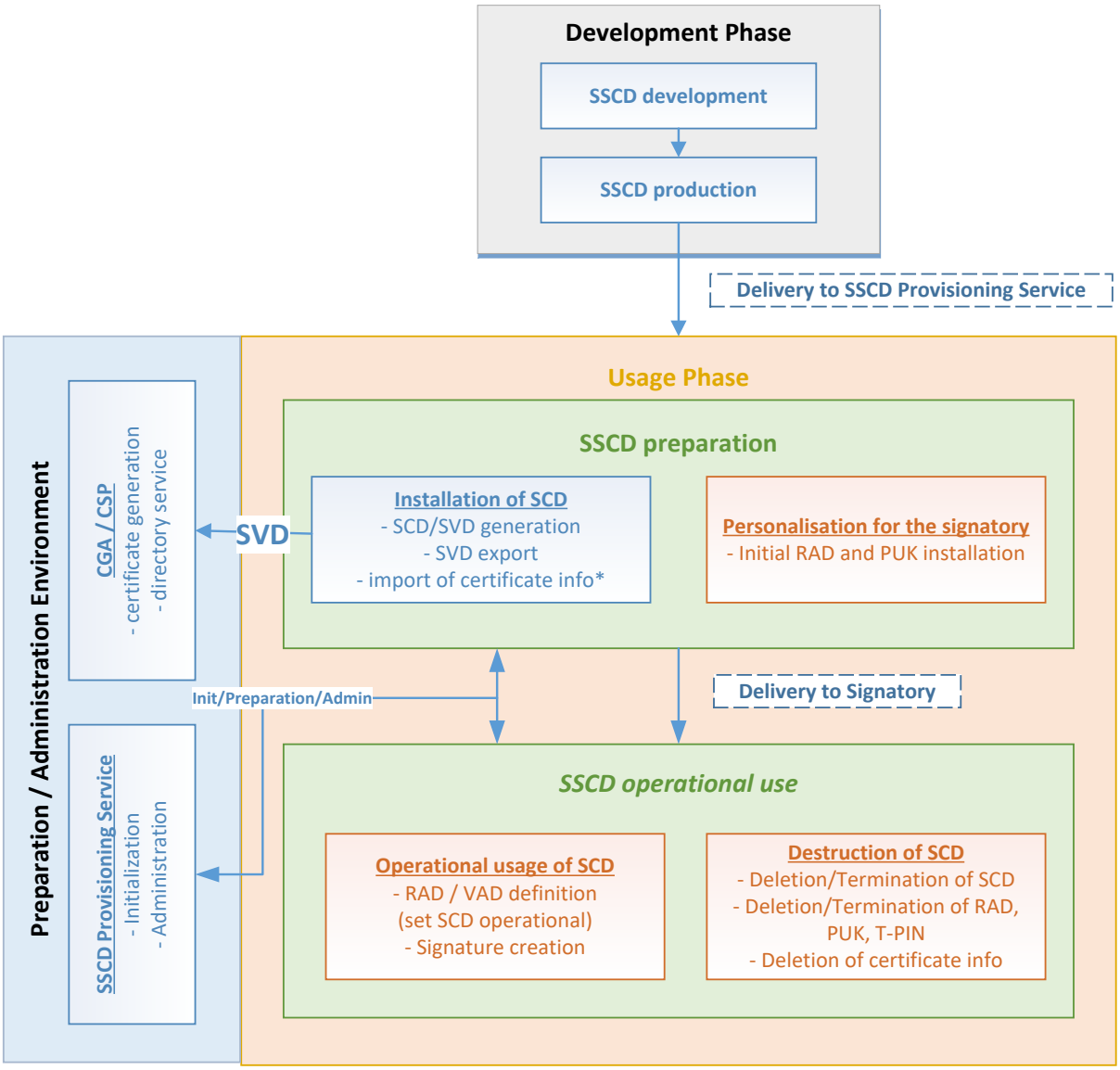


Figure 2: LC Overview with KG

*) optional

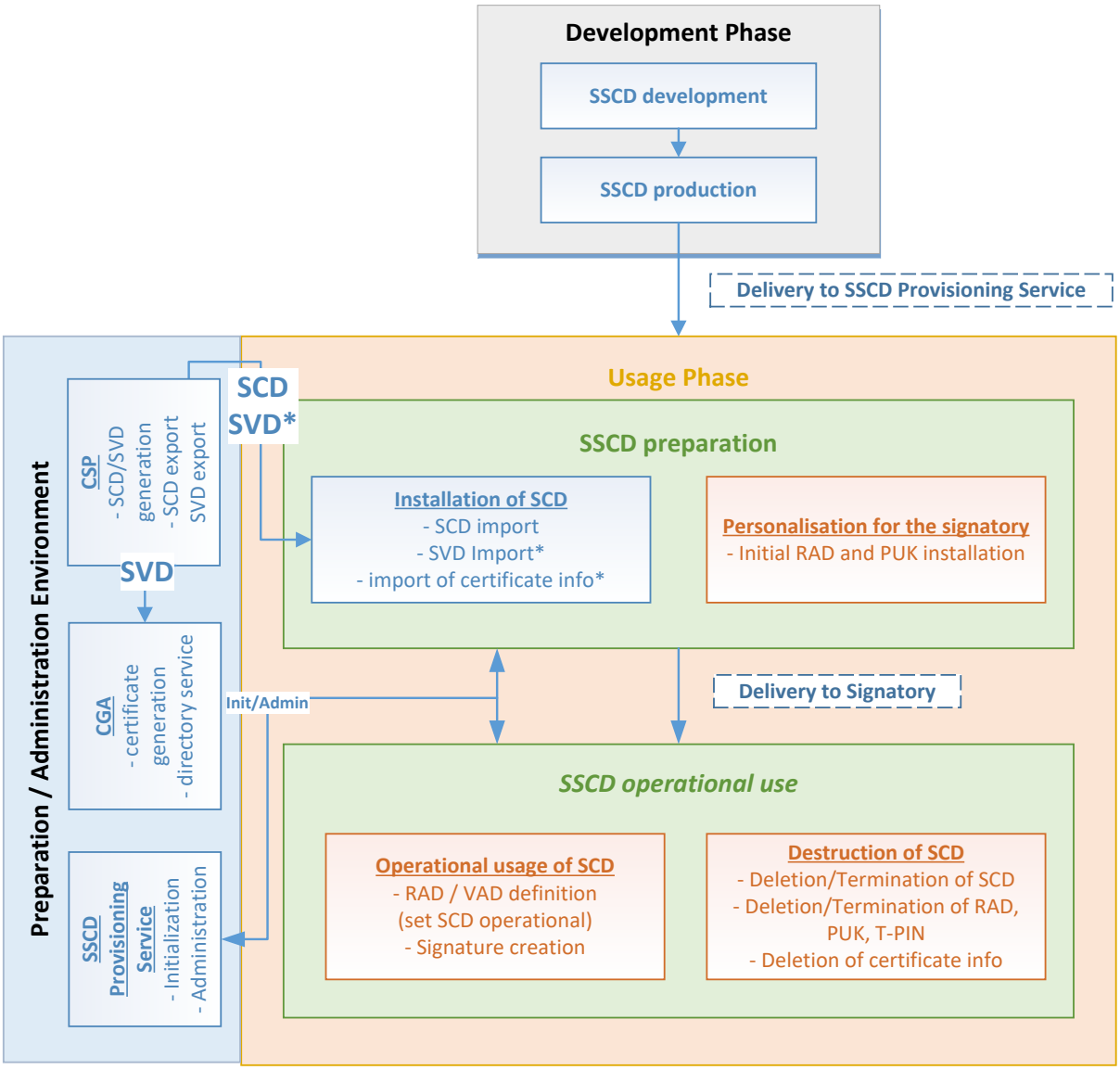


Figure 3: LC Overview with KI

*) optional

The Development Phase comprises the development and production of the TOE. The Development Phase is subject of the evaluation according to the assurance lifecycle (ALC) class. The Development Phase ends with the delivery of the TOE to the SSCD-provisioning service.

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

In the SSCD operational phase the SSCD preparation steps may be repeated by the CSP to install additional SCD/SVD or to replace existing SCD/SVD after their termination/deletion.

Any TOE phase may end up in a final Termination Phase if the TOE's security mechanisms observe an attack, critical operating environment conditions or malfunction.

The Usage Phase after TOE delivery have been considered in the product evaluation process under AGD assurance class.

The Signatory or the SSCD Provisioning Service can make a SCD/SVD pair un-usable at any time.

The following table gives an overview of important objects located inside the SSCD application and their management and use.

	SSCD Preparation / Operational Use (1)		SSCD Operational Use			
Object	Initial Creation / Import / Export	Use	Change / Import	Use	Terminate	Delete
Initial RAD (T-PIN) (2)	Admin	Signatory (to set SCD operational and define RAD)	-	-	Admin	Signatory
RAD	-	-	Signatory	Signatory	Admin	Signatory
PUK	Admin	-	-	Signatory	Admin	Signatory
SCD	Admin	-	-	Signatory	Admin	Signatory
SVD	Admin	-	-	Signatory (export)	Admin	Signatory
AUTHKEYS	Admin	Any User	Admin	Any User	Admin	Admin
Additional Files (e.g. certificate files)	Admin	Admin	(3)	(3)	(3)	(3)

Notes:

1) Additional SCD with associated RAD, T-PIN and PUK can be installed during “SSCD Operation Use” but at least one must be installed during “SSCD Preparation”. Each SCD is associated with exactly one RAD, T-PIN and one optional PUK.
2) The initial RAD value refer to a Transport PIN value (T-PIN). The signatory uses the T-PIN to define the signatory PIN and set the SCD to operational. The T-PIN only be used once and cannot be used to create signatures using SCD.
3) The Admin defines Access Rules during initial creation; those rules may include Admin, Signatory, Any User and Nobody.

2.3.4.1 Development Phase

The roles relevant for the Development Phase are defined as follows:

1) IC developer: Infineon Technology AG (as defined by the IC Certificate)
2) IC Manufacturer: Production Sites in charge of Infineon (as defined by the IC Certificate)
3) IC Embedded Software Developer: Austria Card-Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Lamezanstraße 4-8, 1230 Wien, Austria (Development Site as covered by Site Certificate BSI-DSZ-CC-S-0153)

The TOE makes use of a Flash-Technology IC product in combination with “Loader functionality” (provided by the “secure flash loader package” of the IC / IC dedicated software), which is a

dedicated secure method, covered by the IC certification , see also “Package Loader, Package 1” and “Package Loader, Package 2” acc. [25]) to load the IC Embedded Software. The IC Security Target [25] addresses this topic in “P.Lim_Block_Loader” and “P.Ctrl_Loader”. See also [25] Annex 7, especially Table 17 and Application Note 32.

Delivery and Loading Options

IC Embedded Software (ACOS-ID Operation System and Application Code, Libraries) reside in non-volatile programmable memory (Flash). Therefore the IC Embedded Software may either be written by

- Option a) the IC Manufacturer or by
- Option b) the SSCD-Provisioning Service using the “Loader functionality”

In both cases Austria Card delivers the Guidance Documentation of the TOE (including ePassport application TSF data), initialization data as well as necessary keys to the SSCD-Provisioning Service. Additionally

in case of Option a)

- the IC including the IC embedded software is delivered to the SSCD-Provisioning Service

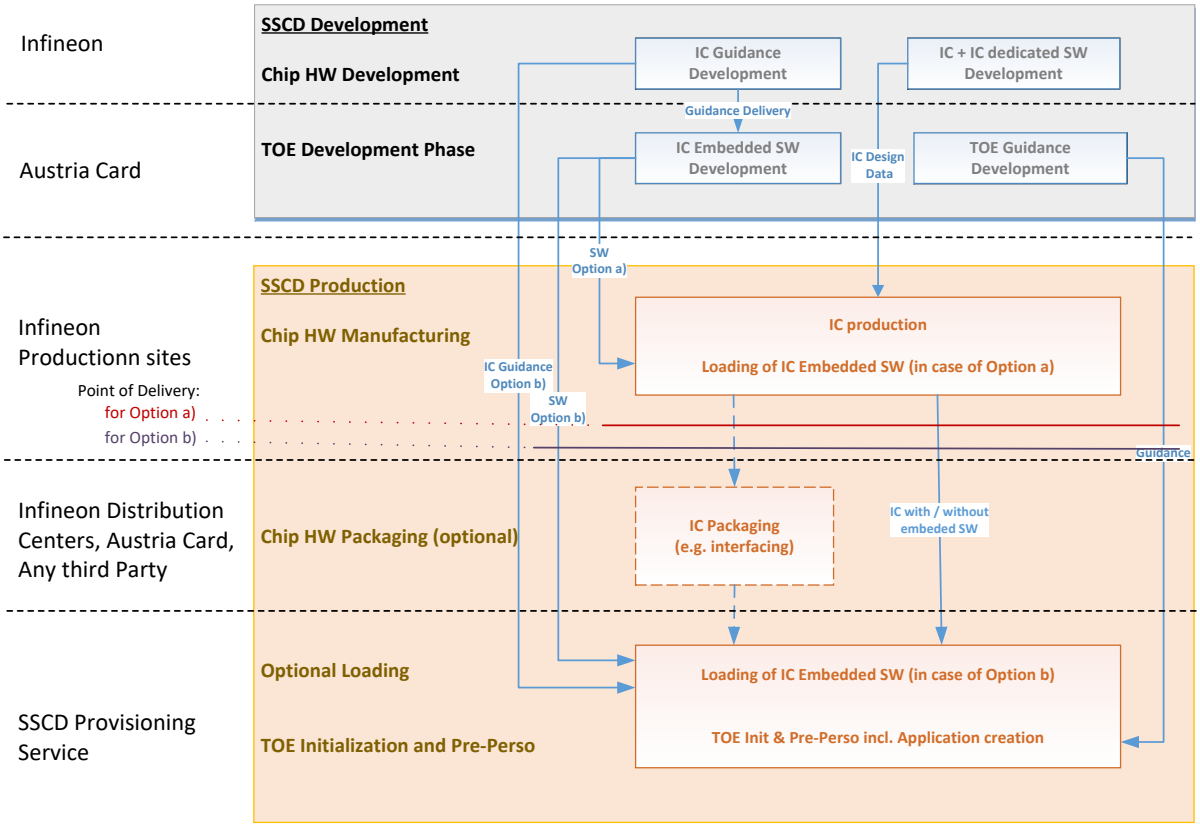
in Case of Option b)

- the IC Embedded Software is delivered from Austria Card to the SSCD-Provisioning Service.
- the IC without the IC embedded software is delivered to the SSCD-Provisioning Service
- For acceptance, processing of the IC and loading the SSCD-Provisioning Service follows the Guidance Documentation of the IC
- Directly after successfully loading the IC Embedded Software the TOE exists for the first time and the SSCD-Provisioning Service follows the guidance documentation of the TOE.

For both Options the IC is delivered from Production Sites via “Distribution Centers” – both in charge of Infineon (as defined in the IC certification) - to the SSCD-Provisioning Service or from Production Sites via “Distribution Centers” – both in charge of Infineon (as defined in the IC certification) - to Austria Card and from Austria Card to the SSCD-Provisioning Service.

This ST considers the Development Phase as part of the evaluation (under ALC class) and therefore to define the TOE delivery according to CC directly after the Development Phase (which includes the development and production of the IC).

The following diagram gives an overview of the Development Phase of the TOE.



2.3.4.2 Preparation stage

The SSCD provisioning service may be any entity authorized by Austria Card and may interact with a CSP (operating the CGA).

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

During preparation of the TOE, as specified above, an SSCD-provisioning service provider performs the following tasks (Note that only actions 5) and 6) are including the TOE itself):

1) Obtain information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user of the TOE.
2) Generate one or more PIN(s) / Password(s) to store this data as initial RAD in the TOE later)
3) Optionally generate one or more PUKs for unblocking the associated RAD (to store this data in the TOE later)
4) Link 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.
5) Initialize the TOE, including i.e.
   a) Initialising 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
   b) and at least one from i) or ii) or both or more
      i) the TOE generating an SCD/SVD pair and exporting SVD from the TOE; and/or

ii) the CSP generates the SCD/SVD pair by means of a SCD/SVD generation device, loads the SCD and optionally also SVD to the TOE, and sends the SVD to the CGA. The TOE may import and store the SCD/SVD pair.

6) The personalisation of the TOE for use by the signatory
   a) the installation of the initial RAD in the TOE
   b) Optionally the installation of the PUK(s) in the TOE associated to the RAD
7) The generation of (qualified) certificate(s) containing among others (cf. the directive, Annex II)
   a) the SVD which correspond to SCD under the control of the signatory;
   b) the name of the signatory or a pseudonym, which is to be identified as such,
   c) an indication of the beginning and end of the period of validity of the certificate.
8) optional loading of the certificate info into the SSCD for signatory convenience (alternatively this can be done in the operational phase)
9) prepare information about the VAD (of the initial RAD) and optional PUK(s) for delivery to the legitimate user / signatory and handover of VAD and optional PUK(s) to the legitimate user / signatory

In this stage the SSCD provision service also defines the Configuration of the TOE (Configuration A or B) by setting the appropriate access conditions according to the TOE Guidance.

Notes:

(1) The initial RAD / VAD mentioned in 2) and 9) refer to a Transport PIN (T-PIN). The signatory uses the Transport PIN to define the signatory PIN and set the SCD to operational.
(2) Each SCD is associated with exactly one RAD, T-PIN and one optional PUK

Details on CSP/Certificate related tasks

In case of 5) b) ii) the CSP ensures

a) that before generating a (qualified) certificate, the SCD is stored in the SSCD
b) the correspondence between SCD and SVD,
c) that algorithm and key size for the SVD are appropriate,

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

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

This ST requires the TOE to provide mechanisms for import of SCD, implementation of the SCD, generation of SCD, export of SVD and personalisation (import RAD, PUK(s)). The data transmission between the TOE and the CGA / Provisioning Service is performed by a secure channel (ensuring integrity, authenticity and confidentiality).

The environment is assumed to protect all other processes (except the TOE itself and the transmission between TOE and CGA / Provisioning Service) for TOE preparation.

The SVD certification task (item 7) listed above) of an SSCD-provisioning service provider as specified in this ST may support a centralised, pre-issuing key generation process, with at least one key generated and certified, before delivery to the legitimate user. Additionally, that task supports key

generation by the signatory after delivery and outside the secure preparation environment. The TOE supports both key generation processes, for example with a first key generated centrally and additional keys generated by the signatory in the operational use stage.

Data required for inclusion in the SVD certificate at least includes (cf. the directive, Annex II)

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

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

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

a) establishing the sender as genuine SSCD;
b) establishing the integrity of the SVD to be certified as sent by the originating SSCD;
c) establishing that the originating SSCD has been personalised for the legitimate user;
d) establishing correspondence between SCD and SVD; and
e) an assertion that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

The proof of correspondence between an SCD stored in the TOE and an SVD is performed implicitly in the security mechanisms applied by the CGA. The TOE does not provide an additional function for explicit proof of correspondence.

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

2.3.4.3 Operational Use Stage

In this lifecycle stage the signatory can use the TOE to create advanced / qualified electronic signatures and seals.

The operational phase of the TOE starts when at least one SCD/SVD pair has been generated or imported (in the preparation stage and/or in the operational stage) either

- by the TOE and SVD exported from the TOE and/or
- by the CSP and the SCD is imported into the SSCD

and when the signatory takes control over the TOE, obtains the initial VAD and has made the SCD operational.

The TOE provides a trusted channel to the CGA protecting the authenticity, integrity and confidentiality of the SCD/SVD during transfer.

Further SCD/SVD generation by the TOE and SVD export from the TOE as well as generation by the CGA and import to the TOE may take place in the in the operational use stage. The TOE then provides a trusted channel to the CGA protecting the integrity, authenticity and confidentiality of the SCD/SVD. For an additional key the signatory is allowed to choose the kind of certificate (qualified, or not) to obtain for the SVD of the new key. The signatory is also 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[4]. If the conditions to obtain a qualified certificate are met, the new key can also be used to create advanced electronic signatures. These TOE functions for additional key generation and certification are the same as used for initial SCD.

The SSCD Provisioning Service can render an SCD in the TOE permanently unusable (by terminating the RAD and/or SCD).

The Signatory can destroy SCD and the associated RAD, T-PIN and PUK.

When SCD and associated objects have been destroyed they can be created again completely newly by the SSCD provisioning service.

Details on CSP/Certificate related tasks

When keys and/or certificates are generated in operational phase the same tasks apply as in the preparational phase.

Details on Signatory related tasks

The signatory uses the TOE with a trustworthy SCA in a secured environment only. The SCA is assumed to protect the DTBS/R during the transmission to the TOE. In addition the TOE enforces the use of a trusted channel to the SCA / HID to protect authenticity, integrity and confidentiality of DTBS/R and VAD.

The signatory can also interact with the SSCD to perform management tasks, e.g. reset a RAD value if the password/PIN in the reference data has been blocked. Such management tasks require a secure environment. The TOE offers a secure channel to the SCA / HID to protect authenticity, integrity and confidentiality of DTBS/R and VAD to support this.

The signatory can render an SCD in the TOE permanently unusable (by deleting the RAD and/or SCD). The TOE life cycle as SSCD ends when all SCD stored in the TOE are destructed or the phase termination is entered. This may include deletion of the corresponding certificates.

2.3.4.4 Termination Phase

If the TOE's security mechanisms observe an attack, critical operating environment conditions or a malfunction it shuts itself down permanently. This state can be reached any time after the IC Embedded Software (operating system) has been installed and initially started (after Development Phase) and is final. Encrypted log data can be read that allow tracing back to cause of the shut-down.

2.3.5 Non-TOE Hardware/Software/Firmware Required by the TOE

The TOE requires specific components in its operational environment for some specific tasks:

- Certificate Generation Application (CGA) interacting with a Certification Service Provider (CSP) to obtain a certificate for the Signature Verification Data (SVD) corresponding to the Signature Creation Data (SCD) either generated by the TOE or by the CSP.
- SSCD Provisioning Services / Applications
    - To initially personalize the TOE it with the initial value of the Reference Authentication Data (RAD) before the TOE is operational.

[4] 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

    - To provide management services/applications for the TOE in operational phase: e.g. for reset a blocked RAD, change of RAD, installation of additional SCD, destruction/deletion of SCD.
- Signature Creation Application (SCA): the SCA provides the data to be signed (DTBS) or a unique representation thereof (DTBS/R) as input to the TOE and initiates the signature creation after authenticating of the signer as Signatory.
- Human Interface Device (HID) to enter the VAD and sent it to the TOE.

Such components may consist of hardware, software and firmware to perform its tasks and for communication to the TOE. They also may be combined in a single device, e.g. a smart card terminal, may provide the required environment for management and signing (including HID for VAD entry).

The CGA, SCA and HID must provide a trusted channel functionality to communicate with the TOE.

In any case those components in the environment (signing / management /preparation environment) are secure and protect data exchanged with the TOE.

Note: the TOE is defined to comprise the hardware chip (silicon) and the complete operating system and application code and SSCD application data. A module (including bonding wires) holding the chip as well as optional antenna and card body / booklet are irrelevant for the secure operation of the TOE and therefore out of scope.

2.3.6 TOE Components

The TOE consists of the following components:

Category	**Definition**
Secure Chip Hardware	Infineon Security Controller IFX_CCI_000005h H13 and IFX_CCI_000008h H13, for certification see [24]
Secure Chip Firmware	80.100.17.3, 80.100.17.2
Secure Chip Vendor Software Libraries	Crypto Library (ACL): v2.08.007 Hardware Support Layer (HSL): 03.12.8812
Operating System	ACOS-IDv2.0 Builds: 0x8C1D, 0x62D7 and 0x9486 Those builds differ in their support of different configurations of the same TOE Hardware (RAM Size, User NVM Size, availability of the Very High Bit Rate (VHBR) feature). The builds and the underlying code are represented by the label “REL_ACOS-IDv2.0_01” in the repository. This chip embedded software version corresponds to the Version Identifier “v2.0” of the TOE (part of the TOE name).
Guidance Documentation	The Guidance consists of the following documents: • “Preparation and Operational Manual - ACOS-IDv2.0 SSCD (A)”, Version v1.01, Date 2021-11-16, [26] • “ACOS-ID User Manual”, Version 2.12, Date 19.05.2021 [27] • “Internal Operation Manual - ACOS-IDv2.0”, Version 1.2, 2021-07-19, [28] (only used Austria Card internal)

	Those documents are represented by the label “REL_ACOS-IDv2.0_SSCD_CC-DOC_01” in the repository. This documentation version is reflected by the text “SSCD (A)” part of the TOE name, where “SSCD” refers to documentation for a specific type of certification and “(A)” to the specific version of the documentation.

3 Conformance Claims (ASE_CCL)

3.1 CC Conformance Claim

This ST claims conformance to the Common Criteria version 3.1 Revision 5, [29] [30] [31] as follows:

- Part 2 extended due to the use of
  - FPT_EMS.1 from [1], [2] and
  - FIA_API.1 from [3]
- Part 3 conformant.

For the evaluation the following methodology is used: [32]

3.2 PP Claim

This Security Target claims strict conformance to the Protection Profiles:

Protection profiles for secure signature creation device -

- Part 2: Device with key generation, Version 2.0.1, BSI-CC-PP-0059-2009-MA-01 [1] (PP SSCD KG)
- Part 3: Device with key import, Version 1.0.2, BSI-CC-PP-0075 [2] (PP SSCD KI)
- Part 4: Extension for device with key generation and trusted channel to certificate generation application, Version 1.01, BSI-CC-PP-0071 [3] (PP SSCD KG TCCGA)
- Part 5: Extension for device with key generation and trusted channel to signature creation application, Version 1.01, BSI-CC-PP-0072 [4] (PP SSCD KG TCSCA)
- Part 6: Extension for device with key import and trusted channel to signature creation application, Version 1.0.4, BSI-CC-PP-0076 [5] (PP SSCD KI TCSCA)

3.3 Package claim

This Security Target is conforming to assurance package EAL4 augmented with:

- AVA_VAN.5

due to [1], [2], [3], [4], [5].

And additionally:

- ALC_CMS.5
- ALC_DVS.2
- ALC_FLR.1
- ALC_TAT.2
- ATE_DPT.2

as defined in CC part 3 [31].

3.4 Conformance Claim Rationale

This Security Target claims strict conformance to the protection profiles to [1], [2], [3], [4], [5] as required.

The chapter Security Problem Definition (ASE_SPD) is the union of the SPD of the claimed PPs without changes.

4 Security Problem Definition (ASE_SPD)

The following chapters 4.1, 4.2, 4.3 and 4.4 (Assets, Threats, Organizational Security Policies, Assumptions) are taken from [1] (identical to the corresponding chapters in [2], [3], [4], [5]) without modification (except typographical and referencing).

4.1 Assets, users and threat agents

ISO/IEC 15408 defines 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.

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 initialisation, TOE personalisation or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.
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.

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 got a high attack potential and knows no secret.

4.2 Threats

4.2.1 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.

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.2.5 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.

4.2.6 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.

4.2.7 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.

4.3 Organisational security policies

4.3.1 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.

4.3.2 P.QSign Qualified electronic signatures

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. the directive, Article 1, Clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the directive Annex I). The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD

implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

4.3.3 P.Sigy_SSCD TOE as secure signature creation device

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

4.3.4 P.Sig_Non-Repud Non-repudiation of signatures

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

4.4 Assumptions

4.4.1 A.CGA Trustworthy certificate generation application

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

4.4.2 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.

4.4.3 A.CSP Secure SCD/SVD management by CSP

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

5 Security objectives

5.1 Security objectives for the TOE

5.1.1 Relation to PP SSCD KG, PP SSCD KI and PP SSCD TCCGA

This Security Target covers all OT from PP SSCD KG [1] and PP SSCD KI [2] and PP SSCD TCCGA [3].

Security objectives for the TOE as stated identically in PP SSCD KG and PP SSCD KI, are OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID and OT.Tamper_Resistance (these are independent from the fact whether SCD are generated by the TOE itself or imported from the operational environment).

The remaining security objectives for the TOE

- OT.SCD/SVD_Auth_gen
- OT.SCD_Unique and
- OT.SCD_SVD_Corresp

cover different aspects of the SCD/SVD generation by the TOE and are not present in PP SSCD KI and are not relevant in case of key import.

Instead, in PP SSCD KI the analogous security objectives for the operational environment OE.SCD/SVD_Auth_gen, OE.SCD_Unique and OE.SCD_SVD_Corresp are defined, as with key import the operational environment is responsible for the key generation.

The remaining security objective for the TOE OT.SCD_Auth_Imp is related to SCD import only and is therefore not present in PP SSCD KG and is not relevant in case of key generation.

The following security objectives for the TOE of the PP SSCD KG, OT.SCD/SVD_Auth_Gen, OT.SCD_Unique and OT.SCD_SVD_Corresp are not relevant for the TOE in case of key import.

PP SSCD KG TCCGA additionally adds the following OTs:

- OT.TOE_SSCD_Auth
- OT_TOE_TC_SVD_Exp

5.1.2 Relation to PP SSCD KG TCSCA and PP SSCD KI TCSCA

This Security Target additionally covers all OT from PP SSCD KG TCSCA [4] and PP SSCD KI TCSCA [5].

In fact PP SSCD KG TCSCA adds the same two OT as also defined in PP SSCD KI TCSCA which are:

- OT.TOE_TC_VAD_Imp
- OT.TOE_TC_DTBS_Imp

5.1.3 OT.Lifecycle_Security Lifecycle security

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

Application Note: The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD, e.g. after the (qualified) certificate for the corresponding SVD has been expired.

5.1.4 OT.SCD/SVD_Auth_Gen Authorised SCD/SVD generation

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

5.1.5 OT.SCD_Unique Uniqueness of the signature creation data

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

5.1.6 OT.SCD_SVD_Corresp Correspondence between SVD and SCD

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

5.1.7 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.

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

5.1.8 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.

5.1.9 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.

5.1.10 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.

5.1.11 OT.EMSEC_Design Provide physical emanations security

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

5.1.12 OT.Tamper_ID Tamper detection

The TOE shall provide system features that detect physical tampering of its components, and us es those features to limit security breaches.

5.1.13 OT.Tamper_Resistance Tamper resistance

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

5.1.14 OT.SCD_Auth_Imp Authorised SCD import

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

5.1.15 OT.TOE_SSCD_Auth Authentication proof as SSCD

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

5.1.16 OT.TOE_TC_SVD_Exp TOE trusted channel for SVD export

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

5.1.17 OT.TOE_TC_VAD_Imp Trusted channel of TOE for VAD import

Note: this OT is identical for PP SSCD KG TCSCA and PP SSCD KI TCSCA.

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.

Application note: This security objective for the TOE is partly covering OE.HID_VAD from the core PP (PP SSCD KG). While OE.HID_VAD in the core PP requires only the operational environment to protect VAD, this PP 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 this PP 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.

5.1.18 OT.TOE_TC_DTBS_Imp Trusted channel of TOE for DTBS import

Note: this OT is identical for PP SSCD KG TCSCA and PP SSCD KI TCSCA.

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.

Application note: This security objective for the TOE is partly covering OE.DTBS_Protect from the core PP. While OE.DTBS_Protect in the core PP requires only the operational environment to protect DTBS, this PP 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 this PP 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.

5.2 Security objectives for the operational environment

5.2.1 Relation to PP SSCD KG and PP SSCD KI and PP SSCD TCCGA

This ST covers all OE from PP SSCD KG and PP SSCD KI and PP SSCD TCCGA as follows:

Security objectives for the operational environment are identically stated in the PP SSCD KG and PP SSCD KI, those are OE.SVD_Auth, OE.CGA_QCert, OE.SSCD_Prov_Service, OE.HID_VAD, OE.DTBS_Intend, OE.DTBS_Protect and OE.Signatory (these are independent from the fact whether SCD are generated by the TOE itself or imported from the operational environment).

Furthermore PP SSCD KI adds OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique and OE.SCD_SVD_Corresp in order to address objectives which are part of the OT for PP SSCD KG but moved to the environment for PP SSCD KI since those functionality is moved to the environment.

However PP SSCD KG TCCGA substitutes OE.SSCD_Prov_Service (which is therefore removed completely) by OE.Dev_Prov_Service and adds security objectives for the operational environment OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp in order to address the additional method of use as SCD/SVD pair generation after delivery to the signatory and outside the secure preparation environment.

5.2.2 Relation to PP SSCD KG TCSCA and PP SSCD KI TCSCA

This ST additionally covers all OE from PP SSCD KG TCSCA [4] and PP SSCD KI TCSCA [5]. PP SSCD KG TCSCA and PP SSCD KI define (both in the same way) the following modifications in relation to PP SSCD KG [1], PP SSCD KI [2] and PP SSCD TCCGA:

OE.HI_VAD is substituted by OE.HID_TC_VAD_Exp and OE.DTBS_Protect is substituted by OE.SCA_TC_DTBS_Exp.

5.2.3 OE.SVD_Auth Authenticity of the SVD

The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

5.2.4 OE.CGA_QCert Generation of qualified certificates

The CGA shall generate a qualified certificate that includes (amongst others):

a) the name of the signatory controlling the TOE;
b) the SVD matching the SCD stored in the TOE and being under sole control of the signatory;
c) the advanced signature of the CSP.

The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a SSCD.

5.2.5 OE.Dev_Prov_Service Authentic SSCD provided by SSCD Provisioning Service

The SSCD Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, 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: This objective replaces OE.SSCD_Prov_Service from the core PP, which is possible as it does not imply any additional requirements for the operational environment when compared to OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_Service).

5.2.6 OE.HID_VAD Protection of the VAD

Note: this OE is substituted by 5.2.7 OE.HID_TC_VAD_Exp Trusted channel of HID for VAD export.

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.

5.2.7 OE.HID_TC_VAD_Exp Trusted channel of HID for VAD export

Note: this OE substitutes 5.2.6 OE.HID_VAD Protection of the VAD.

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.

Application note: This security objective for the TOE is partly covering OE.HID_VAD from the core PP. While OE.HID_VAD in the core PP requires only the operational environment to protect VAD, this PP 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 this ST 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.

5.2.8 OE.DTBS_Intend SCA sends data intended to be signed

The signatory shall use a trustworthy SCA that:

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

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

5.2.9 OE.DTBS_Protect SCA protects the data intended to be signed

Note: this OE is substituted by 5.2.10 OE.SCA_TC_DTBS_Exp Trusted channel of SCA for DTBS export.

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.

5.2.10 OE.SCA_TC_DTBS_Exp Trusted channel of SCA for DTBS export

Note: this OE substitutes 5.2.9 OE.DTBS_Protect SCA protects the data intended to be signed.

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.

Application note: This security objective for the TOE is partly covering OE.DTBS_Protect from the core PP. While OE.DTBS_Protect in the core PP requires only the operational environment to protect DTBS, this PP 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 this ST 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.

5.2.11 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.

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

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

5.2.13 OE.CGA_TC_SVD_Imp CGA trusted channel for SVD import

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

The developer prepares the TOE by pre-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 a 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 a SCD the TOE will be a SSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the signatory in the operational use stage the TOE provides additional security functionality addressed by OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp. But this security functionality shall be initialized by the SSCD Provisioning Service as described in OE.Dev_Prov_Service. Therefore this ST 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.

5.2.14 OE.SCD/SVD_Auth_Gen Authorised SCD/SVD generation

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

5.2.15 OE.SCD_Secrecy SCD Secrecy

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

5.2.16 OE.SCD_Unique Uniqueness of the signature creation data

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

5.2.17 OE.SCD_SVD_Corresp Correspondence between SVD and SCD

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

5.3 Security Objectives Rationale

The following table provides an overview for security objectives coverage.

5.4 Security objectives backtracking

The table below gives the mapping of security problem definition to security objectives. It is the combination of the mapping tables of the underlying protection profiles.

	OT.Lifecycle_Security	*OT.SCD/SVD_Auth_Gen*	*OT.SCD_Unique*	*OT.SCD_SVD_Corresp*	*OT.SCD_Secrecy*	*OT.Sig_Secure*	*OT.Sigy_SigF*	*OT.DTBS_Integrity_TOE*	*OT.EMSEC_Design*	*OT.Tamper_ID*	*OT.Tamper_Resistance*	*OT.SCD_Auth_Imp*	*OT.TOE_SSCD_Auth*	*OT.TOE_TC_SVD_Exp*	*OT.TOE_TC_VAD_Imp*	*OT.TOE_TC_DTBS_Imp*	*OE.SVD_Auth*	*OE.SCD/SVD_Auth_Gen*	*OE.SCD_Secrecy*	*OE.SCD_Unique*	*OE.SCD_SVD_Corresp*	*OE.CGA_QCert*	*OE.Dev_Prov_Service*	*OE.HID_VAD*	*OE.HID_TC_VAD_Exp*	*OE.DTBS_Intend*	*OE.DTBS_Protect*	*OE.SCA_TC_DTBS_Exp*	*OE.Signatory*	*OE.CGA_SSCD_Auth*	*OE.CGA_TC_SVD_Imp*
T.SCD_Divulg		x			x							x						x	X												
T.SCD_Derive		x	x			x														X											
T.Hack_Phys					x				x	x	x																				
T.SVD_Forgery				x										x			x				X										x
T.SigF_Misuse	x						x	x							x	x								x	x	x	x	x	x		
T.DTBS_Forgery								x								x										x	x	x			
T.Sig_Forgery			x			x														x		x									
P.CSP_QCert	x			x								x	x					x			x	x								x	
P.QSign						x	x															x				x					
P.Sigy_SSCD	x	x	x		x	x	x	x	x		x	x	x	x				x	x	x			x							x	x
P.Sig_Non-Repud	x		x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x		x	x		x	x	x	x	x	x	x
A.CGA																	x					x									
A.SCA																										x					
A.CSP		x	x	x	x													x	x	x	x										

5.5 Security objectives sufficiency

This chapter shows the security objectives sufficiency mainly by providing a combination of the text from the underlying protection profiles. Editorial changes to resolve slight differences in equivalent text (e.g. reference to the directive, adding filler words) have been made to harmonize the text. In some cases textual deviations (still with the same meaning) exist: in those cases both texts are shown separated by "/" (slash) or by the term "resp." (respectively) in between.

Countering of threats by security objectives:

T.SCD_Divulg (Storing, copying and releasing of the signature creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in recital (18) of the directive. This threat is countered by OT.SCD_Secrecy, which assures the secrecy of the SCD used for signature creation, resp.

- OE.SCD_Secrecy, which assures the secrecy of the SCD in the CSP environment, and
- OT.SCD_Secrecy, which assures the secrecy of the SCD during use by the TOE for signature creation.

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

T.SCD_Derive (Derive the signature creation data) deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. OT.SCD/SVD_Auth_Gen resp. OE/SCD/SVD_Auth_Gen counters this threat by implementing

cryptographically secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographically secure electronic signatures.

T.Hack_Phys (Exploitation of physical vulnerabilities) deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. OT.EMSEC_Design counters physical attacks through the TOE interfaces and observation of TOE emanations. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tampering attacks.

T.SVD_Forgery (Forgery of the signature verification data) deals with the forgery of the SVD (either exported by the TOE or generated externally) given to the CGA for certificate generation. T.SVD_Forgery is addressed by OT.SCD_SVD_Corresp resp. OE.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth which ensures integrity/authenticity of the SVD (either exported by the TOE or generated externally) given to the CGA of the CSP and verification of the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

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 an electronic signature (SDO) on data for which the signatory has not expressed the intent to sign/has not decided to sign, as required by paragraph 1(c) of Annex III. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by / on demand of the signatory. OT.Sigy_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. In addition the combination of OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission over the channel form the SCA to the TOE.

OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides the human interface for the user authentication

- OE.HID_VAD (Protection of the VAD) resp.
- OE.HID_TC_VAD_Exp (Trusted channel of the HID for VAD) requires the HID to protect

provides confidentiality and integrity of the VAD as needed by the authentication method employed.

The HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD).

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. OE.Signatory ensures also that the signatory keeps their VAD confidential.

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

The TOE IT environment also addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which

- ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of OE.DTBS_Protect, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE
- ensures that the SCA sends only those DTBS intended to be signed by the signatory, and OE.DTBS_Protect, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE

The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R inside the TOE.

In addition the threat T.DTBS_Forgery is addressed by the security objectives OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS), which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE. The TOE counters internally this threat by the means of OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensuring the integrity of the DTBS/R inside the TOE.

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique resp. OE.SCD_Unique and OE.CGA_QCert address this threat in general. OT.Sig_Secure (Cryptographic security of the electronic signature) ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. OT.SCD_Unique resp. OE.SCD_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

Enforcement of OSPs by security objectives:

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

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- OE.SCD/SVD_Auth_Gen, which ensures that the SCD/SVD generation can be invoked by authorised users only,
- OT.SCD_Auth_Imp which ensures that authorised users only may invoke the import of the SCD,
- OT.SCD_SVD_Corresp resp. OE_SCD_SVD_Corresp, which requires (the CSP) to ensure the correspondence between the SVD and the SCD during their generation;

- 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.

In addition P.CSP_QCert (CSP generates qualified certificates) provides that the TOE and the SCA may be employed to sign data with (qualified) electronic signatures, as defined by the Directive, Article 5, paragraph 1. Directive [1], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The OE.CGA_QCert addresses the requirement of qualified (or advanced) electronic signatures as being based on qualified (or non-qualified) certificates. According to OT.TOE_SSCD_Auth the copies of the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD to prove this identity as SSCD to the CGA. The OE.CGA_SSCD_Auth ensures that the SP checks the proof of the device presented of the applicant that it is a SSCD. The OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE to the CGA corresponds to the SCD stored in the TOE and used by the signatory. The OT.Lifecycle_Security ensures that the TOE detects flaws during the initialization, personalization and operational usage.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.

OT.Sig_Secure ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

P.Sigy_SSCD (TOE as secure signature creation device) requires the TOE to meet Annex III. This is ensured as follows:

- OT.SCD_Unique resp. OE.SCD_Unique meets the paragraph 1(a) of Annex III, by the requirements that the SCD used for signature creation can practically occur only once;
- OT.SCD_Unique, resp. OE.SCD_Unique, OT.SCD_Secrecy resp. OE_SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(a) of Annex III by the requirements to ensure the secrecy of the SCD. OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of the SCD against specific attacks;
- OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III by the requirements to ensure that the SCD cannot be derived from SVD, the electronic/digital signatures or any other data exported outside the TOE;
- OT.Sigy_SigF and OE.SCD_Secrecy meet meets the requirement in paragraph 1(c) of Annex III by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others;
- OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of Annex III as the TOE shall not alter the DTBS/R.

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

Please take note, the requirements of the Directive, Annex III, 2., that the SSCD does not prevent the data to be signed from being presented to the signatory prior to the signature process is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the signatory and send them to the SSCD for signing.

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

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

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

In more detail 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 feature (addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA_SSCD_Auth and the received SVD is sent by this SSCD as required by OE.CGA_TC_SVD_Imp. Thus the obligation of the SSCD provisioning 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 (Authentic SSCD provided by SSCD-provisioning service) ensures that the signatory obtains/uses an authentic copy of the TOE, initialised and personalised as SSCD from the SSCD-provisioning service for the signatory.

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

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.
- authenticity of the SVD included in the certificate and to ensure the correspondence of the SVD to the SCD stored in the SSCD.

OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented/implemented in the TOE. OT.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 of the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure the authenticity of the SVD as being exported by the TOE under sole control of the signatory.

OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD- provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD).

The TOE security feature addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp supported by OE.Dev_Prov_Service enables the verification whether the device presented by the applicant is a SSCD as required by OE.CGA_SSCD_Auth and the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA_TC_SVD_Imp.

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.

The confidentiality of VAD is protected during the transmission between the HI device and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD).

OE.DTBS_Intend, OE.DTBS_Protect , T.DTBS_Integrity_TOE, OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) and OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

Upkeep of assumptions by security objectives:

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

A.CGA (Trustworthy certificate generation application) establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert (Generation of qualified certificates), which ensures the generation of qualified certificates, and by OE.SVD_Auth (Authenticity of the SVD / CGA proves the authenticity of the SVD), which ensures the protection/verification of the

integrity/authenticity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

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

6 Extended Component Definition (ASE_ECD)

6.1 Definition of the Family FPT_EMS

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

FPT_EMS TOE Emanation

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS TOE Emanation	1

FPT_EMS.1 TOE Emanation has two constituents:

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

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

FPT_EMS.1 TOE Emanation

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

FPT_EMS.1.1 The TOE shall not emit *[*assignment*: types of emissions]* in excess of *[*assignment*: specified limits]* enabling access to [assignment*: list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMS.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6.2 Definition of the Family FIA_API

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

FIA_API Authentication Proof of Identity

Family behaviour

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

Component levelling:

Management: FIA_API.1

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

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

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

7 Security Requirements (ASE_REQ)

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 (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.

A **selection** operation is used to select one or more options provided by the CC in stating a requirement. A selection that has been made in this ST (as in the underlying PPs) is indicated as underlined text and the original text of the component is given by a footnote.

An **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment that that has been made in this European Standard is indicated as underlined text and the original text of the component is given by a footnote. Assignments left to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicized*.

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.

The SFRs in this chapter are a combination of all SFRs of the underlying (claimed) PPs.

The following SFRs have been renamed to enable iteration:

- FCS_CKM.1 renamed to FCS_CKM.1/SCD_SVD
- FCS_COP.1 renamed to FCS_COP.1/SIG_GEN
- FIA_AFL.1 renamed to FIA_AFL.1/PIN
- FPT_EMS.1 renamed to FPT_EMS.1/SCD_RAD

Furthermore the following SFRs are added:

- FCS_CKM.1/DH_PACE (from BSI-CC-PP-0068 [33])
- FCS_CKM.1/SYM_AUTH (from Common Criteria Part 2 [30])
- FCS_COP.1/SM_ENC and FCS_COP.1/SM_MAC (which are the renamed FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_ENC from BSI-CC-PP-0068 [33] which are modified to additionally include secure messaging after symmetric authentication)
- FCS_COP.1/SYM_AUTH (from Common Criteria Part 2 [30])
- FDP_ITC.1/AUTHKEYS (from Common Criteria Part 2 [30], due to dependency of FCS_COP.1)
- FDP_ACC.1/AUTHKEY_Admin (from Common Criteria Part 2 [30], due to dependency of FDP_ITC.1)
- FDP_ACF.1/AUTHKEY_Admin (from Common Criteria Part 2 [30], due to dependency of FDP_ITC.1)
- FMT_MSA.3/AUTHKEY (from Common Criteria Part 2 [30], due to dependency of FDP_ITC.1)
- FPT_EMS.1/KEYS iterated to cover additional secrets (e.g. session keys, authentication keys, PACE secrets)
- FIA_AFL.1/PACE iterated (similar to FIA_AFL.1/PACEfrom BSI-CC-PP-0068 [33])

7.1 Cryptographic support (FCS)

The cryptographic algorithms and cryptographic key sizes and other cryptographic parameters are chosen in accordance with ANSSI-PG-083 [8] and SOGIS Agreed Cryptographic Mechanisms [9].

7.1.1 FCS_CKM.1/SCD_SVD Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/SCD_SVD The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm EC key generation and RSA key generation[5] and specified cryptographic key sizes 256, 384, 512, 521 resp. 1984, 2048, 2688, 3072, 4096[6] that meet the following:[7]

- EC: ANSI X.9.62 [34] and ISO /IEC 14888-3 [35] with domain parameters NIST P-256, NIST P-384, NIST P-521 acc. FIPS 186-4 [36] and Brainpool P256r1, Brainpool P384r1, Brainpool P512r1 acc. RFC 5639 [37]
- RSA: ANSI X9.31 [38] for minimum distance of primes

Note: The refinement in the element FCS_CKM.1/SCD_SVD.1 substitutes “cryptographic keys” by “SCD/SVD pairs” because it clearly addresses the SCD/SVD key generation.

7.1.2 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]

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 [39][8] and specified cryptographic key sizes 256, 384, 512, 521[9] that meet the following: [21].

Note: The TOE generates a shared secret value K with the terminal during the PACE protocol, see [21]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [40]) or on the ECDH compliant to TR- 03111 [39] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [21] and [39] for details). The shared secret value K is used for deriving the AES or DES session keys for message encryption and message

[5] [assignment: *cryptographic key generation algorithm*]
[6] [assignment: *cryptographic key sizes*]
[7] [assignment: *list of standards*]
[8] [selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [30]]
[9] [assignment: cryptographic key sizes]

authentication (PACE-K MAC, PACE-K Enc) according to [21] for the TSF required by FCS_COP.1/SM_ENC and FCS_COP.1/SM_MAC.

Note: the PACE protocol defines three different "mapping" methods (see [21] chapt. 4.4: This SFR FCS_CKM.1/DH_PACE covers "generic mapping" (see [21] chapt. 4.4.3.3.1) and "integrated mapping" (see sect. 4.4.3.3.2) but not "chip authentication mapping" (see chapt. 4.4.3.3.3).

7.1.3 FCS_CKM.1/SYM_AUTH Cryptographic key generation – Device Authentication for 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/SYM_AUTH The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Session Key Derivation as defined for Symmetric Authentication[10] and specified cryptographic key sizes 112 (TDES), 128 (AES), 192 (AES), 256 (AES)[11] that meet the following: [20] Chapt 3.8.

Note: The TOE generates a shared secret value $K_{IFD/ICC}$ with the terminal during the Device Authentication protocol (see [33] chapter 3.8ff). The shared secret value $K_{IFD/ICC}$ is used for deriving (see [20] chapter 3.10ff for computation of session keys) the AES or DES session keys for message encryption and message authentication (Secure Messaging ENC / MAC according to [21]) for the TSF required by FCS_COP.1/SM_ENC and FCS_COP.1/SM_MAC.

7.1.4 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting with constant or random data[12] that meets the following: none[13].

7.1.5 FCS_COP.1/SIG_GEN Cryptographic operation – Signature Generation

Hierarchical to: No other components.

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

[10] [assignment: cryptographic key generation algorithm]
[11] [assignment: cryptographic key sizes]
[12] [assignment: *cryptographic key destruction method]*
[13] [assignment: *list of standards]*

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SIG_GEN The TSF shall perform digital signature creation[14] in accordance with a specified cryptographic algorithm[15] EC-DSA and RSA and cryptographic key sizes[16] 256, 384, 512, 521 resp. 1984, 2048, 2688, 3072, 4096] that meet the following:[17]

- EC-DSA: plain message according BSI TR 03111 [41], Signature according ANSI X9.62 [34], BSI TR 03111 and ISO-IEC-14888-3 [35],
- RSA: message generation and signature scheme EMSA-PSS acc. RSA Cryptography Specifications Version 2.2 [42] and signature using CRT
- and optional for RSA and EC-DSA: hashing of message using either
  - SHA-256: ISO/IEC 10118-3:2018 [43], dedicated hash function 4 and NIST FIPS PUB 180-4
  - SHA384: ISO/IEC 10118-3:2018, dedicated hash function 5 and NIST FIPS PUB 180-4
  - SHA-512: ISO/IEC 10118-3:2018, dedicated hash function 6 and NIST FIPS PUB 180-4

7.1.6 FCS_COP.1/SYM_AUTH Cryptographic operation – Symmetric Authentication

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SYM_AUTH The TSF shall perform Symmetric Authentication Scheme[18] in accordance with a specified cryptographic algorithm[19] TDES and AES and cryptographic key sizes 112 Bit (TDES), 128 Bit (AES), 192 Bit (AES), 256 Bit (AES)[20] that meet the following: [20] Chapt 3.8 [21]

7.1.7 FCS_COP.1/SM_ENC Cryptographic operation – Encryption / Decryption AES/TDES

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]

[14] [assignment: *list of cryptographic operations]*
[15] [assignment: *cryptographic algorithm]*
[16] [assignment: *cryptographic key sizes]*
[17] [assignment: l*ist of standards]*
[18] [assignment: *list of cryptographic operations]*
[19] [assignment: *cryptographic algorithm]*
[20] [assignment: *cryptographic key sizes]*
[21] [assignment: l*ist of standards]*

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SM_ENC The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm AES, TDES[22] in CBC mode and cryptographic key sizes 112, 128, 192, 256[23] bit that meet the following: compliant to [21].

Note: 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 either as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-KEnc) or as a part of Symmetric Authentication defined in [20], Chapt 3.8 according to FCS_CKM.1/SYM_AUTH.

7.1.8 FCS_COP.1/SM_MAC Cryptographic operation – MAC AES/TDES

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SM_MAC The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm CMAC (AES), Retail-MAC (TDES)[24] and cryptographic key sizes 112 (TDES), 128 (AES), 192 (AES), 256 (AES) [25] bit that meet the following: compliant to [21].

Note: This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal either as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-KMac) or as a part of Symmetric Authentication defined in [20], Chapt 3.8 according to FCS_CKM.1/SYM_AUTH.

Note that in accordance with [21] the (two-key) Triple-DES could be used in Retail mode for secure messaging.

7.2 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

[22] [selection: AES, 3DES]
[23] [selection: 112, 128, 192, 256]
[24] [selection: CMAC, Retail-MAC]
[25] [selection: 112, 128, 192, 256]

S.User	SCD/SVD Management	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)
AUTHKEYS	(This ST does not define security attributes for AUTHKEYS)	(This ST does not define security attributes for AUTHKEYS)

Table 2 — Subjects and security attributes for access control

7.2.1 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[26] on:

1. subjects: S.User,
2. objects: SCD, SVD,
3. operations: generation of SCD/SVD pair[27].

7.2.2 FDP_ACF.1/SCD/SVD_Generation Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/SCD/SVD_Generation The TSF shall enforce the SCD/SVD Generation SFP[28] to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management"[29].

FDP_ACF.1.2/SCD/SVD_Generation The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to generate SCD/SVD pair[30].

[26] [assignment: *access control SFP*]
[27] [assignment*: list of subjects, objects, and operations among subjects and objects covered by the SFP]*
[28] [assignment: *access control SFP]*
[29] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]*
[30] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*

FDP_ACF.1.3/SCD/SVD_Generation The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[31].

FDP_ACF.1.4/SCD/SVD_Generation The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair[32].

7.2.3 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[33] on

1. subjects: S.User,
2. objects: SCD,
3. operations: import of SCD[34].

7.2.4 FDP_ACF.1/SCD_Import Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/SCD_Import The TSF shall enforce the SCD Import SFP[35] to objects based on the following:
the S.User is associated with the security attribute "SCD/SVD Management"[36].

FDP_ACF.1.2/ SCD_Import The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to import SCD[37].

FDP_ACF.1.3/SCD_Import The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[38].

FDP_ACF.1.4/SCD_Import The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

---

[31] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[32] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects]*
[33] [assignment: *access control SFP]*
[34] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP]*
[35] [assignment: *access control SFP]*
[36] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP- relevant security attributes, or named groups of SFP-relevant security attributes]*
[37] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*
[38] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*

S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to import SCD[39].

7.2.5 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[40] on:

1. subjects: S.User;
2. objects: SVD;
3. operations: export[41].

7.2.6 FDP_ACF.1/SVD_Transfer Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/SVD_Transfer The TSF shall enforce the SVD Transfer SFP[42] to objects based on the following:

1. the S.User is associated with the security attribute Role;
2. the SVD[43].

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 or R.Sigy[44] is allowed to export SVD[45].

FDP_ACF.1.3/SVD_Transfer The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[46].

FDP_ACF.1.4/SVD_Transfer The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[47].

7.2.7 FDP_ACC.1/Signature_Creation Subset access control

Hierarchical to: No other components.

[39] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects]*
[40] [assignment: *access control SFP]*
[41] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[42] [assignment: *access control SFP]*
[43] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[44] [selection: *R.Admin, R.Sigy]*
[45] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[46] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[47] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Signature_Creation The TSF shall enforce the Signature Creation SFP[48] on:

1. subjects: S.User;
2. objects: DTBS/R, SCD;
3. operations: signature creation[49].

7.2.8 FDP_ACF.1/Signature_Creation Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Signature_Creation The TSF shall enforce the Signature Creation SFP[50] to objects based on the following:

1. the user S.User is associated with the security attribute "Role"; and
2. the SCD with the security attribute "SCD Operational"[51].

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"[52].

FDP_ACF.1.3/ Signature_Creation The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[53].

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"[54].

7.2.9 FDP_ACC.1/AUTHKEY_Admin Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/AUTHKEY_Admin The TSF shall enforce the Authentication Key Administration SFP[55] on:

---

[48] [assignment: *access control SFP]*
[49] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP]*
[50] [assignment: *access control SFP]*
[51] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]*
[52] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*
[53] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects]*
[54] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects]*
[55] [assignment: *access control SFP]*

4. subjects: S.Admin;
5. objects: AUTHKEYS
6. operations: create, import, change, delete, deactivate, terminate[56].

7.2.10 FDP_ACF.1/AUTHKEY_Admin Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/AUTHKEY_Admin The TSF shall enforce the Authentication Key Administration SFP[57] to objects based on the following:

1. the user S.User is associated with the security attribute "Role"; and
2. the AUTHKEYS (without security attributes[58].

FDP_ACF.1.2/AUTHKEY_Admin The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
Only R.Admin is allowed to create, import, change, delete, deactivate, terminate AUTHKEYS.

FDP_ACF.1.3/AUTHKEY_Admin The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[59].

FDP_ACF.1.4/ AUTHKEY_Admin The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[60].

7.2.11 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[61].

FDP_DAU.2.2/SVD The TSF shall provide CGA[62] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

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

Hierarchical to: No other components.

---

[56] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP]*
[57] [assignment: *access control SFP]*
[58] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]*
[59] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects]*
[60] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects]*
[61] [assignment: list of objects or information types]
[62] [assignment: *list of subjects*]

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1/SCD The TSF shall enforce the SCD Import SFP[63] 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[64].

7.2.13 FDP_ITC.1/AUTHKEYS Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1/AUTHKEYS The TSF shall enforce the Authentication Key Admin SFP[65] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/ AUTHKEYS The TSF shall ignore any security attributes associated with the ~~user data~~ **Authentication Keys** when imported from outside the TOE.

FDP_ITC.1.3/ AUTHKEYS The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none[66].

7.2.14 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[67] to receive[68] ~~user data~~ **SCD** in a manner protected from unauthorised disclosure.

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

[63] [assignment: *access control SFP(s) and/or information flow control SFP(s)]*
[64] [assignment: *additional importation control rules]*
[65] [assignment: *access control SFP(s) and/or information flow control SFP(s)]*
[66] [assignment: *additional importation control rules]*
[67] [assignment: *access control SFP(s) and/or information flow control SFP(s)]*
[68] [selection: *transmit, receive]*

7.2.15 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[69] the following objects: SCD[70].

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".

7.2.16 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[71] on all objects, based on the following attributes: integrity checked stored data[72].

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[73].

7.2.17 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[74] on all objects, based on the following attributes: integrity checked stored DTBS[75].

FDP_SDI.2.2/DTBS Upon detection of a data integrity error, the TSF shall:

1. prohibit the use of the altered data;

[69] [selection: *allocation of the resource to, deallocation of the resource from*]
[70] [assignment: *list of objects]*
[71] [assignment: *integrity errors]*
[72] [assignment: *user data attributes]*
[73] [assignment: *action to be taken]*
[74] [assignment: *integrity errors]*
[75] [assignment: *user data attributes*]

2. inform the S.Sigy about integrity error[76].

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

7.2.18 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[77] to receive[78] user data in a manner protected from modification and insertion[79] errors.

FDP_UIT.1.2/DTBS The TSF shall be able to determine on receipt of user data, whether modification and insertion[80] has occurred.

7.3 Identification and authentication (FIA)

7.3.1 FIA_AFL.1/PIN Authentication failure handling - PIN

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PIN The TSF shall detect when an administrator configurable positive integer within 1 to 10 (decimal) [81] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[82].

FIA_AFL.1.2/PIN When the defined number of unsuccessful authentication attempts has been met[83], the TSF shall block RAD[84].

Note: the missing operation in the element FIA_AFL.1.1 has been performed consistently with the other implemented authentication mechanisms and to be resistant against attacks with high attack potential.

7.3.2 FIA_AFL.1/PACE Authentication failure handling - PACE authentication using non-blocking authorisation data

Hierarchical to: No other components.

[76] [assignment: *action to be taken]*
[77] [assignment: *access control SFP(s) and/or information flow control SFP(s)]*
[78] [selection: *transmit, receive]*
[79] [selection: *modification, deletion, insertion, replay*]
[80] [selection: *modification, deletion, insertion, replay]*
[81] [selection*: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[82] [assignment: *list of authentication events]*
[83] [selection: *met ,surpassed]*
[84] [assignment: *list of actions]*

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PACE The TSF shall detect when an administrator configurable positive integer within 1 to 16 (decimal) [85] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the PACE password (MRZ) or PACE CAN as a shared password[86].

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been met[87], the TSF shall activate authentication delay for following authentication attempts, starting with a delay of 1 second and exponentially growing[88].

Note: the missing operation in the element FIA_AFL.1.1 has been performed consistently with the other implemented authentication mechanisms and to be resistant against attacks with high attack potential.

7.3.3 FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a Symmetric Authentication according to EN 419212-3 [20], Section 3.8[89] to prove the identity of the SSCD[90].

Note: the operation performed in the element FIA_API.1.1 assigns a Symmetric Authentication Mechanism which includes Mutual Authentication of the TOE and the terminal using TOE specific keys and enables to authentication of the TOE as SSCD.

7.3.4 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. selection of an authentication key or PIN/PUK
3. performing PACE protocol (including all necessary steps) and establishment of a trusted channel between TOE and HID or SCA, i.e. FTP_ITC.1/DTBS and FTP_ITC.1/VAD
4. performing Symmetric Authentication (including all necessary steps) and establishment of a trusted channel between TOE and CGA or SSCD Provisioning Service, i.e. FTP_ITC.1/SVD and FTP_ITC.1/SCD[91] [92]

[85] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[86] [assignment: *list of authentication events]*
[87] [selection: *met ,surpassed]*
[88] [assignment: *list of actions]*
[89] [assignment: *authentication mechanism]*
[90] [assignment: *authorized user or rule]*
[91] [assignment: *list of additional TSF-mediated actions]*
[92] [assignment: *list of TSF-mediated actions]*

5. reading or modifying (optional) EFs inside the SSCD Application
6. using MPA applications

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.

7.3.5 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,[93] [94]
5. establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SCD,
6. selection of an authentication key or PIN/PUK
7. establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS,
8. performing PACE protocol (including all necessary steps)
9. performing Symmetric Authentication protocol (including all necessary steps)
10. reading or modifying (optional) EFs inside the SSCD Application
11. using MPA applications

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

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

7.4 Security management (FMT)

7.4.1 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

[93] [assignment: *list of TSF mediated actions]*
[94] [assignment: *list of additional TSF-mediated actions]*

FMT_SMR.1.1 The TSF shall maintain the roles R.Admin and R.Sigy[95].

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

7.4.2 FMT_SMF.1 Security management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. creation and modification of RAD;
2. enabling the signature creation function;
3. modification of the security attribute SCD/SVD management, SCD operational;
4. change the default value of the security attribute SCD Identifier;
5. termination of the SCD, RAD, TPIN, PUK
6. deletion of the SCD, RAD, TPIN, PUK
7. creation of the SCD
8. generation of the SCD/SVC
9. import of the SCD
10. export of SVD
11. creation, deletion, update of additional optional EFs
12. creation, import, change, deletion, deactivation, termination of symmetric Authentication Keys (of SSCD Provisioning Service and CGA)[96] [97].

7.4.3 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1 The TSF shall restrict the ability to enable[98] the functions signature creation function[99] to R.Sigy[100].

7.4.4 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

[95] [assignment: *the authorised identified roles]*
[96] [assignment: *list of other security management functions to be provided by the TSF]*
[97] [assignment: *list of security management functions to be provided by the TSF]*
[98] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
[99] [assignment: *list of functions]*
[100] [assignment: *the authorised identified roles*]

FMT_MSA.1.1/Admin_KG The TSF shall enforce the SCD/SVD Generation SFP[101] to restrict the ability to modify and none[102] [103] the security attributes SCD/SVD management[104] to R.Admin[105].

Note: the SFR "FMT_MSA.1/Admin" taken from (PP SSCD KG) has been renamed to "FMT_MSA.1/Admin_KG" to distinguish it from FMT_MSA.1/Admin taken from PP SSCD KI).

7.4.5 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[106] to restrict the ability to modify and none[107] [108] the security attributes SCD/SVD management[109] to R.Admin[110].

Note: the SFR "FMT_MSA.1/Admin" taken from PP SSCD KI has been renamed to "FMT_MSA.1/Admin_KI" to distinguish it from FMT_MSA.1/Admin taken from PP SSCD KG and added as an iteration operation.

7.4.6 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[111] to restrict the ability to modify[112] the security attributes SCD operational[113] to R.Sigy[114].

7.4.7 FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

[101] [assignment: *access control SFP(s), information flow control SFP(s)]*
[102] [assignment: *other operations]*
[103] [selection: *change_default, query, modify, delete, [assignment: other operations]]*
[104] [assignment: *list of security attributes]*
[105] [assignment: *the authorised identified roles]*
[106] [assignment: *access control SFP(s), information flow control SFP(s)]*
[107] [assignment: *other operations]*
[108] [selection: *change_default, query, modify, delete, [assignment: other operations]]*
[109] [assignment: *list of security attributes]*
[110] [assignment: *the authorised identified roles]*
[111] [assignment: *access control SFP(s), information flow control SFP(s)]*
[112] [selection: *change_default, query, modify, delete, [assignment: other operations]]*
[113] [assignment: *list of security attributes]*
[114] [assignment: *the authorised identified roles]*

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[115].

Note: The security attributes "SCD/SVD Management" and "SCD operational" may have the values "yes" or "no". SCD/SVD Management" may have those values in both the preparation phase and the usage phase while "SCD operational" set to "yes" can only be set in the usage phase (in fact setting "SCD operational to "yes" performs the transition). S.Admin cannot generate / import new SCD/SVD key pair values in the usage phase since the key values can be written/imported only once and the same holds for Transport PIN and PUK. Therefore also the combination "SCD operational" set to "true" and "SCD/SVD management" set to "true" is secure.

7.4.8 FMT_MSA.3/KG Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1/KG The TSF shall enforce the SCD/SVD Generation SFP, SVD Transfer SFP and Signature Creation SFP[116] to provide restrictive[117] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/KG The TSF shall allow the R.Admin[118] to specify alternative initial values to override the default values when an object or information is created.

Note: an iteration has been made on the SFR "FMT_MSA.3" taken from PP SSCD KG to distinguish it from the SFR with the same name in PP SSCD KI.

7.4.9 FMT_MSA.3/KI Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1/KI The TSF shall enforce the SCD Import SFP and Signature Creation SFP[119] to provide restrictive[120] default values for security attributes that are used to enforce the SFP.

[115] [selection: *list of security attributes]*
[116] assignment: *access control SFP, information flow control SFP]*
[117] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
[118] [assignment: *the authorised identified roles]*
[119] assignment: *access control SFP, information flow control SFP]*
[120] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

FMT_MSA.3.2/KI The TSF shall allow the R.Admin[121] to specify alternative initial values to override the default values when an object or information is created.

Note: an iteration has been made on the SFR "FMT_MSA.3." taken from PP SSCD KI to distinguish it from the SFR with the same name in PP SSCD KG.

7.4.10 FMT_MSA.3/AUTHKEY Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1/KI The TSF shall enforce the Authentication Key Administration SFP[122] to provide restrictive[123] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/KI The TSF shall allow the nobody[124] to specify alternative initial values to override the default values when an object or information is created.

7.4.11 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.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation.
2. If S.Sigy successfully generates an SCD/SVD pair the security attribute "SCD operational of the SCD" shall be set to "yes" as a single operation.[125]

Note: The TOE does not support generating an SVD/SCD pair by the signatory alone, therefore rule (2) is not relevant.

Note: an iteration has been made on the SFR "FMT_MSA.4" taken from PP SSCD KG to distinguish it from the SFR with the same name in PP SSCD KI.

7.4.12 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:

[121] [assignment: *the authorised identified roles]*
[122] assignment: *access control SFP, information flow control SFP]*
[123] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
[124] [assignment: *the authorised identified roles]*
[125] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]]*

1. If S.Admin imports SCD while S.Sigy is not currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "no" after import of the SCD as a single operation.
2. If S.Admin imports SCD while S.Sigy is currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "yes" after import of the SCD as a single operation. [126]

Note: The TOE does not support importing an SVD/SCD pair by the signatory alone, therefore rule (2) is not relevant.

Note: an iteration has been made on the SFR "FMT_MSA.4" taken from PP SSCD KG to distinguish it from the SFR with the same name in PP SSCD KI.

7.4.13 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[127] the RAD[128] to R.Admin[129].

7.4.14 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 or unblock[130] [131] the RAD[132] to R.Sigy[133].

7.5 Protection of the TSF (FPT)

7.5.1 FPT_EMS.1/SCD_RAD TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1/SCD_RAD The TOE shall not emit **variations in IC power consumption or electromagnetic emissions or variations in command execution time**[134]] in

[126] [assignment: *rules for setting the values of security attributes]*
[127] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]]*
[128] [assignment: *list of TSF data]*
[129] [assignment: *the authorised identified roles]*
[130] [assignment: *other operations]*
[131] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]]*
[132] [assignment: *list of TSF data]*
[133] [assignment: the authorised identified roles]
[134] [assignment: *types of emissions]*

excess of **limits specified by the state of the art attacks on smart card IC**[135] enabling access to RAD[136] and SCD[137].

FPT_EMS.1.2/SCD_RAD The TSF shall ensure any users[138] are unable to use the following interface secure chip contacts[139] to gain access to RAD[140] and SCD[141].

7.5.2 FPT_EMS.1/KEYS TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1/KEYS The TOE shall not emit **variations in IC power consumption or electromagnetic emissions or variations in command execution time**[142]] in excess of **limits specified by the state of the art attacks on smart card IC**[143] enabling access to

- SM session keys (derived by PACE or Symmetric Authentication),
- PACE MRZ or CAN,
- Authentication Key of SSCD Provisioning Service and Authentication Key of CGA[144].

FPT_EMS.1.2/KEYS The TSF shall ensure any users[145] are unable to use the following interface secure chip contacts[146] to gain access to

- SM session keys (derived by PACE or Symmetric Authentication),
- PACE MRZ or CAN,
- Authentication Key of SSCD Provisioning Service and Authentication Key of CGA[147].

7.5.3 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:

[135] [assignment: *specified limits]*
[136] [assignment: *list of types of TSF data]*
[137] [assignment: *list of types of user data]*
[138] [assignment: *type of users]*
[139] [assignment: *type of connection]*
[140] [assignment: *list of types of TSF data]*
[141] [assignment: *list of types of user data]*
[142] [assignment: *types of emissions]*
[143] [assignment: *specified limits]*
[144] [assignment: *list of types of user data]*
[145] [assignment: *type of users]*
[146] [assignment: *type of connection]*
[147] [assignment: *list of types of user data]*

1. self-test according to FPT_TST fails;
2. power loss during transaction;
3. permanent and/or transient memory failure (e.g. wear out);
4. operating conditions out of range (e.g. voltage, temperature sensors) [148] [149].

7.5.4 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.

7.5.5 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[150] to the TSF[151] by responding automatically such that the SFRs are always enforced.

Note: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks the TOE can by no means detect attacks on all of its elements (e.g. the TOE is destroyed). In case of physical tampering or manipulation the TSF may not provide the intended functions for SCD/SVD pair generation or signature creation but ensures the confidentiality of the SCD by e.g. blocking these functions. The "automatic response" in the element FPT_PHP.3.1 means (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

7.5.6 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, periodically during normal operation and at each OS start-up (after reset)[152]** to demonstrate the correct operation of the TSF[153].

[148] [assignment: *list of other types of failures in the TSF]*
[149] [assignment: *list of types of failures in the TSF*]
[150] [assignment: *physical tampering scenarios]*
[151] [assignment: *list of TSF devices/elements]*
[152] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-test should occur]]*
[153] [selection: *[assignment: parts of TSF], the TSF*

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data[154].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of TSF[155].

7.6 Trusted Path / Channels (FTP)

7.6.1 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[156] 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 [157] [158].

7.6.2 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[159] 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 [160] [161].

---

[154] [selection: *[assignment: parts of TSF data], TSF data]*
[155] [selection: *[assignment: parts of TSF], TSF]*
[156] [selection: *the TSF, another trusted IT product]*
[157] [assignment: *list of other functions for which a trusted channel is required]*
[158] [assignment: *list of functions for which a trusted channel is required]*
[159] *[selection: the TSF, another trusted IT product*]
[160] [assignment*: list of other functions for which a trusted channel is required]*
[161] *[assignment: list of functions for which a trusted channel is required]*

7.6.3 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[162] 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

a. User authentication according to FIA_UAU.1,

b. None[163] [164].

Note: The component FTP_ITC.1/VAD requires the TSF to support a trusted channel established by the HID to send the VAD which is a PIN or Password which needs protection in confidentiality.

7.6.4 FTP_ITC.1/DTBS Inter-TSF trusted channel – Signature creation Application

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/DTBS The TSF shall provide a communication channel between itself and 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[165] 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

a. signature creation,

b. none [166] [167].

Note: the “signature creation” above covers the transfer of the DTBS (to be first hashed then signed by the TOE) and transfer of DTBS/R (already hashed data to be signed by the TOE).

[162] [selection: *the TSF, another trusted IT product*]
[163] [assignment: list of other functions for which a trusted channel is required]
[164] [assignment: *list of functions for which a trusted channel is required*]
[165] [selection: *the TSF, another trusted IT product*]
[166] [assignment: *list of other functions for which a trusted channel is required]*
[167] [assignment: *list of functions for which a trusted channel is required*]

7.7 Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 4 (EAL4)

augmented by the following components:

- AVA_VAN.5
- ALC_DVS.2
- ATE_DPT.2
- ALC_FLR.1
- ALC_CMS.5
- ALC_TAT.2

Note: The TOE shall protect the assets against high attack potential. This includes intermediate storage in the chip as well as secure channel communications (see FDP_UIT.1, FTP-ITC.1).

7.8 Security Requirements Rationale

7.8.1 Security Requirements Coverage

The following table provides an overview for security functional requirements coverage.

	OT.Lifecycle_Security	*OT.SCD/SVD_Auth_Gen*	*OT.SCD_Unique*	*OT.SCD_SVD_Corresp*	*OT.SCD_Secrecy*	*OT.Sig_Secure*	*OT.Sigy_SigF*	*OT.DTBS_Integrity_TOE*	*OT.EMSEC_Design*	*OT.Tamper_ID*	*OT.Tamper_Resistance*	*OT.SCD_Auth_Imp*	*OT.TOE_SSCD_Auth*	*OT.TOE_TC_SVD_Exp*	*OT.TOE_TC_VAD_Imp*	*OT.TOE_TC_DTBS_Imp*
PP-Part 2, PP-0059-MA1, (PP SSCD KG)																
FCS_CKM.1/SCD_SVD	x		x	x	x											
FCS_CKM.4	x				x											
FCS_COP.1/SIG_GEN	x					x										
FDP_ACC.1/SCD/SVD_Generation	x	x														
FDP_ACF.1/SCD/SVD_Generation	x	x														
FDP_ACC.1/SVD_Transfer	x													x		
FDP_ACF.1/SVD_Transfer	x													x		
FDP_ACC.1/Signature_Creation	x						x									
FDP_ACF.1/Signature_Creation	x						x									
FDP_RIP.1					x		x									
FDP_SDI.2/Persistent				x	x	x										
FDP_SDI.2/DTBS							x	x								
FIA_AFL.1/PIN							x									

FIA_UID.1		x					x					x				
FIA_UAU.1		x					x					x	x			
FMT_SMR.1	x						x									
FMT_SMF.1	x			x			x									
FMT_MOF.1	x						x									
FMT_MSA.1/Admin_KG	x	x					x									
FMT_MSA.1/Signatory	x						x									
FMT_MSA.2	x	x					x									
FMT_MSA.3/KG	x	x					x									
FMT_MSA.4/KG	x	x		x			x									
FMT_MTD.1/Admin	x						x									
FMT_MTD.1/Signatory	x						x									
FPT_EMS.1/SCD_RAD					x				x							
FPT_FLS.1					x											
FPT_PHP.1										x						
FPT_PHP.3					x						x					
FPT_TST.1	x				x	x										
PP-Part 3, PP-0075, (PP SSCD KI)																
FDP_ACC.1/SCD_Import	x											x				
FDP_ACF.1/SCD_Import	x											x				
FDP_ITC.1/SCD	x															
FDP_UCT.1/SCD	x				x											
FMT_MSA.1/Admin_KI	x															
FMT_MSA.3/KI	x						x									
FMT_MSA.4/KI	x						x									
FTP_ITC.1/SCD	x				x											
PP-Part 4, PP-0071, (PP SSCD KG TCCGA)																
FDP_DAU.2/SVD														x		
FIA_API.1													x			
FTP_ITC.1/SVD														x		
PP-Part 5, PP-0072, (PP SSCD KG TCSCA) and PP-Part 6, PP-0076, (PP SSCD KI TCSCA)																
FDP_UIT.1/DTBS																x
FTP_ITC.1/VAD															x	
FTP_ITC.1/DTBS																x
Added additionally																
FCS_CKM.1/DH_PACE															x	x
FCS_CKM.1/SYM_AUTH	x			x								x	x	x		
FCS_COP.1/SM_MAC				x								x	x	x	x	x
FCS_COP.1/SM_ENC				x								x	x	x	x	x
FCS_COP.1/SYM_AUTH	x			x								x	x	x		
FPT_EMS.1/KEYS									x							
FIA_AFL.1/PACE															x	x
FTP_ITC.1/AUTHKEY	x			x								x	x	x		

FDP_ACC.1/AUTHKEY_Admin	x			x							x	x	x		
FDP_ACF.1/AUTHKEY_Admin	x			x							x	x	x		
FMT_MSA.3/AUTHKEY	x			x							x	x	x		

7.8.2 Security Requirements Sufficiency

The security objective **OT.Lifecycle_Security** "Lifecycle security" is provided by the SFR for SCD/SVD generation FCS_CKM.1/SCD_SVD, SCD usage FCS_COP.1/SIG_GEN and SCD destruction FCS_CKM.4 which ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer.
The SCD 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, 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 lifecycle.
FCS_CKM.1/SYM_AUTH, FCS.COP.1/SYM_Auth, FDP_ITC.1/AUTH_KEY, FDP_ACC.1/AUTHKEY_Admin, FDP_ACF.1/AUTHKEY_Admin and FMT_MSA.3/AUTHKEY provide an authentication of Admin/CGA and trusted channel and the related management functions for administration of the authentication keys needed.

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

The security objective **OT.SCD_Auth_Imp** "Authorised SCD import" is provided by the security functions specified by the following SFR. FIA_UID.1 and FIA_UAU.1 ensure that the user is identified and authenticated before SCD can be imported. FDP_ACC.1/SCD_Import and FDP_ACF.1/SCD_Import ensure that only authorised users can import SCD.
FCS_CKM.1/SYM_AUTH, FCS_COP.1/SM_MAC, FCS_COP.1/SM_ENC and FCS_COP.1/SYM_AUTH provide an authentication of Admin/CGA and trusted channel for SCD import to detect any modification of SCD during import. FTP_ITC.1/AUTHKEY, FDP_ACC.1/AUTHKEY_Admin, FDP_ACF.1/AUTHKEY_Admin and FMT_MSA.3/AUTHKEY provide the necessary management functions for import and management of the authentication keys.

The security objective **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) of thed irective, which is provided by the cryptographic algorithms specified by FCS_CKM.1/SCD_SVD.

The security objective **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_SVD 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. FCS_CKM.1/SYM_AUTH, FCS_COP.1/SM_MAC, FCS_COP.1/SM_ENC and FCS_COP.1/SYM_AUTH provide an authentication of Admin/CGA and trusted channel for SVD export to detect any modification of SVD during export. FTP_ITC.1/AUTHKEY, FDP_ACC.1/AUTHKEY_Admin, FDP_ACF.1/AUTHKEY_Admin and FMT_MSA.3/AUTHKEY provide the necessary management functions for import and management of the authentication keys.

The security objective **OT.SCD_Secrecy** “Secrecy of signature creation data” is provided by the security functions specified by the following SFR. FCS_CKM.1/SCD_SVD ensures the use of secure cryptographic algorithms for SCD/SVD generation.
The confidentiality for SCD import is provided by the security functions specified by the following SFR. FDP_UCT.1/SCD and FTP_ICT.1/SCD.
Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.
The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).
SFR FPT_EMS.1/SCD_RAD and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

The security objective **OT.Sig_Secure** “Cryptographic security of the electronic signature” is provided by the cryptographic algorithms specified by FCS_COP.1/SIG_GEN, 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.

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

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

The security objective **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.

The security objective **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.

The security objective **OT.EMSEC_Design** "Provide physical emanations security" covers that no intelligible information is emanated. This is provided by FPT_EMS.1/SCD_RAD.1. and FPT_EMS.1/KEYS for the authentication keys of SSCD Provisioning Service and CGA, PACE MRZ/CAN and Secure Messaging Session Keys.

The security objective **OT.Tamper_ID "**Tamper detection" is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

The security objective **OT.Tamper_Resistance** "Tamper resistance**"** is provided by FPT_PHP.3 to resist physical attacks.

The security objective **OT.TOE_SSCD_Auth** "Authentication proof as SSCD" requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by FIA_API.1 (Authentication Proof of Identity). The SFR FIA_UAU.1 allows (additionally to the core PP SSCD KG) establishment of the trusted channel before (human) user is authenticated.

FCS_CKM.1/SYM_AUTH and FCS_COP.1/SYM_AUTH provide an authentication of Admin/CGA and TOE which is a mutual authentication with TOE individual keys and therefore allows authentication of the TOE as SSCD. FTP_ITC.1/AUTHKEY, FDP_ACC.1/AUTHKEY_Admin, FDP_ACF.1/AUTHKEY_Admin and FMT_MSA.3/AUTHKEY provide the necessary management functions for import and management of the authentication keys.

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

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

- FTP_ITC.1/SVD Inter-TSF trusted channel), which requires the TOE to provide a trusted channel to the CGA.

FCS_CKM.1/SYM_AUTH, FCS_COP.1/SM_MAC, FCS_COP.1/SM_ENC and FCS_COP.1/SYM_AUTH provide an authentication of Admin/CGA and trusted channel for SVD export to detect any modification of SVD during export. FTP_ITC.1/AUTHKEY, FDP_ACC.1/AUTHKEY_Admin, FDP_ACF.1/AUTHKEY_Admin and FMT_MSA.3/AUTHKEY provide the necessary management functions for import and management of the authentication keys.

The security objective **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. FCS_CKM.1/DH_PACE, FCS_COP.1/SM_MAC, FCS_COP.1/SM_ENC and FIA_AFL.1/PACE provide an authentication of HID and trusted channel for VAD import to protect the VAD.

The security objective **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. FCS_CKM.1/DH_PACE, FCS_COP.1/SM_MAC, FCS_COP.1/SM_ENC and FIA_AFL.1/PACE provide an authentication of SCA and trusted channel for DTBS import to protect the DTBS.

7.8.3 Satisfaction of dependencies of security requirements

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non- dissolved dependencies are appropriately explained.

The following Table shows the dependencies between the SFR of the TOE:

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/SCD_SVD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/SIG_GEN, FCS_CKM.4
FCS_CKM.1/DH_PACE	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	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.
FCS_CKM.1/SYM_AUTH	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/SYM_AUTH, FCS_CKM.4

FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1/SCD_SVD, FCS_CKM.1/DH_PACE, FCS_CKM.1/SYM_AUTH
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/SCD_SVD, FCS_CKM.4
FCS_COP.1/SM_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/DH_PACE, FCS_CKM.1/SYM_AUTH, FCS_CKM.4
FCS_COP.1/SM_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/DH_PACE, FCS_CKM.1/SYM_AUTH, FCS_CKM.4
FCS_COP.1/SYM_AUTH	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_ITC.1/AUTHKEY, FCS_CKM.4
FDP_ACC.1/AUTHKEY_Admin	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/AUTHKEY_Admin

FDP_ACF.1/AUTHKEY_Admin	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/AUTHKEY_Admin, FMT_MSA.3/AUTHKEY
FDP_ACC.1/SCD/SVD_Generation	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/SCD/SVD_Generation
FDP_ACF.1/SCD/SVD_Generation	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3/KG.
FDP_ACC.1/SCD_Import	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/ SCD_Import
FDP_ACF.1/ SCD_Import	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/ SCD_Import, FMT_MSA.3/KI
FDP_ACC.1/SVD_Transfer	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SVD_Transfer	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/SVD_Transfer, FMT_MSA.3/KG
FDP_ACC.1/Signature_Creation	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/ Signature_Creation
FDP_ACF.1/ Signature_Creation	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/Signature_Creation, FMT_MSA.3/KG, FMT_MSA.3/KI
FDP_ITC.1/AUTH_KEY	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_ACC.1/AUTHKEY_Admin, FMT_MSA.3/AUTHKEY
FDP_RIP.1	No dependencies	n.a.
FDP_SDI.2/Persistent	No dependencies	n.a.
FDP_SDI.2/DTBS	No dependencies	n.a.
FIA_AFL.1/PIN	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_AFL.1/PACE	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_SMF.1	No dependencies	n.a.

FMT_MOF.1	FMT_SMR.1 Security roles, FMT_SMF.1 Security management functions	Fulfilled by FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin_KG	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Security management functions	Fulfilled by FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin_KI	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Security management functions	Fulfilled by FDP_ACC.1/SCD_Import, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Security management functions	Fulfilled by FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[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	Fulfilled by FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/SCD_Import, FDP_ACC.1/Signature_Creation, FMT_MSA.1/Admin_KG, FMT_MSA.1/Admin_KI, FMT_MSA.1/Signatory FMT_SMR.1
FMT_MSA.3/AUTHKEY	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Justification: the object AUTHKEYS has no security attributes assigned, therefore management of those makes no sense (FMT_MSA.1) makes no sense in this case, FMT_SMR.1
FMT_MSA.3/KG	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Fulfilled by FMT_MSA.1/Admin_KG, FMT_MSA.1/Signatory FMT_SMR.1
FMT_MSA.3/KI	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Fulfilled by FMT_MSA.1/Admin_KI, FMT_MSA.1/Signatory FMT_SMR.1
FMT_MSA.4/KG	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation

FMT_MSA.4/KI	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FDP_ACC.1/SCD_Import, FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	FMT_SMR.1 Security roles, FMT_SMF.1 Security management functions	Fulfilled by FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1 Security roles, FMT_SMF.1 Security management functions	Fulfilled by FMT_SMR.1, FMT_SMF.1
FPT_EMS.1/SCD_RAD	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.
FDP_ITC.1/SCD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_ACC.1/SCD_Import, FMT_MSA.3/KI
FDP_UCT.1/SCD	[FTP_ITC.1 Import of user data without security attributes, FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FTP_ITC.1/SCD, FDP_ACC.1/SCD_Import
FTP_ICT.1/SCD	No dependencies	n.a.
FDP_DAU.2/SVD	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_API.1	No dependencies	n.a.
FTP_ITC.1/SVD	No dependencies	n.a.
FDP_UIT.1/DTBS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Import of user data without security attributes, FTP_TRP.1 Trusted path]	Fulfilled by FDP_ACC.1/Signature_Creation FTP_ITC.1/DTBS
FTP_ITC.1/VAD	No dependencies	n.a.
FTP_ITC.1/DTBS	No dependencies	n.a.

The following Table shows the dependencies of the security assurance requirements:

Assurance requirement(s)	Dependencies	Support of the Dependencies

EAL4 package	dependencies of EAL4 package are not reproduced here)	Fulfilled by construction, all dependencies are satisfied in a CC EAL package
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	Fulfilled by ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.2. (included in the EAL4 assurance package)
ALC_CMS.5	No dependencies	
ALC_DVS.2	No dependencies	
ALC_FLR.1	No dependencies	
ALC_TAT.2	ADV_IMP.1	Fulfilled by ADV_IMP.1. (included in the EAL4 assurance package)
ATE_DPT.2	ADV_ARC.1, ADV_TDS.3, ADV_FUN.1	Fulfilled by ADV_ARC.1, ADV_TDS.3, ADV_FUN.1. (included in the EAL4 assurance package)

7.8.4 Rationale for chosen security assurance requirements

The assurance level for this protection profile is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialised processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this Security Target is just such a product.

Augmentation results from the selection of:

- AVA_VAN.5 Advanced methodical vulnerability analysis (as in the underlying PP):
  the TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, i.e. the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure.
- ALC_DVS.2 Sufficiency of security measures:
  the selection of the component ALC_DVS.2 provides a higher assurance of the security of the TOE's development and manufacturing especially for the secure handling of the TOE's material.

- ATE_DPT.2 Testing: security enforcing modules:
  the selection of the component ATE_DPT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR-enforcing modules.
- ALC_FLR.1 Basic flaw remediation:
  the selection of the component ALC_FLR.1 provides basic handling of security flaws. This component provides guidance procedures on how to handle security flaws (i.e.: tracking, documentation, correction, status).
- ALC_CMS.5 Development tools CM coverage
  the selection of the component ALC_CMS.5 provides the highest available assurance level regarding the management of configuration items. The configuration lists contains configuration items such as the implementation representation, development tools and security flaws. This configuration items play an important role in the production of a quality TOE version and are important to maintain in a controlled manner.
- ALC_TAT.2 Compliance with implementation standards:
  The selection of the component ALC_TAT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring to document the TOE development tools.

The component ALC_DVS.2 has no dependencies.

The component ATE_DPT.2 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_TDS.3 Basic modular design
- ADV_FUN.1 Functional testing

All of these are met or exceeded in the EAL4 assurance package.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_PRE .1 Preparative procedures

All of these are met or exceeded in the EAL4 assurance package.

The component ALC_FLR.1 has no dependencies.

The component ALC_CMS.5 has no dependencies.

The component ALC_TAT.2 has the following dependencies: ADV_IMP.1 which is met by the EAL4 assurance package.

8 TOE summary specification (ASE_TSS)

This TOE provides the following Security Services:

- Identification and Authentication
- Access Control
- Cryptographic Operations
- Data Confidentiality and Integrity
- Protection

8.1 TOE Security Services

8.1.1 Identification and Authentication

This service provides identification and authentication of the following user roles:

1. R.Admin (SSCD Provisioning Service and CGA)
2. R.Sigy (Signatory)

Note: a user acting in the role of a (Pre-)Personalization Agent acts in the role of the Administrator R.Admin.

The TOE does not provide any security services or allows any actions by any subjects unless identified and authenticated except (FIA_UID.1, FIA_UAU.1):

1. to establish a trusted channel between
    a. the SSCD Provisioning Service and the TOE
    b. the CGA and the TOE
    c. the HID / SCA and the TOE
2. to identify themselves by selection of the authentication key/PIN,
3. to authenticate using authentication key/PIN
4. to perform self-test
5. to read/update additional EFs inside the SSCD application
6. to use MPA applications

PIN Verification / Authentication
This service provides the PIN / Password Verification for PIN, TPIN and PUK according [19] (FIA_AFL.1/PIN, FMT_MSA.1, FMT_MTD.1, FDP_ACF.1/Signature Creation, FDP_ACC.1/Signature_Creation) for authentication of the user roles R.Sigy.

PACE Protocol Authentication
This service provides the PACE Protocol according to [44], covered by FCS_CKM.1/DH_PACE, FIA_AFL.1/PACE and FIA_UAU.1 for establishing a trusted channel between the HID and the TOE (FTP_ITC.1/VAD) as well as between the SCA and the TOE (FTP_ITC.1/DTBS).

Symmetric Mutual Authentication
The TOE provides Symmetric Authentication according to EN 419212-3 [20], Section 3.8 for Authentication of the SSCD Provisioning Service or the CGA, for identification of the TOE as SSCD and for establishing a trusted channel between the SSCD Provisioning Service / CGA and the TOE (FTP_ITC.1/SVD, FTP_ITC.1/SCD, FCS_COP.1/SYM_AUTH, FCS_CKM.1/SYM_AUTH) and is used for secure public key export (FDP_DAU.1) / import of SCD and for administration / configuration tasks. In addition this service is also used for all (pre-)personalization tasks.

TOE identification
The TOE provides Symmetric Authentication (which is a mutual authentication) using a TOE unique key which allows TOE identification (FIA_API.1), see above.

8.1.2 Access Control

This service provides access control to protect data and/or keys from unauthorized modification and/or disclosure. The access control is based on security roles for Administrator and Signatory (FMT_SMR.1).

Only subjects that can be successfully authenticated and authorized are allowed to write or modify data on the TOE. Also reading of data and/or using keys is limited to authenticated entities.

TOE Management
Only the Signatory can enable the Signature Creation Function for each SCD (FMT_MSA.1/Signatory) by entering initial RAD (transport PIN, which can be used only once).

Only the Administrator (SSCD Provisioning Service, CGA) can configure the TOE / perform management functions (FCS_COP.1/SYM_AUTH, FCS_CKM.1/SYM_AUT, FMT_SMF.1, FMT_MOF.1, FMT_MSA.3/KG, FMT_MSA.3/KI, FMT_MSA.3/AUTHKEY, FMT_MSA.4/KG and FMT_MSA.4/KI).

Write Access
Only the SSCD Provisioning Service and CGA can

- Initiate generation of keys by the TOE for signature (FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation)
- import keys for signature creation to the TOE (FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FDP_ITC.1/SCD, FMT_MSA.1/Admin_KG, FMT_MSA.1/Admin_KI).

Only the SSCD Provisioning Service can

- create the RAD, T-PIN and PUK (FMT_MTD.1/Admin, FMT_SMF.1)
- create SCD / SVD (FMT_SMF.1)
- write T-PIN and PUK value (FMT_SMF.1)
- terminate SCD, RAD, TPIN and (PUK FMT_SMF.1)
- create additional EFs
- delete SSCD application
- create, import, change, delete, deactivate, terminate AUTHKEYS (FDP_ACC.1/AUTHKEY_Admin, FDP_ACF.1/AUTHKEY_Admin)

Only the Signatory can

- modify, unblock the RAD (FMT_MTD.1/Signatory)
- delete RAD, PUK, TPIN and SCD/SVD (FMT_SMF.1)

In the development phase the developer can write initial authentication keys for later authentication of the SSCD Provisioning Service (for pre-personalization) and identification data.

Read Access
The CGA and SSCD Provisioning Service and Signatory can read the SVD (FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer).

Use of Keys for Signature Creation
Only the Signatory can use the keys for signature creation (FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation).

8.1.3 Cryptographic Operations

Signature Generation and Hashing
This service provides cryptographic signature generation (FCS_COP.1/SIG_GEN) over the data to be signed DTBS). The DTBS are either sent by the terminal in form of representation as a hash value (DTBS/R) or as a whole and are hashed by the TOE.

Key Generation and Destruction
This service provides a cryptographic key generation (FCS_CKM.1/SCD_SVD, FCS_CKM.1/DH_PACE, FCS_CKM.1/SYM_AUTH) and destruction (FCS_CKM.4).

Cryptographic Authentication
PACE Protocol Authentication and Symmetric Mutual Authentication (as described above) covered by FCS_CKM.1/DH_PACE, FCS_CKM.1/SYM_AUTH, FCS_COP.1/SYM_AUTH.

8.1.4 Data Confidentiality and Integrity

This service provides the Secure Messaging in MAC-ENC mode according to [44] and integrity self tests and monitoring.

Secure Messaging
After successfully running the PACE protocol according to [44] or performing Symmetric Authentication according [20] Chapt 3.8 this service provides an AES or TDES encrypted data stream between an authenticated entity (SSCD Provisioning Service, CGA, SCA, HID) and the TOE (FCS_COP.1/SM_ENC, FCS_COP.1/SM_MAC).

It protects confidentiality of the transmitted data (especially DTBS, VAD, SCD/SVD, Management Data) and from modification, deletion, insertion and replay of transmitted data and detects such (FDP_UIT.1/DTBS, FDP_UCT.1/SCD, FDP_DAU.2/SVD, FTP_ITC.1/ SVD, FTP_ITC.1/VAD, FTP_ITC.1/DTBS).

Integrity Self Test and Monitoring
This service runs data integrity self-test after reset on OS start-up and periodically during normal operation (FPT_TST.1), especially it ensures that sensitive data stored on the TOE, in particular TSF and user data or keys used by the security functionality and any code are integrity protected and that data integrity is verified on any data access.

This service ensures furthermore that only executable code is stored on the TOE which integrity is verified. The integrity of code is verified during loading in life-cycle “Development Phase” and “SSCD Preparation”.

This service also ensures that the integrity of DTBS is checked when stored in the TOE (FSP_SDI.2/DTBS) as well as integrity of SCD and SVD (when persistently stored in the TOE, FDP_SDI.2/Persistent Stored data integrity monitoring and action).

8.1.5 Protection

Hardware and Software (IC Security Embedded Software)
This service ensures that the TOE always operates in a secure state (TOE reset or switching to life-cycle TERMINATED) even if an attack or failure is detected or operating conditions are causing a malfunction (FPT_FLS, FPT_PHP.1, FPT_PHP.3).

This service ensures that no variations in IC power consumption or electromagnetic emissions and variations in command execution time are emitted by the TOE to allow an attacker to gain sensitive data stored on the TOE that is used for identification, authentication and secure messaging purposes or to corrupt the security functionality of the TOE (software: FPT_EMS.1/SCD_RAD and FPT_EMS.1/KEYS hardware: FDP_ITT.1).

Software (IC embedded software)
The service protects cryptographic key data by securely destroying it (FCS_CKM.4) when they are not needed any more and/or in case of TOE termination.

8.2 Statement of Compatibility

This section shows the compatibility of this Composite ST and the Platform-ST as required by [45].

The Platform-ST is the security target of Infineon Security Controller IFX_CCI_000005h H13 and IFX_CCI_000008h H13 used by this TOE as platform.

8.2.1 Security Assurance Requirements

The Hardware-Platform Security Target provides

- EAL6 augmented by ALC_FLR.1

The Composite-ST requires:

- EAL4 augmented with ALC_DVS.2, ATE_DPT.2, AVA_VAN.5, ALC_FLR.1, ALC_CMS.5 and ALC_TAT.2.

8.2.2 Assumptions

The following table list all assumptions of the hardware platform related to its operational environment not relevant for this ST.

Assumptions of the HW platform related to its operational environment inherited from [25]	Meaning	Operational Environment of this TOE
A.Plat-Appl	Usage of Hardware Platform	n.a.

The following table list all relevant assumptions of the hardware platform related to its operational environment which are fulfilled by the ST.

Assumptions of the HW platform related to its	Meaning	Operational Environment of this TOE

operational environment inherited from [25]		
A.Resp-Appl	Treatment of User Data	OT.Lifecycle_Security OT.SCD/SVD_Auth_Gen OT.SCD_Unique OT.SCD_SVD_Corresp OT.SCD_Secrecy OT.Sig_Secure OT.Sigy_SigF OT.DTBS_Integrity_TOE OT.EMSEC_Design OT.Tamper_ID OT.Tamper_Resistance OT.SCD_Auth_Imp OT.TOE_SSCD_Auth OT.TOE_TC_SVD_Exp OT.TOE_TC_VAD_Imp OT.TOE_TC_DTBS_Imp
A.Key-Function	Usage of Key-dependent Functions	OT.EMSEC_Design
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation	n.a.

8.2.3 Security Objectives

The following table lists those security objectives of the hardware platform which can be mapped to the relevant security objective of this ST.

Security objectives of the Platform-ST	OTs of the Composite-ST						
	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
O.Phys-Manipulation						x	x
O.Phys-Probing						x	x
O.Malfunction						x	x
O.Leak-Inherent					x		
O.Leak-Forced			x				
O.Add-Functions	x	x	x	x			

These security objectives of the Platform-ST and the OTs of this Composite-ST are not contradictory since they can be mapped.

The following security objective of platform cannot be mapped to OTs of this ST

- O.Mem-Access
- O.Identification
- O.Cap_Avail_loader
- O.Authentication
- O.Ctrl_Auth_loader
- O.Abuse-Func

since no OT of the Composite-ST needs the respective security functionality. This implies no conflict.

For the following OTs of the Composite-ST no security objectives of platform exists which can be mapped directly. However no conflict was found.

- OT.Lifecycle_Security
- OT.SCD/SVD_Auth_Gen
- OT.Sigy_SigF
- OT.DTBS_Integrity_TOE
- OT.SCD_Auth_Imp
- OT.TOE_SSCD_Auth
- OT.TOE_TC_SVD_Exp
- OT.TOE_TC_VAD_Imp
- OT.TOE_TC_DTBS_Imp

With the mapping of security objectives of platform and the security objectives of this ST all security objectives are listed and therefore the security objectives of the Platform-ST are not contradictory to those of this composite ST.

8.2.4 Security Objectives Environment

The Security Target of the Hardware Platform lists the following Security Objectives for the operational environment:

- OE.Lim_Block_Loader
- OE.TOE_Auth
- OE.Loader_Usage secure
- OE.Process-Sec-IC

According to the “Note 8”, Page 53 of the Security Target these objectives only apply when the HW platform comes with an activated Flash Loader.

This is especially the case for “Option b)” in Life Cycle Phase 1 (see Chapter 2.3.4), which means that the SSCD Provisioning Service is enabled to download the Chip Embedded Software using the Loader provided by the Chip Dedicated software.

In this situation the SSCD Provisioning Service still act’s as the “TOE Manufacturer” in the sense of the Chip Hardware Certification and therefore the Objectives for the Operational Environment as given in the Hardware Platform Security Target apply to him directly and therefore don’t need to be re-stated in the Security Target at hand.

In the sense of ASE_COMP.1 these Objectives are rated as Ir.OE as they address the TOE Manufacturer in the sense of the Chip Hardware Certification.

Note: The IC Embedded Software to be loaded does not provide Loader Functionality itself.

Objective for the Operational Environment in the HW platform ST	Meaning	Classification	Operational Environment of this TOE
OE.Lim_Block_Loader	Limitation of capability and blocking the Loader	Ir.OE	n/a
OE.TOE_Auth	Authentication to external entities	Ir.OE	n/a
OE.Loader_Usage secure	communication and usage of the Loader	Ir.OE	n/a
OE.Process-Sec-IC	Protection during composite product manufacturing	Ir.OE	n/a

8.2.5 Organizational Security Policies

The Platform-ST lists two organizational security policies:

- P.Process-TOE
- P.Add-Functions.

OSP P.Process-TOE of the platform is not relevant since this organizational security policy is valid before the IC Embedded Software is loaded which means before the composite TOE described by this ST exists.

OSP P.Add-Functions of the platform is relevant since this policy provides security functionality needed by

- P.Sigy_SSCD

of the composite ST.

The organizational security policies of the Platform-ST and the OTs of this Composite-ST are not contradictory since they are not relevant or can be used directly by this TOE.

8.2.6 Threats

The following table provides a mapping of the threats of the Platform-ST to the threats of this ST.

Threats of the Platform-ST	Threats of this ST	
T.Leak-Inherent	x	
T.Phys-Probing		x
T.Malfunction		x
T.Phys-Manipulation		X
T.Leak-Forced	x	
T.Abuse-Func		x
T.RND	x	

The threats of the Platform-ST and the threats of this ST are not contradictory since they can be mapped.

The following threats of platform cannot be mapped to the threats of this ST:

- T.Mem-Access

For the following threats of the Composite-ST no threats of the platform exists:

- T.SCD_Derive
- T.SVD_Forgery
- T.SigF_Misuse
- T.DTBS_Forgery
- T.Sig_Forgery

8.2.7 Security Functional Requirements

The relevant security requirements of the composite TOE can be mapped directly to the hardware's SFRs. When the relation is not obvious an explanation is given in brackets.

None of them show any conflicts between each other. Platform SFRs that are not used by the composite ST are not listed.

Platform SFR	Meaning	Category[168]	Supports TOE SFR
FRU_FLT.2	Limited Fault Tolerance	RP_SFR-MECH	FPT_TST.1, FPT_PHP.1, FPT_PHP.3, FPT_FLS.1
FPT_FLS.1	Failure with Preservation of Secure State	RP_SFR-MECH	FPT_FLS.1, FPT_PHP.1, FPT_PHP.3
FPT_PHP.3	Resistance to Physical Attack	RP_SFR-MECH	FPT_PHP.1, FPT_PHP.3
FDP_ITT.1	Basic Internal Transfer Protection	RP_SFR-MECH	FPT_EMS.1/SCD_RAD, FPT_EMS.1/KEYS
FDP_IFC.1	Subset Information Flow Control	RP_SFR-MECH	FPT_EMS.1/SCD_RAD, FPT_EMS.1/KEYS
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	RP_SFR-MECH	FPT_EMS.1/SCD_RAD, FPT_EMS.1/KEYS
FCS_RNG.1	Quality Metric for Random Numbers	RP-SFR-SERV	FCS_CKM.1/SCD_SVD, FCS_COP.1/SIG_GEN, FCS_CKM.1/DH_PACE, FIA_UID.1 (for PACE), FPT_EMS.1/SCD_RAD (for blinding), FCS_COP.1/SYM_AUTH, FPT_EMS.1/KEYS (for blinding)
FPT_TST.2	Subset TOE Security Testing	RP_SFR-MECH	FPT_TST.1, FPT_PHP.3
FCS_CKM.1/EC	Cryptographic key generation	RP-SFR-SERV	FCS_CKM.1/SCD_SVD, FCS_CKM.1/DH_PACE

[168] Either „IP_SFR": irrelevant, „RP-SFR-SERV": relevant in TSFI implementation, "RP_SFR-MECH": relevant and addressed in ARC

FCS_COP.1/ECDH	Cryptographic Support (ECDH)	RP-SFR-SERV	FIA_UID.1, FTP_ITC.1/VAD, FTP_ITC.1/DTBS, FCS_CKM.1/DH_PACE
FCS_COP.1/ECDSA	Cryptographic Support (ECDSA)	RP-SFR-SERV	FCS_COP.1/SIG_GEN
FCS_CKM.1/RSA	Cryptographic key generation	RP-SFR-SERV	FCS_CKM.1/SCD_SVD
FCS_COP.1/RSA	Cryptographic Support (RSA)	RP-SFR-SERV	FCS_COP.1/SIG_GEN
FCS_COP.1/DES	Cryptographic Support (3DES)	RP-SFR-SERV	FCS_COP.1/SM_ENC, FCS_COP.1/SM_MAC FCS_COP.1/SYM_AUTH, FDP_UCT.1, FDP_DAU.2/SVD, FIA_API.1, FIA_UID.1, FTP_ITC.1/VAD, FTP_ITC.1/DTBS, FTP_ITC.1/SCD, FTP_ITC.1/SVD (all for PACE, Symmetric Auth and secure messaging)
FCS_COP.1/AES	Cryptographic Söupport (AES)	RP-SFR-SERV	FCS_COP.1/SM_ENC, FCS_COP.1/SM_MAC, FCS_COP.1/SYM_AUTH, FDP_UCT.1, FDP_DAU.2/SVD, FIA_API.1, FIA_UID.1, FTP_ITC.1/VAD, FTP_ITC.1DTBS, FTP_ITC.1/SCD, FTP_ITC.1/SVD (all for PACE, Symmetric Auth and secure messaging)
FAU_SAS.1	Audit Storage	IP_SFR	not used by TSF directly
FMT_LIM.1	Limited Capabilities	RP_SFR-MECH	not used by TSF directly
FMT_LIM.2	Limited Availability	RP_SFR-MECH	not used by TSF directly
FDP_ACC.1	Subset Access Control	RP_SFR-MECH	FPT_FLS.1
FDP_ACF.1	Security Attribute Based Access Control	RP_SFR-MECH	FPT_FLS.1
FDP_SDI.1	Stored Data Integrity Monitoring	RP_SFR-MECH	FDP_SDI.2/Persistent, FDP_SDI.2/DTBS, FPT_PHP.3
FDP_SDI.2	Stored Data Integrity Monitoring and Action	RP_SFR-MECH	FDP_SDI.2/Persistent, FDP_SDI.2/DTBS,

			FPT_PHP.3
FMT_MSA.1	Management of Security Attributes	RP_SFR-MECH	FPT_EMS.1/SCD_RAD, FPT_FLS.1, FPT_PHP.3
FMT_MSA.3	Static Attribute Initialization	RP_SFR-MECH	FPT_EMS.1/SCD_RAD, FPT_FLS.1, FPT_PHP.3
FMT_SMF.1	Specification of Management Functions	RP_SFR-MECH	FPT_FLS.1, FPT_PHP.3

There is no conflict between the security problem definition, the security objectives and the security requirements of the composite ST and the platform ST. All related details (operations on SFRs, definition of security objectives, threats) can be found in both STs.

9 Acronyms

Acronym	Term
AUTHKEYS	Symmetric Keys for mutual authentication between SSCD Provisioning Service / CGA / (Pre-)Personalizer and the TOE.
BIS	Basic Inspection System
BIS-PACE	Basic Inspection System with PACE
CAN	Card Access Number
CC	Common Criteria
CGA	Certificate Generation Application
CSP	Certificate Service Provider
DTBS	Data To Be Signed
DTBS/R	Unique Representation of DTBS
EAL	Evaluation Assurance Level
EF	Elementary File
HID	Human Interface Device
ICCSN	Integrated Circuit Card Serial Number.
MF	Master File
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PP	Protection Profile
PP SSCD KG	Protection Profile for Secure Signature Creation Device with Key Generation
PP SSCD KI	Protection Profile for Secure Signature Creation Device with Key Import
PP SSCD KG TCCGA	Protection Profile for Secure Signature Creation Device with Key Generation and Trusted Communication with Certificate Generation Application
PP SSCD KG TCSCA	Protection Profile for Secure Signature Creation Device with Key Generation and Trusted Communication with Signature Creation Application
PP SSCD KI TCSCA	Protection Profile for Secure Signature Creation Device with Key Import and Trusted Communication with Signature Creation Application
RA	Registration Authority
RAD	Reference Authentication Data

RF	Radio Frequency
SAR	Security assurance requirements
SCA	Signature Creation Application
SCD	Signature Creation Data
SFP	Security Function Policy
SFR	Security functional requirement
SIP	Standard Inspection Procedure
SSCD	Secure Signature (and seal) Creation Device
ST	Security Target
SVD	Signature Verification Data
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy (defined by the current document)
VAD	Verification Authentication Data

10 Bibliography

[1] *CEN, EN 419211-2, Edition: 2013-09-15, Protection profiles for secure signature creation device - Part 2: Device with key generation, Version 2.0.1, BSI-CC-PP-0059-2009-MA-01.*

[2] *CEN, EN 419211-3, Edition: 2014-02-01, Protection profiles for secure signature creation device - Part 3: Device with key import, Version 1.0.2, BSI-CC-PP-0075.*

[3] *CEN, EN 419211-4, Edition: 2014-02-01, Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application, Version 1.01, BSI-CC-PP-0071.*

[4] *CEN, EN 419211-5, Edition: 2014-02-01, Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application, Version 1.01, BSI-CC-PP-0072.*

[5] *CEN, EN 419211-6, Edition: 2014-11-15, Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application, Version 1.0.4, BSI-CC-PP-0076.*

[6] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093.*

[7] *Austria Card, Security Target ACOS-IDv2.0 SSCD (A) CB-Comm, Version 1.01, Date 2021-11-16.*

[8] *ANSSI –PG-083, "GUIDE DES MÉCANISMES CRYPTOGRAPHIQUES, RÈGLES ET RECOMMANDATIONS CONCERNANT LE CHOIX ET LE DIMENSIONNEMENT DES MÉCANISMES CRYPTOGRAPHIQUES", Version 2.04, 01.01.2021.*

[9] *SOG-IS Crypto Working Group, Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2, January 2020, https://www.sogis.eu/uk/supporting_doc_en.html.*

[10] *Security Target - ACOS-IDv2.0 eMRTD (A) EAC/PACE configuration, Version 1.01, Date 2021-07-19.*

[11] *ISO/IEC 7816-3 Identification cards - Integrated circuit - Cards with contacts - Electrical interface and transmission protocols, Third edition 2006-11-01.*

[12] *ISO/IEC 7816-4 "Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange", third edition 2013-04-15.*

[13] *ISO/IEC 7816-8 "Identification cards - Integrated circuit cards - Part 8: Commands and mechanisms for security operations", third edition 2016-11-01.*

[14] *ISO/IEC 7816-9 "Identification cards - Integrated circuit cards - Part 9: Commands for card management", 2017, third edition 2017-12.*

[15] *ISO/IEC 14443-1:2018 Cards and security devices for personal identification - Contactless proximity objects - Part 1: Physical characteristics.*

[16] *ISO/IEC 14443-2:2016, Identification cards - Contactless integrated circuit, cards - Proximity cards - Part 2: Radio frequency power and signal interface.*

[17] *ISO/IEC 14443-3:2018, Cards and security devices for personal identification - Contactless proximity objects - Part 3: Initialization and anticollision.*

[18] *Technical Guideline TR-03110 Part 1-4, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token.*

[19] *EN 419212-2 Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part-2: Signature and Seal Service, Edition 2018-03-01.*

[20] *EN 419212-3 Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part-3: Device authentication protocols, Edition 2017-11-01.*

[21] *International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Part 11: Security Mechanisms for eMRTDs", seventh edition, 2015.*

[22] *Infineon, Common Criteria Public Security Target, EAL6 augmented / EAL6+, IFX_CCI_000003h,000005h, 000008h, 00000Ch, 000013h, 000014h,000015h, 00001Ch, 00001Dh, 000021h, 000022h H13, Revision 1.6, 2019.*

[23] *Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014..*

[24] BSI, "Certification Report BSI-DSZ-CC-1110-V4-2021," 2021.

[25] *Eurosmart Security IC Platform Protection Profile with Augmentation Packages, registered under BSI-CC-PP-0084-2014, Version 1.0, dated 2014-01-13.*

[26] *Austria Card, "Preparation and Operational Manual - ACOS-IDv2.0 SSCD (A)", Version v1.01, Date 2021-11-16.*

[27] *Austria Card, ACOS-ID User Manual, Version 2.12, Date 19.05.2021.*

[28] *Austria Card, Internal Operation Manual - ACOS-IDv2.0, Version 1.2, 2021-07-19.*

[29] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017.*

[30] *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, July 2017.*

[31] *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, July 2017.*

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

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

[34] *American National Standards Institute, The Elliptic Curve Digital Signature Algorithm (ECDSA)m ANSI X9.62-2005, 2005-11-16.*

[35] *ISO /IEC 14888-3:2006, Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms, including technical corrigendum 2, published 2009-02-15.*

[36] *NIST Federal Information Processing Standards Publication, FIPS PUB 186-4, Digital Signature Standard (DSS), 2013-07.*

[37] *IETF, RFC-5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010.*

[38] *ANSI X9.31, DIGITAL SIGNATURES USING REVERSIBLE PUBLIC KEY CRYPTOGRAPHY FOR THE FINANCIAL SERVICES INDUSTRY, 1998 Edition, September 9, 1998.*

[39] BSI-TR-03111, *Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111, Version 1.11, 17.04.2009.*

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

[41] *Technical Guideline BSI TR-03111, Elliptic Curve Cryptography, Version 2.10, 2018.*

[42] *IETF, PKCS #1: RSA Cryptography Specifications Version 2.2, November 2016.*

[43] *ISO/IEC 10118-3:2018, IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions, 2018-10.*

[44] *International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010.*

[45] *BSI, Anwendungshinweise und Interpretationen zum Schema, AIS36: Kompositionsevaluierung, Version 4, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik.*

[46] *BSI-CC-PP-0056-V2-2012, Common Criteria Protection Profile / Machine ReadableTravelDocumentwith 'ICAOApplication', Extended Access Control with PACE, BSI, Version 1.3.2, 2012-12-05..*

[47] *Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009.*

[48] *ISO/IEC 11770-3: Information technology — Security techniques — Key management -- Part 3: Mechanisms using asymmetric techniques, 2008.*

[49] *BSI, Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik.*

[50] *Common Criteria Public Security Target, IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h Revision: 1.6, 2019-06-05.*

[51] *NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, December 2001.*

[52] *FIPS 197, Advanced Encryption Standard (AES), NIST 2001.*

[53] *ISO/IEC. ISO/IEC 18033-3:2010 – Information technology – Security techniques – Encryption Algorithms – Part 3: Block ciphers. 2010..*

[54] *ISO/IEC 10116:2006 – Information technology – Security techniques – Modes of operation for an n-bit block cipher. 2006..*

[55] *ISO/IEC, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 2011.*

[56] *REGULATION (EC) No 444/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 28 May 2009..*

[57] *REGULATION (EU) 2017/1954 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, amending Council Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, 25 October 2017..*

[58] *ISO/IEC 14443-4:2018, Cards and security devices for personal identification - Contactless proximity objects - Part 4: Transmission protocol.*

[59] *ISO/IEC 18013-1:2018 Information technology — Personal identification — ISO-compliant driving licence — Part 1: Physical characteristics and basic data set.*

[60] *ISO/IEC TR 19446:2015 Differences between the driving licences based on the ISO/IEC 18013 series and the European Union specifications.*

[61] *COMMISSION REGULATION (EU) No 383/2012 aying down technical requirements with regard to driving licences which include a storage medium, of 4 May 2012.*

[62] *Anwendungsschnittstelle für sichere Elemente zur elektronischen Identifikation, Authentisierung und für vertrauenswürdige Dienste.*

[63] *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; https://eur-lex.europa.eu/lega.*

[intentionally blank]