Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD)

Security Target

BSI-DSZ-CC-1032

Common Criteria / ISO 15408

EAL 5+

Document Version 1.9 • 2018-12-07

cv cryptovision GmbH • Munscheidstr. 14 • 45886 Gelsenkirchen • Germany
www.cryptovision.com • info@cryptovision.com • +49-209-167-2450

Content

Version Control

Version	Date	Author	Changes to Previous Version
1.9	2018-12-07	Thomas Zeggel	Release version.

1 Introduction

1.1 ST/TOE Identification

Title:	Veridos Suite v3.0 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key Generation (SSCD) – Security Target
Document Version:	v1.9
Origin:	cv cryptovision GmbH
Compliant to:	Protection profiles for secure signature creation device – Part 2: Device with key generation; English version EN 419211-2:2013, English translation of DIN EN 419211-2:2013-12; PP Registration: BSI-CC-PP-0059-2009-MA-02; December 2013 [PP0059]
Product identification:	Veridos Suite v3.0 - cryptovision ePasslet Suite
TOE identification:	Veridos Suite v3.0 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD)
Short TOE name:	ePasslet3.0/SSCD
Javacard OS platform:	SmartCafe Expert 7.0 C3 [ZertSmartCafe], BSI-DSZ-CC-1028-2017-MA-01
Security controller:	IFX M5073 G11 [ZertIC], BSI-DSZ-CC-0951-2015-RA-01
TOE documentation:	Administration and user guide [Guidance_PRE], [Guidance_OPE], [Guidance_GEN]

1.2 ST overview

This document contains the security target for SSCD compliant configuration of the Veridos Suite v3.0 – cryptovision ePasslet Suite. Veridos Suite v3.0 – cryptovision ePasslet Suite is a set of Javacard applications intended to be used exclusively on the SmartCafe Expert 7.0 C3 Javacard OS platforms, which is certified according to CC EAL 5+ [ZertSmartCafe]. Veridos Suite v3.0 – cryptovision ePasslet Suite as well as the SmartCafe Expert 7.0 C3 operating system are provided on a smart card chip based on the Infineon M5073 G11 security controller, which is itself certified according to CC EAL 5+ [ZertIC].

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

The main objectives of this ST are:

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

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

1.3 TOE overview

1.3.1 Overview of Veridos Suite v3.0 – cryptovision ePasslet Suite

Veridos Suite v3.0 – cryptovision ePasslet Suite is a set of Java Card applets for e-ID document applications built upon an underlying core library. The following *Table 1* provides an overview of the individual applications included in Veridos Suite v3.0 – cryptovision ePasslet Suite:

Product / Application	Specification	Configuration
ICAO MRTD application with Basic Access Contro (BAC) and Supplemental Access Control (SAC)	ICAO Doc 9303	ePasslet3.0/MRTD-BAC
ISO File System application	ISO 7816	ePasslet3.0/ISO-FS
ISO Driving License application with Basic Access Protection (BAP) or Supplemental Access Control (SAC)	ISO 18013	ePasslet3.0/IDL-Basic
ISO Driving License application with Extended Access Protection (EAP) or Extended Access Control (EACv1)	ISO 18013	ePasslet3.0/IDL-Extended
ICAO MRTD application with Extended Access Control (EACv1)	ICAO Doc 9303, TR03110v1.11	ePasslet3.0/MRTD-EAC
Secure Signature Creation Device application supporting PKI utilization	ISO 7816, PKCS#15	ePasslet3.0/SSCD
EU Electronic Vehicle Registration application	EU Council Directive 1999/37/EC	ePasslet3.0/eVR
EU Electronic Health Insurance application	CWA 15974	ePasslet3.0/eHIC
German eID Document application	ICAO Doc 9303, TR03110v2.11, TR03127 v1.15	ePasslet3.0/GeID
Customizable eID Document application	ICAO Doc 09303 and TR03110v2.11	ePasslet3.0/GenID
EU Electronic Residence Permit application	TR03127 v1.15	ePasslet3.0/eRP

Table 1: Configurations of the Veridos Suite v3.0 – cryptovision ePasslet Suite. Please note that not all configurations are certified according to Common Criteria. ***The TOE of this ST is marked in yellow.***

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

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

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

1.3.2 TOE definition

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

- the circuitry of the chip (the integrated circuit, IC) including the contact-based interface with hardware for the contactless interface including contacts for the antenna, providing basic cryptographic functionalities,
- the platform with the Java Card operation system SmartCafe Expert 7.0 C3 by Giesecke&Devrient in the configuration 1 (compliant to the GlobalPlatform Card Common Implementation Configuration [GP_CIC], verifiable according to platform guidance [AGD_PRE], chapter 8),
- Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing a secure signature creation device (SSCD)[1]
- the associated Administrator and User Guidance [Guidance_PRE], [Guidance_OPE], [Guidance_GEN].

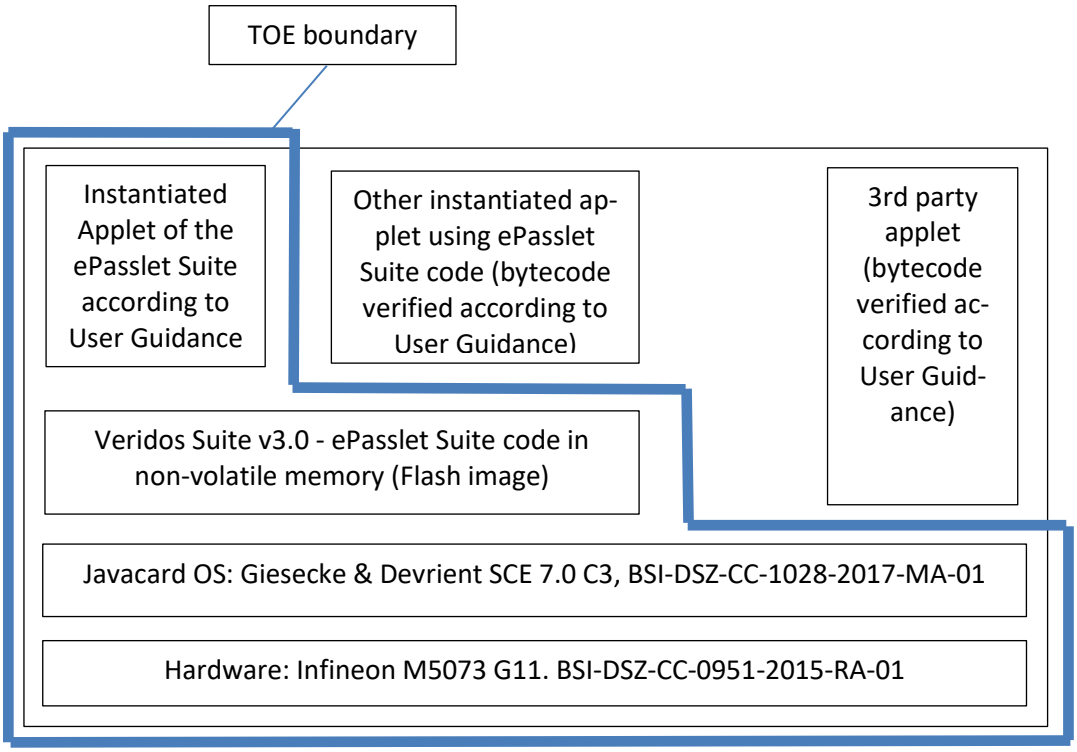


Figure 1: Schematic view on the Target of Evaluation (TOE) and its boundaries. The TOE is based on the certified hardware and Javacard OS. Besides the Veridos Suite v3.0 - ePasslet Suite code in non-volatile memory and the applet instantiated from it which forms the TOE of this security target, it may also contain additional applets which are not part of the TOE.

The TOE's functionality claimed by this security target is realized by the Veridos Suite v3.0 – cryptovision ePasslet Suite in SSCD configuration. The SSCD configuration provides a PKCS#15 compliant file structure

[1] Please note that there are two different options: a configuration for the contact-based interface, or a configuration for the contactless interface with additional PACE mechanism.

and a separate DF for the SSCD functionality (D.Sig). While D.Sig provides the TOE's functionality claimed by this security target, the PKCS#15 part is out of scope of the certification.

1.3.2.1 TOE identification

Identification of the TOE is performed by several GET DATA and GET STATUS commands according to [AGD_PRE] chapter 8.

Step 1	Send GET DATA to the card
	`80 CA 00 C8 06`
	and verify that the card returns
	`C8 04 8D 89 E8 6F`

Step 2	Send GET STATUS to the card
	`80 F2 80 00 02 4F 00`
	and verify that the card returns
	`08 A0 00 00 00 03 00 00 00 0F 9E`

Step 3	Send GET DATA (CPLC) to the card
	`80 CA 9F 7F 00`
	and verify that the card response begins with
	`9F 7F 2A 00 05 00 79 D0 01 xx xx 01 03`

The "xx xx" in step 3 denote the production image release date and may vary. Once the platform is identified correctly, the version of ePasslet Suite can be verified as descibed in [Guidance_PRE].

Note that two software versions with different internal version numbers exist that fall under this certification; details regarding the identification of the two versions are described in [Guidance_PRE].

1.3.3 TOE functions

The SSCD protects the SCD during its whole life cycle as to be used in a signature-creation process solely by its signatory. The TOE provides the following functions:

- to generate signature-creation data (SCD) and the correspondent signature-verification data (SVD),
- to export the SVD for certification,
- to, optionally, receive and store certificate info,
- to switch the TOE from a non-operational state to an operational state, and
- if in an operational state, to create electronic signatures for data with the following steps:
  a) select an SCD if multiple are present in the SSCD,
  b) receive data to be signed or a unique representation thereof (DTBS/R)
  c) authenticate the signatory and determine its intent to sign,
  d) apply an appropriate cryptographic signature-creation function using the selected SCD to the DTBS/R.

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

The TOE is prepared for the signatory's use by

- generating at least one SCD/SVD pair, and
- personalising for the signatory by storing in the TOE:
  a) the signatory's reference authentication data (RAD)
  b) optionally, certificate info for at least one SCD in the TOE.

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

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

If continued use of an SCD is no longer required the TOE will disable an SCD it holds, e.g. by erasing it from memory.

1.3.4 Operation of the TOE

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

- The preparation environment, where it interacts with a certification service provider through a certificate-generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with signature creation data (SCD) the TOE has generated. The initialization environment interacts further with the TOE to personalize it with the initial value of the reference-authentication data (RAD).
- The signing environment where it interacts with a signer through a signature-creation application (SCA) to sign data after authenticating the signer as its signatory. The signature-creation application provides the data to be signed, or a unique representation thereof (DTBS/R) as input to the TOE signature-creation function and obtains the resulting electronic signature.
- 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 shall provide 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 of the SCD and restricts its use in signature creation to its signatory. The electronic signature created with the TOE is a qualified electronic signature as defined in [Directive][2] if the certificate for the SVD is a qualified certificate ([Directive], Annex I)[3]. Determining the state of the certificate as qualified in beyond the scope of this standard.

[2] References to articles and paragraphs in [Directive] follow the style used in the according protection profile [PP0059]: "([Directive]: n.m)". References to one of the Annexes of [Directive] name the Annex explicitly.

[3] Please note that while this security target - following the according protection profile BSI-CC-PP-0059-2009-MA-02 - references the [Directive], it also incorporates the requirements of the eIDAS regulation [Regulation] and the according commission implementing regulation [Implementing].

The signature creation application shall protect the integrity of the input it provides to the TOE signature-creation function as being consistent with the user data authorized for signing by the signatory. Unless implicitly known to the TOE, the SCA indicates the kind of the signing input (as DTBS/R) it provides and computes any hash values required. The TOE may augment the DTBS/R with signature parameters it stores and then computes a hash-value over the input as needed by the kind of input and the used cryptographic algorithm.

The TOE stores signatory reference authentication data (RAD) 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 may provide a user interface to directly receive verification authentication data (VAD) from the user, alternatively, the TOE receive the VAD from the signature- creation application. If the signature-creation application handles, is requesting or obtaining a VAD from the user, it shallis assumed to protect the confidentiality and integrity of this data.

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

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

In the case at hand the TOE is a smart card or electronic ID document. In this case a smart-card terminal may be deployed that provides the required secure environment to handle a request for signatory authorization. A signature can be obtained on a document prepared by a signature-creation application component running on personal computer connected to the card terminal. The signature creation application, after presenting the document to the user and after obtaining the authorization PIN initiates the electronic signature creation function of the smart card through the terminal.

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

1.3.5 Major security features of the TOE

The TOE provides the following TOE security functionalities:

- TSF_Access manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data[4].
- TSF_Admin manages the storage of manufacturing data, pre-personalization data and personalization data.
- TSF_Secret ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These mechanisms are mainly provided by TSF_OS.
- TSF_Crypto performs high level cryptographic operations. The implementation is mainly based on the Security Functionalities provided by TSF_OS.

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

- TSF_SecureMessaging realizes a secure communication channel.
- TSF_Auth realizes two authentication mechanisms: PIN verification and alternatively authentication with the PACE protocol.
- TSF_Integrity protects the integrity of internal applet data like the Access control lists.
- TSF_OS contains all security functionalities provided by the certified platform (IC, Javacard operation system). The cryptographic operations needed for this TOE are provided by the platform:
    - Electronic signature-generation (and key generation) with RSA and key sizes of 2048 up to 4096 bit with CRT and 2048 bit without CRT, or ECDSA with key sizes of 160, 192, 224, 256, 320, 384, 512, 521 bit.
    - Secure messaging with AES (128, 192 or 256 bit key length).
    - PACE authentication with key lengths of 160, 192, 224, 256, 320, 384, 512, 521 bit (ECC); the implementation utilizes platform SFR FCS_CKM.1/ECC.

1.3.6 TOE life cycle

This paragraph is based on the protection profile [PP0059].

1.3.6.1 General

The TOE life cycle distinguishes stages for development, production, preparation and operational use. The development and production of the TOE (cf. CC part 1 [CC_1], para.139) together constitute the development phase of the TOE.

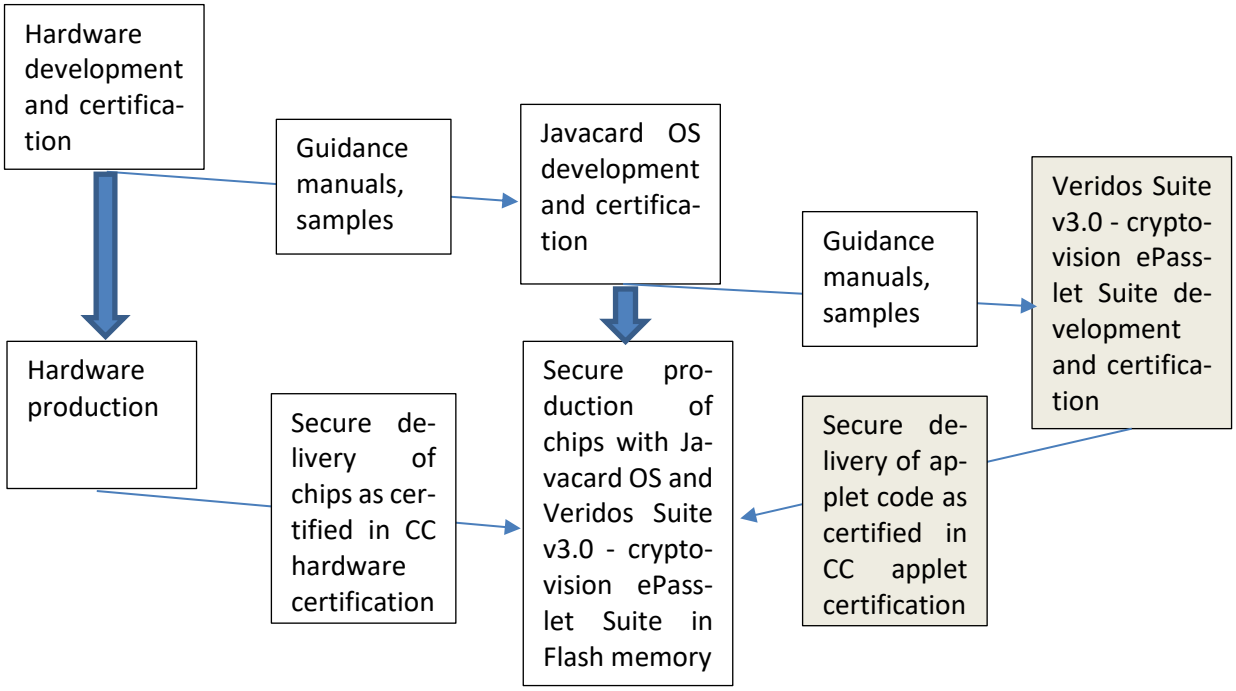


Figure 2: Overview of the development phase of the TOE, which contains development and production of the TOE. After the secure production following the process certified for the Javacard OS, the chips are delivered to the SSCD provisioning service using the delivery process already established for the OS. Gray boxes indicate the steps which are subject to evaluation according to the assurance life cycle (ALC) class.

The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class.

The development phase ends with the delivery of the TOE to an SSCD-provisioning service provider or a card manufacturer (see footnote 4). This is also the end of the scope of the certification according to Common Criteria.

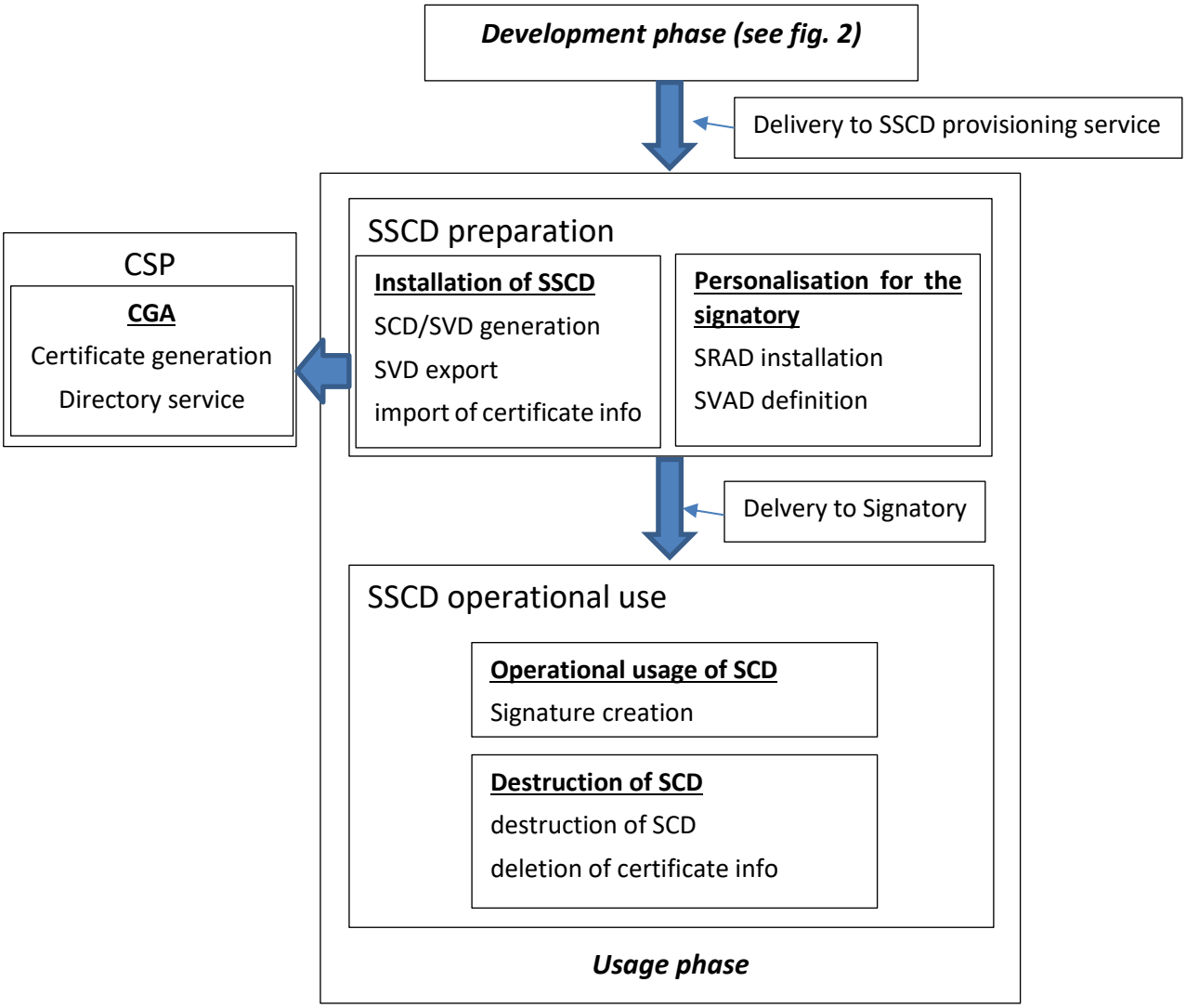


Figure 3: Example of TOE lifecycle following figure 1 of [PP0059]. Note that import of certificate info during TOE preparation and export of certificate info when SCD is destroyed are optional. The delivery to the SSCD provisioning service after the development phase is also the end of the scope of the certification according to Common Criteria.

The operational usage of the TOE comprises the preparation stage and the operational use stage. The TOE operational use stage begins when the signatory performs the TOE operation to enable it for use in signing operations. Enabling the TOE for signing requires at least one keyset of SCD stored in its memory.

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

1.3.6.2 Preparation stage

An SSCD-provisioning service provider having accepted the TOE from a manufacturer prepares the TOE for use and delivers it to its legitimate user. The preparation phase ends when the legitimate user of the TOE, having received it from an 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:

- Create and configure the signature application according to AGD_PRE; this step involves applet instanciation as well as creation of the file system (card profile).[5]
- 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.
- Generate a PIN and/or obtain a biometric sample of the legitimate user, store this data as RAD in the TOE and prepare information about the VAD for delivery to the legitimate user.
- Generate a certificate for at least one SCD either by:
  a) The TOE generating an SCD/SVD pair and obtaining a certificate for the SVD exported from the TOE, or
  b) Initializing security functions in the TOE for protected export of the SVD and obtaining a certificate for the SVD after receiving a protected request from the TOE,
- Optionally, present certificate info to the SSCD.
- Deliver the TOE and the accompanying VAD info to the legitimate user.

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

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

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

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

Before initiating the actual certificate signature the certificate-generating application verifies the SVD received from the TOE by:

- establishing the sender as genuine SSCD

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

- establishing the integrity of the SVD to be certified as sent by the originating SSCD,
- establishing that the originating SSCD has been personalized for the legitimate user,
- establishing correspondence between SCD and SVD, and
- an assertion that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

The proof of correspondence between an SCD stored in the TOE and an SVD may be implicit in the security mechanisms applied by the CGA. Optionally, the TOE may support a function to provide an explicit proof of correspondence between an SCD it stores and an SVD realized by self-certification. Such a function may be performed implicitly in the SVD export function and may be invoked in the preparation environment without explicit consent of the signatory. Security requirements to protect the SVD export function and the certification data if the SVD is generated by the signatory and then exported from the SSCD to the CGA are specified in a separate PP (see section 5.3).

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

1.3.6.3 Operational use stage

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

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

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

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

The TOE may support functions to generate additional signing keys. If the TOE supports these functions it will support further functions to securely obtain certificates for the new keys. For an additional key the signatory may be allowed to choose the kind of certificate (qualified, or not) to obtain for the SVD of the new key. The signatory may also be allowed to choose some of the data in the certificate request for instance to use a pseudonym instead of the legal name in the certificate7. If the conditions to obtain a qualified certificate are met the new key can also be used to create advanced electronic signatures. The optional TOE functions for additional key generation and certification may require additional security functions in the TOE and an interaction with the SSCD-Provisioning service provider in an environment that is secure.

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

2 Conformance claims

2.1 CC conformance

This security target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012; CCMB-2012-09-001, [CC_1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 4, September 2012; CCMB-2012-09-002, [CC_2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, September 2012; CCMB-2012-09-003, [CC_3],

as follows:

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

This security target is strictly conformant to the protection profile [PP0059]. To cover the additional PACE functionality the following SFR have been added:

- FCS_COP.1/PACE
- FCS_RND.1

The evaluation of the TOE uses the result of the CC evaluation of the Infineon M5073 G11 chip claiming conformance to the PP [PP0084]. The hardware part of the composite evaluation is covered by the certification report [ZertIC]. In addition, the evaluation of the TOE uses the result of the CC evaluation of the SmartCafe Expert 7.0 C3 Javacard OS. The Javacard OS as part of the composite evaluation is covered by the certification report [ZertSmartCafe].

2.2 Statement of Compatibility concerning Composite Security Target

2.2.1 Assessment of the Platform TSFs

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

Platform TSF-group	Correspondence in this ST	References/Remarks
SF.TRANSACTION	No correspondence, internal Java card mechanisms.	This security function provides atomic transactions according to the Java Card Transaction and Atomicity mechanism with commit and roll-back capability for updating persistent data in flash memory.
SF.ACCESS_CONTROL	No correspondence, internal Java card mechanisms.	This security function provides control for the TOE. It is in charge of the FIREWALL access control SFP and the JCVM information flow control SFP. It enforces applet isolation located in different packages and controls the access to global data containers shared by all applet instances.
SF.CRYPTO	TSF_Crypto	This security function controls all the operations related to the cryptographic key management and cryptographic operations.
SF.INTEGRITY	TSF_Integrity, TSF_Secret	This security function provides a means to check the integrity of checksummed data stored in flash memory.
SF.SECURITY	TSF_Secret	This security function ensures a secure state of information, the non-observability of operations on it and the unavailability of previous information content upon deallocation.
SF.APPLET	No correspondence, internal Java card mechanisms.	This security function ensures the secure loading of a package or installing of an applet and the secure deletion of applets and/or packages.
SF.CARRIER	TSF_Crypto (regarding Secure Messaging)	This security function ensures secure downloading of applications on the card.

Table 2: Relevant platform TSF-groups and their correspondence

2.2.2 Assessment of the Platform SFRs

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

Platform SFR	Correspondence in this ST	References/Remarks
CoreG_LC Security Functional Requirements (chapter 8.1.1 in platform ST)		
Firewall Policy (chapter 8.1.1.1 in platform ST)		
FDP_ACC.2/FIREWALL	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for

Platform SFR	Correspondence in this ST	References/Remarks
		applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FDP_ACF.1/FIREWALL	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FDP_IFC.1/JCVM	No correspondence	Out of scope (internal Java Virtual Machine). No contradiction to this ST.
FDP_IFF.1/JCVM	No correspondence	Out of scope (internal Java Virtual Machine). No contradiction to this ST.
FDP_RIP.1/OBJECTS	No correspondence.	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_MSA.1/JCRE	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_MSA.1/JCVM	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_MSA.2/FIREWALL-JCVM	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FMT_MSA.3/FIREWALL	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FMT_MSA.3/JCVM	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_SMF.1	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_SMR.1	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
Application Programming Interface (chapter 8.1.1.2 in platform ST)		
FCS_CKM.1 (FCS_CKM.1.1/RSA, FCS_CKM.1.1/ECC, FCS_CKM.1.1/3DES, FCS_CKM.1.1/AES)	FCS_CKM.1	The requirement in this ST is equivalent to parts of the platform ST.
FCS_CKM.2	No correspondence	Out of scope (managed within Java Card OS). No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
FCS_CKM.3	No correspondence	Out of scope (managed within Java Card OS). No contradiction to this ST.
FCS_CKM.4	FCS_CKM.4	The requirements are compatible (physically overwriting the keys, physically overwriting the keys with zeros).
FCS_COP.1 (FCS_COP.1.1/RSA-CRT-SIGN, FCS_COP.1.1/RSA-SIGN, FCS_COP.1.1/RSA-VERI, FCS_COP.1.1/MAC-DES FCS_COP.1.1/MAC-AES, FCS_COP.1.1/CMAC-AES, FCS_COP.1.1/3DES, FCS_COP.1.1/AES, FCS_COP.1.1/RSA-DEC, FCS_COP.1.1/RSA-CRT-DEC, FCS_COP.1.1/RSA-ENC, FCS_COP.1.1/ECDSA-SIGN, FCS_COP.1.1/ECDSA-VERI, FCS_COP.1.1/HASH)	FCS_COP.1/SIG FCS_COP.1/PACE	The requirement FCS_COP.1/SIG of this ST targets electronic signature generation and is fulfilled by the platform SFR targeting RSA signature generation (FCS_COP.1/ECDSA-SIGN, FCS_COP.1/RSA-SIGN, FCS_COP.1.1/RSA-CRT-SIGN). FCS_COP.1/PACE uses the platform functionality required by FCS_COP.1/AES. The according hash functions of FCS_COP.1/SIG of this ST are provided by FCS_COP.1.1/HASH. No contradictions to this ST.
FCS_RNG.1	FCS_RND.1	In this ST, random numbers according to AIS20 class DRG.4 are required. The platform generates random numbers with a defined quality metric (DRG.4) that can be used directly.
FDP_RIP.1/ABORT	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/APDU	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/bArray	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/KEYS	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/TRANSIENT	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ROL.1/FIREWALL	No correspondence.	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
Card Security Management (chapter 8.1.1.3 in platform ST)		
FAU_ARP.1	FPT_FLS.1, FPT_PHP.3	Not directly corresponding, but platform SFR is basis of fulfillment of FPT_FLS.1 and FPT_PHP.3. Internal

Platform SFR	Correspondence in this ST	References/Remarks
		counter for security violations complement Java Card OS mechanisms- No contradiction to this ST.
FDP_SDI.2	FPT_FLS.1, FPT_PHP.3	Not directly corresponding, but platform SFR is basis of fulfillment of FPT_FLS.1 and FPT_PHP.3. No contradiction to this ST.
FPR_UNO.1	FPT_EMS.1	Not directly corresponding, but relevant for the fullfillment of FPT_EMS.1. No contradiction to this ST.
FPT_FLS.1	FPT_FLS.1	The fulfillment of the platform SFR is part of the basis of the fulfillment of the SFR of this ST. Internal countermeasures for detecting security violations complement Java Card OS mechanisms. No contradiction to this ST.
FPT_TDC.1	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_TST.1	FPT_TST.1	Self-testing is provided by the Java Card platform during initial start-up.
Aid Management (chapter 8.1.1.4 in platform ST)		
FIA_ATD.1/AID	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_UID.2/AID	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_USB.1/AID	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MTD.1/JCRE	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MTD.3/JCRE	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
INSTG Security Functional Requirements (chapter 8.1.2 in platform ST) This group consists of the SFRs related to the installation of the applets, which addresses security aspects outside the runtime.		
FDP_ITC.2/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMR.1/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_RCV.3/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
ADELG Security Functional Requirements (chapter 8.1.3 in platform ST) This group consists of the SFRs related to the deletion of applets and/or packages, enforcing the applet deletion manager (ADEL) policy on security aspects outside the runtime.		
FDP_ACC.2/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ACF.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.3/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMF.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMR.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
ODELG Security Functional Requirements (chapter 8.1.4 in platform ST) The following requirements concern the object deletion mechanism. This mechanism is triggered by the applet that owns the deleted objects by invoking a specific API method.		
FDP_RIP.1/ODEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/ODEL	FPT_FLS.1	The fulfillment of the platform SFR is part of the basis of the fulfillment of the SFR of this ST. Internal countermeasures for detecting security violations complement Java Card OS mechanisms. No contradiction to this ST.
CARG Security Functional Requirements (chapter 8.1.5 in platform ST) This group includes requirements for preventing the installation of packages that has not been bytecode verified, or that has been modified after bytecode verification.		
FCO_NRO.2/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_IFC.2/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_IFF.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_UIT.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
FIA_UID.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.3/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMF.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMR.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FTP_ITC.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
CMGR Security Functional Requirements (chapter 8.1.6 in platform ST) In the PP of the Java Card certification [PP_Javacard], objectives for Card Management were objectives for the environment. Since the card manager has been defined to be part of the TOE, they were transformed into objectives for the TOE and are covered by SFRs in the platform ST.		
FTP_ITC.1/CMGR	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
SCPG Security Functional Requirements (chapter 8.1.7 in platform ST) In the PP of the Java Card certification [PP_Javacard], objectives for the smart card platform are objectives for the environment. Since the smart card platform has been defined to be part of the TOE, they were transformed into objectives for the TOE and are covered by SFRs in the platform ST.		
FPT_PHP.3	FPT_PHP.3 FPT_EMS.1	The fulfillment of the SFR in this ST is based on the platform SFR (together with additional countermeasures).

Table 3: Assessment of the platform SFRs.

2.2.3 Assessment of the Platform Objectives

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

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

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

Table 4: Assessment of the platform objectives.

2.2.4 Assessment of Platform Threats

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

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

Table 5: Threats of the platform ST.

2.2.5 Assessment of Platform Organisational Security Policies

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

2.2.6 Assessment of Platform Operational Environment

2.2.6.1 Assessment of Platform Assumptions

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

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

Table 6: Assumptions of the Platform ST.

2.2.6.2 Assessment of Platform Objectives for the Operational Environment

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

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

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

3 Security problem definition

This chapter has been taken from [PP0059] with minor modifications.

3.1 Assets, users and threat agents

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

Assets and objects:

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

User and subjects acting for users:

1. User: End user of the TOE who can be identified as Administrator or Signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.
2. Administrator: User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as Administrator.
3. Signatory: User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.

Threat agents:

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

3.2 Threats

3.2.1 T.SCD_Divulg: Storing, copying, and releasing of the signature-creation data

An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature-creation in the TOE.

3.2.2 T.SCD_Derive: Derive the signature-creation data

An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

3.2.3 T.Hack_Phys: Physical attacks through the TOE interfaces

An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

3.2.4 T.SVD_Forgery: Forgery of the signature-verification data

An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

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

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

3.2.6 T.DTBS_Forgery: Forgery of the DTBS/R

An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign.

3.2.7 T.Sig_Forgery: Forgery of the electronic signature

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

3.3 Organisational Security Policies

3.3.1 P.CSP_QCert: Qualified certificate

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate ([Directive]: 2:9, Annex I) for the SVD 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.

3.3.2 P.QSign: Qualified electronic signatures

The signatory uses a signature-creation system to sign data with an advanced electronic signature ([Directive]: 1, 2), which is a qualified electronic signature if it is based on a valid qualified certificate ([Directive], Annex I). The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

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

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

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

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

3.4 Assumptions

3.4.1 A.CGA: Trustworthy certificate-generation application

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

3.4.2 A.SCA: Trustworthy signature-creation application

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data the signatory wishes to sign in a form appropriate for signing by the TOE.

4 Security Objectives

4.1 General

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

4.2 Security Objectives for the TOE

4.2.1 OT.Lifecycle_Security: Lifecycle security

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

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

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.2.5 OT.SCD_Secrecy: Secrecy of the signature-creation data

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

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

4.2.6 OT.Sig_Secure: Cryptographic security of the electronic signature

The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

4.2.7 OT.Sigy_SigF: Signature creation function for the legitimate signatory only

The TOE shall provide the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

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

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

4.2.9 OT.EMSEC_Design: Provide physical-emanation security

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

4.2.10 OT.Tamper_ID: Tamper detection

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

4.2.11 OT.Tamper_Resistance: Tamper resistance

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

4.3 Security Objectives for the Operational Environment

4.3.1 OE.SVD_Auth: Authenticity of the SVD

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

4.3.2 OE.CGA_QCert: Generation of qualified certificates

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

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

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

4.3.3 OE.SSCD_Prov_Service: Authentic SSCD provided by SSCD Provisioning Service

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

4.3.4 OE.HID_VAD: Protection of the VAD

If an external device provides the human interface for user authentication, this device shall ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface. In particular, if the TOE requires a trusted channel for import of the VAD, the HID shall support usage of this trusted channel.

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

The Signatory shall use a trustworthy SCA that

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

Application note 3: The SCA should be able to support advanced electronic signatures. Currently, there exist three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CAdES, XAdES and PAdES. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.

4.3.6 OE.DTBS_Protect: SCA protects the data intended to be signed

The operational environment shall ensure that the DTBS/R cannot be altered in transit between the SCA and the TOE. In particular, if the TOE requires a trusted channel for import of the DTBS/R, the SCA shall support usage of this trusted channel.

4.3.7 OE.Signatory: Security obligation of the Signatory

The signatory shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The signatory shall keep their VAD confidential.

4.4 Security Objectives Rationale

4.4.1 Security Objectives Coverage

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

	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	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory
T.SCD_Divulg					x													

	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	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory
T.SCD_Derive		x				x												
T.Hack_Phys					x				x	x	x							
T.SVD_Forgery				x									x					
T.SigF_Misuse	x						x	x							x	x	x	x
T.DTBS_Forgery								x								x	x	
T.Sig_Forgery			x			x						x						
P.CSP_QCert	x			x								x						
P.QSign						x	x					x				x		
P.Sigy_SSCD	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
A.CGA												x	x					
A.SCA																x		

Table 8: Mapping of threats, policies and assumptions to the security objectives.

4.4.2 Security Objectives Sufficiency

Countering of threats by security objectives:

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

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

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

T.SVD_Forgery (*Forgery of the signature verification data***)** deals with the forgery of the SVD exported by the TOE to the CGA for certificate generation. T.SVD_Forgery is addressed by OT.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to 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

on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of [Directive], Annex III. OT.Lifecycle_Security (*Lifecycle security*) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. OT.Sigy_SigF (*Signature creation function for the legitimate signatory only*) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (*Data intended to be signed*) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. OT.DTBS_Integrity_TOE (*DTBS/R integrity inside the TOE*) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, OE.HID_VAD (*Protection of the VAD*) provides confidentiality and integrity of the VAD as needed by the authentication method employed. OE.Signatory 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 sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of OE.DTBS_Protect, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R inside the TOE.

T.Sig_Forgery (*Forgery of the electronic signature***)** deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique and OE.CGA_QCert address this threat in general. OT.Sig_Secure (*Cryptographic security of the electronic signature*) ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. OT.SCD_Unique and 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,
- OT.SCD_SVD_Corresp, which requires 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.

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 [Directive], Annex III. This is ensured as follows:

- OT.SCD_Unique meets the paragraph 1(a) of [Directive], Annex III, by the requirements that the SCD used for signature creation can practically occur only once;
- OT.SCD_Unique, OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(a) of [Directive], Annex III by the requirements to ensure secrecy of the SCD. OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of the SCD against specific attacks;
- OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE;
- OT.Sigy_SigF meets the requirement in paragraph 1(c) of [Directive], 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 [Directive], Annex III as the TOE must not alter the DTBS/R.

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

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

- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialisation, personalisation and operational usage,
- OT.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only, and
- 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 SSCD from an SSCD-provisioning service.

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

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

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

OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD-provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory ensures that the signatory keeps their VAD confidential. OE.DTBS_Intend, OE.DTBS_Protect and OT.DTBS_Integrity_TOE ensure that the TOE 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), which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

5 Extended Component Definition

5.1 Definition of the Family FPT_EMS

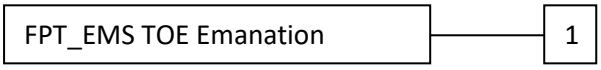
The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation. The definition of the family FPT_EMS is taken from the Protection Profile Secure Signature Creation Device [PP0006].

5.1.1 FPT_EMS TOE Emanation

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMS.1 TOE Emanation has two constituents:

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

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

FPT_EMS.1: TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1

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

FPT_EMS.1.2

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

5.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional FCS_RND is not limited to generation of cryptographic keys unlike the component FCS_CKM.1.

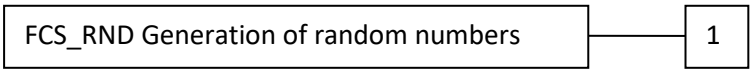
The family “Generation of random numbers (FCS_RND)” is specified as follows.

5.2.1 FCS_RND Generation of random numbers

Family behavior

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

Component leveling:



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

6 IT Security Requirements

6.1 General

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

Section 6.2 provides the security functional requirements. Operations for assignment, selection and refinement that are added to the content of the according protection profile [PP0059] are marked with bold characters.

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

6.2 TOE Security Functional Requirements

6.2.1 Use of requirement specifications

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

Operations already performed in the underlying PP [PP0059] are uniformly marked by ***bold italic*** font style; for further information on details of the operation, please refer to [PP0059].

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

6.2.2 Cryptographic support (FCS)

Application note 4: Member states of the European Union have specified entities as responsible for accreditation and supervision of the evaluation process for products conforming to this standard and for determining admissible algorithms and algorithm parameters ([Directive]: 1.1b and 3.4).

6.2.2.1 FCS_CKM.1: Cryptographic key generation

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

FCS_CKM.1.1

The TSF shall generate an **SCD/SVD** pair in accordance with a specified cryptographic key generation algorithm:

- **RSA CRT key generation; or ECDSA key generation**[6]

and specified cryptographic key sizes:

- **between 2048 and 4096 bit with CRT, or 2048 bit without CRT; or with 160, 192, 224, 256, 320, 384, 512 or 521 bit corresponding to the used elliptic curves secp{160, 192, 224, 256, 320, 384, 521}r1,**

[6] [assignment: cryptographic key generation algorithm]

brainpoolP{160, 192, 224, 256, 320, 384, 512}r1 and brainpoolP{160, 192, 224, 256, 320, 384, 512} t1 [78]

that meet the following:

- **PKCS#1v2.1 [PKCS1]; or [TR03111] and secp curves according to [FIPS186-3] chapter B.4.1 and D.1.2. and brainpool curves according to [RFC5639] chapter 3.**[9]

PP application note 5: <applied>

6.2.2.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: **overwriting the key values**[10] that meets the following: **none**[11]**.**

PP application note 6: <applied>

6.2.2.3 FCS_COP.1/SIG: Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1/SIG

The TSF shall perform ***digital signature creation*** in accordance with a specified cryptographic algorithm

- **RSA (straight and CRT variant) without internal hash calculation, with SHA-224, SHA-256, SHA-384 or SHA-512; or ECDSA without internal hash calculation, with SHA-224, SHA-256, SHA-384 or SHA-512**[12]

and specified cryptographic key sizes:

[7] [assignment: cryptographic key sizes]

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

[9] [assignment: list of standards]

[10] [assignment: cryptographic key destruction method]

[11] [assignment: list of standards]

[12] [assignment: cryptographic algorithm]

- **2048 bit (without CRT) or 2048, 2304, 2560, 2816, 3072, 3328, 3584, 3840, 4096 bit (with CRT) with the exception of the following specific combinations: 3072 bit and SHA-384, 3328 bit and SHA-512, 3584 bit and SHA-512; or corresponding to the used elliptic curves secp{160, 192, 224, 256, 320, 384, 521}r1 [SEC2], brainpoolP{160, 192, 224, 256, 320, 384, 512}r1 and brainpoolP{160, 192, 224, 256, 320, 384, 512}t1 [RFC5639]** [13]

that meet the following:

- **standard PKCS#1v2.1 [PKCS1] (RSASSA-PKCS1-v15 and RSASSA-PSS) chapter 8, and [FIPS180-4]; or standard [TR03111] (ECDSA), chapter 4.2.1, and [FIPS180-4], together with elliptic curves secp{160, 192, 224, 256, 320, 384, 521}r1, brainpoolP{160, 192, 224, 256, 320, 384, 512}r1 and brainpoolP{160, 192, 224, 256, 320, 384, 512} t1** [14][15]

PP application note 7: <applied>

Developer note: The TOE functionally supports PSS signatures with bit lengths of 512 - 2048 bit in steps of 16 bit without and 512 – 4096 bit in steps of 16 bit with CRT, and specific combinations with SHA variants. Details are described in [Guidance_PRE]. The certified configuration is limited to bit lengths of 2048, 2304, 2560, 2816, 3072, 3328, 3584, 3840, 4096 bit and any of SHA-224, SHA-256, SHA-384 or SHA-512 with the exception of the following specific combinations: 3072 bit and SHA-384, 3328 bit and SHA-512, 3584 bit and SHA-512.

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

6.2.2.4 FCS_COP.1/PACE: PACE authentication protocol

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

FCS_COP.1.1/PACE

The TSF shall perform ***an authentication protocol*** in accordance with a specified cryptographic algorithm

- **PACE version 2**

and specified cryptographic key sizes:

- **160, 192, 224, 256, 320, 384, 512, 521 bit (ECC); 128, 192, 256 bit (AES)**

that meet the following:

- **BSI-TR-03110 [TR03110].**

[13] [assignment: cryptographic key sizes]

[14] [assignment: list of standards]

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

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

Application note: BSI-TR-03110 [TR03110] allows arbitrary combinations of ECC key sizes and AES key lengths in the PACE protocol. It should be noted that ECC key lengths smaller than the AES key length will lead to a reduced AES key space (e.g. a 160 bit entropy in a 192 or 256 bit AES key).

6.2.2.5 FCS_RND.1: Quality metric for random numbers

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet **the AIS20 Class DRG.4 quality metric**[16]**.**

Application note: This SFR was added to the standard set of SFRs to address the requirements of the PACE protocol. The random number generation is provided by the underlying SmartCafe Expert 7.0 C3 platform.

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

- The internal state of the RNG uses a PTRNG of class PTG.2 as a random source.The RNG provides forward secrecy. The RNG provides enhanced backward secrecy even if the current internal state is known.
- The RNG provides enhanced forward secrecy for every call.
- The internal state of the RNG is seeded by a PTRNG of class PTG.2.
- The RNG generates output for which two strings of bit length 128 are mutually different with probability 1 - 2^-128.
- Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A (as defined in [AIS20]).

Thus the platform RNG implements AIS20 [AIS20] class DRG.4.

6.2.3 User data protection (FDP)

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

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin R.Sigy
S.User	SCD / SVD Management	Authorised, not authorised
SCD	SCD Operational	No, yes
SCD	SCD identifier	Arbitrary value

[16] [assignment: a defined quality metric]

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

Table 9: Security attributes and related status.

PP application note 8: <not applicable>

6.2.3.1 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*** on

(1) subjects: S.User,

(2) objects: SCD, SVD,

(3) operations: generation of SCD/SVD pair.

6.2.3.2 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*** to objects based on the following***: the user S.User is associated with the security attribute "SCD / SVD Management".***

FDP_ACF.1.2/ SCD/SVD_Generation

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

S.User with the security attribute "SCD / SVD Management" set to "authorised" is allowed to generate SCD/SVD pair.

FDP_ACF.1.3/ SCD/SVD_Generation

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***none***.

FDP_ACF.1.4/ SCD/SVD_Generation

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

S.User with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.

6.2.3.3 FDP_ACC.1/SVD_Transfer: Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SVD_Transfer

The TSF shall enforce the ***SVD_Transfer_SFP*** on

(1) subjects: S.User,

(2) objects: SVD

(3) operations: export.

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ SVD_Transfer

The TSF shall enforce ***the SVD_Transfer_SFP*** to objects based on the following:

(1) the S.User is associated with the security attribute Role,

(2) the SVD.

FDP_ACF.1.2/ SVD_Transfer

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **R.Sigy and R.Admin**[17] ***is allowed to export SVD.***

FDP_ACF.1.3/ SVD_Transfer

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***none***.

FDP_ACF.1.4/ SVD_Transfer

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***none***.

PP application note 9: <applied>

This ST does not require the TOE to protect the integrity and authenticity of the exported SVD public key but requires such protection by the operational environment. If the operational environment does not provide sufficient security measures for the CGA to ensure the authenticity of the public key the TOE shall implement additional security functions to support the export of public keys with integrity and data origin authentication. See section 4.3 for additional requirements for use of an SSCD in an environment that cannot provide such protection.

6.2.3.5 FDP_ACC.1/Signature-creation: Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Signature-creation

The TSF shall enforce the ***Signature Creation SFP*** on

(1) subjects: S.User,

(2) objects: DTBS/R, SCD,

(3) operations: signature-creation.

6.2.3.6 FDP_ACF.1/Signature-creation: Security attribute based access control

[17] [selection: R.Admin, R.Sigy]

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Signature-creation

The TSF shall enforce the ***Signature Creation SFP*** to objects based on the following:

(1) the user S.User is associated with the security attribute "Role" and

(2) the SCD with the security attribute "SCD Operational".

FDP_ACF.1.2/Signature-creation

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

R.Sigy is allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes".

FDP_ACF.1.3/Signature-creation

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***none***.

FDP_ACF.1.4/Signature-creation

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no".

6.2.3.7 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***de-allocation of the resource from*** the following objects: ***SCD***.

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

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

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

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

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/ Persistent

The TSF shall monitor user data stored in containers controlled by the TSF for ***integrity error*** on all objects, based on the following attributes: ***integrity checked stored data***.

FDP_SDI.2.2/ Persistent

Upon detection of a data integrity error, the TSF shall

(1) prohibit the use of the altered data

(2) inform the S.Sigy about integrity error.

6.2.3.9 FDP_SDI.2/DTBS. Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/DTBS

The TSF shall monitor user data stored in containers controlled by the TSF for ***integrity error*** on all objects, based on the following attributes: ***integrity checked stored DTBS***.

FDP_SDI.2.2/DTBS

Upon detection of a data integrity error, the TSF shall

(1) prohibit the use of the altered data

(2) inform the S.Sigy about integrity error.

PP application note 10: The integrity of TSF data like RAD shall be protected to ensure the effectiveness of the user authentication. This protection is a specific aspect of the security architecture (cf. ADV_ARC.1).

6.2.4 Identification and authentication (FIA)

6.2.4.1 FIA_UID.1. Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1

The TSF shall allow

(1) Self test according to FPT_TST.1,

(2) Receiving DTBS[18]

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

FIA_UID.1.2

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

PP application note 11: <applied>

6.2.4.2 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1

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

The TSF shall allow

(1) Self test according to FPT_TST.1,

(2) Identification of the user by means of TSF required by FIA_UID.1.

(3) Receiving DTBS[19]

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

FIA_UAU.1.2

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

PP application note 12: <applied>

6.2.4.3 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

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

FIA_AFL.1.2

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

PP application note 13: <applied>

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

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

6.2.5 Security management (FMT)

6.2.5.1 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1

The TSF shall maintain the roles ***R.Admin and R.Sigy.***

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

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

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

6.2.5.2 FMT_SMF.1 Security management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1

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

(1) Creation and modification of RAD,

(2) Enabling the signature-creation function,

(3) Modification of the security attribute SCD/SVD management, SCD operational,

(4) Change the default value of the security attribute SCD Identifier,

(5) none[21]

PP application note 14: <applied>

6.2.5.3 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1

The TSF shall restrict the ability to ***enable*** the functions ***signature-creation function*** to ***R.Sigy***.

6.2.5.4 FMT_MSA.1/Admin Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Admin

The TSF shall enforce the ***SCD/SVD_Generation_SFP*** to restrict the ability to ***modify*** the security attributes ***SCD / SVD management*** to ***R.Admin***.

6.2.5.5 FMT_MSA.1/Signatory Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Signatory

The TSF shall enforce the ***Signature Creation SFP*** to restrict the ability to ***modify*** the security attributes ***SCD operational*** to ***R.Sigy***.

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

6.2.5.6 FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for ***SCD / SVD Management and SCD operational***.

PP application note 15: <applied>

6.2.5.7 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1

The TSF shall enforce ***the SCD/SVD_Generation_SFP, SVD_Transfer_SFP and Signature Creation SFP*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the ***R.Admin*** to specify alternative initial values to override the default values when an object or information is created.

6.2.5.8 FMT_MSA.4 Security attribute value inheritance

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FMT_MSA.4.1

The TSF shall use the following rules to set the value of security attributes:

(1) If S.Admin 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.

PP application note 16: The TOE may not support generating an SVD/SCD pair by the Signatory alone, in which case rule (2) is not relevant.

6.2.5.9 FMT_MTD.1/Admin Management of TSF data

Hierarchical to: No other components.

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

FMT_MTD.1.1/Admin

The TSF shall restrict the ability to ***create*** the ***RAD*** to ***R.Admin***.

6.2.5.10 FMT_MTD.1/Signatory Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/ Signatory

The TSF shall restrict the ability to ***modify*** the ***RAD*** to ***R.Sigy***.

PP application note 17: No other operation besides "modify" was added as assignment in FMT_MTD.1/Signatory Managamenet of TSF data.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1

The TOE shall not emit **variations in power consumption or timing during command execution**[22] in excess of **non-useful information**[23] enabling access to ***RAD*** and ***SCD***.

FPT_EMS.1.2

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

PP application note 18: The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.

Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

6.2.6.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1

[22] [assignment: types of emissions]

[23] [assignment: specified limits]

[24] [assignment: type of users]

[25] [assignment: type of connection]

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

(1) Self-test according to FPT_TST fails,

(2) none[26]

PP application note 19: <applied>

6.2.6.3 FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1

The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2

The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

6.2.6.4 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1

The TSF shall resist **physical manipulation and physical probing**[27] to the **security IC**[28] by responding automatically such that the SFRs are always enforced.

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

6.2.6.5 FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[27] [assignment: physical tampering scenarios]

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

FPT_TST.1.1

The TSF shall run a suite of self-tests **during initial start-up** [29] to demonstrate the correct operation of ***the TSF***.

FPT_TST.1.2

The TSF shall provide authorised users with the capability to verify the integrity of ***TSF data***.

FPT_TST.1.3

The TSF shall provide authorised users with the capability to verify the integrity of ***TSF***.

PP application note 21: <applied>

6.3 TOE Security Assurance Requirements

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Architectural Design with domain separation and non-bypassability
	ADV_FSP.5 Complete semi-formal functional specification with additional error information
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.4 Semiformal modular design
	ADV_INT.2 Well-structured internals
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.2 Compliance with implementation standards
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives

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

Assurance Class	Assurance components
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.3 Testing: modular design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

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

6.4 Rationale

6.4.1 Security Requirements Rationale

6.4.1.1 Security Requirement 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.EMS_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.1	x		x	x	x						
FCS_CKM.4	x				x						
FCS_COP.1/SIG	x					x					
FCS_COP.1/PACE							x				
FCS_RND.1							x				
FDP_ACC.1/ SCD/SVD_Generation	x	x									
FDP_ACC.1/ SVD_Transfer	x										
FDP_ACC.1/Signature-creation	x						x				
FDP_ACF.1/ SCD/SVD_Generation	x	x									
FDP_ACF.1/ SVD_Transfer	x										
FDP_ACF.1/Signature-creation	x						x				
FDP_RIP.1					x		x				
FDP_SDI.2/Persistent				x	x	x					

	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.EMS_Design	OT.Tamper_ID	OT.Tamper_Resistance
FDP_SDI.2/DTBS							x	x			
FIA_AFL.1							x				
FIA_UAU.1		x					x				
FIA_UID.1		x					x				
FMT_MOF.1	x						x				
FMT_MSA.1/Admin	x	x									
FMT_MSA.1/Signatory	x						x				
FMT_MSA.2	x	x					x				
FMT_MSA.3	x	x					x				
FMT_MSA.4	x	x					x				
FMT_MTD.1/Admin	x						x				
FMT_MTD.1/Signatory	x						x				
FMT_SMR.1	x						x				
FMT_SMF.1	x						x				
FPT_EMS.1					x				x		
FPT_FLS.1					x						
FPT_PHP.1										x	
FPT_PHP.3					x						x
FPT_TST.1	x				x	x					

Table 11: Functional Requirement to TOE security objective mapping.

6.4.1.2 TOE Security Requirements Sufficiency

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

OT.SCD/SVD_Auth_Gen (Authorized SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The SFR

FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute initialisation. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute “SCD operational” of the SCD.

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

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

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

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

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

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1/SIG, 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 ensure self-tests ensuring correct signature-creation..

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

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

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

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

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

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

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

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

6.4.2 Dependency Rationale for Security functional Requirements

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

Requirement	Dependencies	Fulfilled
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/SIG, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1/SIG	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/PACE	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.4 See justification No. 1 for non-satisfied dependencies
FCS_RND.1	No dependencies	n. a.
FDP_ACC.1/ SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACC.1/ Signature-creation	FDP_ACF.1	FDP_ACF.1/Signature-Creation
FDP_ACC.1/ SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/ SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACF.1/ Signature-creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature-creation, FMT_MSA.3
FDP_ACF.1/ SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDR_RIP.1	No dependencies	n. a.
FDP_SDI.2/Persistent	No dependencies	n. a.
FDP_SDI.2/DTBS	No dependencies	n. a.
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1

Requirement	Dependencies	Fulfilled
FMT_MSA.1/ Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/ Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature_Creation SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation SFP, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/ Signature-creation
FMT_MTD.1/ Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/ Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No dependencies	n. a.
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_EMS.1	No dependencies	n. a.
FPT_FLS.1	No dependencies	n. a.
FPT_PHP.1	No dependencies	n. a.
FPT_PHP.3	No dependencies	n. a.
FPT_TST.1	No dependencies	n. a.

Table 12: Functional Requirements Dependencies.

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

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

6.4.3 Rationale for EAL 5 Augmented

The assurance level for the protection profile [PP0059] is EAL4 augmented with AVA_VAN.5. This security target enhances the security level by choosing EAL 5 augmented with AVA_VAN.5 and ALC_DVS.2 due to market demands.

Augmentation results from the selection of:

AVA_VAN.5 Advanced methodical vulnerability analysis

ALC_DVS.2 Sufficiency of security measures

The TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly

under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. The component AVA_VAN.5 has the following dependencies:

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

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

The component ALC_DVS.2 has no dependencies.

7 TOE summary specification

7.1 Security Functionality

7.1.1 TSF_Access: Access rights

This security functionality manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data. Access control for initialization and pre-personalization in the preparation phase – while the actual applet is not yet present – is based on platform functionality and on the card manager of the underlying SmartCafe Expert 7.0 C3 Java Card platform (SF.AccessControl, SF.I&A).

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

TSF_Access covers the following SFRs:

- FDP_ACC.1.1/SCD/SVD_Generation requires that the TSF shall enforce the SCD/SVD_Generation_SFP on the (1) subjects: S.User, the (2) objects: signature creation data (SCD), signature verification data (SVD), and the (3) operations: generation of a SCD/SVD pair. Access to these operations is realized by TSF_Access (while user authentication is performed by TSF_Auth).
- FDP_ACC.1.1/SVD_Transfer requires that the TSF shall enforce the SVD_Transfer_SFP on (1) subjects: S.User, (2) objects: signature verification data (SVD), and (3) operations: export. Access to these operations is realized by TSF_Access (while user authentication is performed by TSF_Auth).
- FDP_ACC.1.1/Signature-creation requires that the TSF shall enforce the Signature Creation SFP on (1) subjects: S.User, (2) objects: DTBS/R, signature creation data (SCD), and (3) operations: signature-creation. Access to these operations is realized by TSF_Access (while user authentication is performed by TSF_Auth).
- FDP_ACF.1.1/SCD/SVD_Generation requires that the TSF shall enforce the SCD/SVD_Generation_SFP to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management ". Access to these operations is realized by TSF_Access (while user authentication is performed by TSF_Auth).
- FDP_ACF.1.2/SCD/SVD_Generation_ SFP requires that the TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute "SCD / SVD Management" set to "authorised" is allowed to generate a SCD/SVD pair. This is realized by TSF_Access and TSF_Auth.
- FDP_ACF.1.3/SCD/SVD_Generation requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none. This is realized by TSF_Access and TSF_Auth.
- FDP_ACF.1.4/SCD/SVD_Generation requires that the TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute "SCD / SVD manage-ment" set to "not authorized" is not allowed to generate SCD/SVD pair. This is realized by TSF_Access and TSF_Auth.
- FDP_ACF.1.1/ SVD_Transfer requires that the TSF shall enforce the SVD_Transfer_SFP to objects based on the following: (1) the S.User is associated with the security attribute Role, and (2) the signature verification data (SVD). This is realized by TSF_Access and TSF_Auth.
- FDP_ACF.1.2/ SVD_Transfer requires that the TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Admin is allowed to export the signature verification data (SVD). This is realized by TSF_Access and TSF_Auth.

- FDP_ACF.1.3/ SVD_Transfer requires that the TSF shall explicitly authorise access of subjects to objects. This is realized by TSF_Access and TSF_Auth.
- FDP_ACF.1.4/SVD_Transfer requires that the TSF shall explicitly deny access of subjects to objects. This is realized by TSF_Access and TSF_Auth.
- FDP_ACF.1.1/Signature-creation requires that the TSF shall enforce the Signature Creation SFP to objects based on the following: (1) the user S.User is associated with the security attribute “Role” and (2) the signature creation data (SCD) with the security attribute “SCD Operational”. These rules and attributes are controlled by TSF_Access and TSF_Auth.
- FDP_ACF.1.2/Signature-creation requires that the TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Sigy is allowed to create electronic signatures for DTBS/R with signature creation data (SCD) which security attribute “SCD operational” is set to “yes”. These rules and attributes are controlled by TSF_Access and TSF_Auth.
- FDP_ACF.1.3/Signature-creation requires that the TSF shall explicitly authorise access of subjects to objects. This is realized by TSF_Access and TSF_Auth.
- FDP_ACF.1.4/Signature-creation requires that the TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User is not allowed to create electronic signatures for DTBS/R with signature creation data (SCD) which security attribute “SCD operational” is set to “no”. These rules and attributes are controlled by TSF_Access and TSF_Auth.
- FDP_RIP.1.1 requires that the TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from the following objects: signature creation data (SCD). This is realized by TSF_Access.
- FIA_AFL.1.1 requires that the TSF shall detect when an administrator configurable positive integer within [assignment: 1-16] unsuccessful authentication attempts occur related to consecutive failed authentica-tion attempts. This is realized within TSF_Admin and TSF_Auth.
- FIA_AFL.1.2 requires that when the defined number of unsuccessful authentication attempts has been met, the TSF shall block the reference authentication data (RAD). This is realized by TSF_Auth and TSF_Access.
- FIA_UID.1.1 requires that the TSF shall allow (1) self test according to FPT_TST.1, and (2) receiving DTBS on behalf of the user to be performed before the user is identified. This is realized by TSF_Access and TSF_Auth.
- FIA_UID.1.2 requires that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. This is realized by TSF_Access and TSF_Auth.
- FIA_UAU.1.1 requires that the TSF shall allow (1) self test according to FPT_TST.1, (2) identification of the user by means of TSF required by FIA_UID.1, and (3) receiving DTBS on behalf of the user to be performed before the user is authenticated. This is realized by TSF_Access, TSF_Auth and TSF_SecureMessaging.
- FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. This is realized by TSF_Access and TSF_Auth.
- FMT_MOF.1.1 requires that the TSF shall restrict the ability to enable the functions signature-creation function to R.Sigy. This is realized by TSF_Access.
- FMT_MSA.1.1/Admin requires that the TSF shall enforce the SCD/SVD_Generation_SFP to restrict the ability to modify [assignment: other operations] the security attributes SCD / SVD management to R.Admin. This is realized by TSF_Access.

- FMT_MSA.1.1/Signatory requires that the TSF shall enforce the Signature Creation SFP to restrict the ability to modify the security attributes SCD operational to R.Sigy. This is realized by TSF_Access.
- FMT_MTD.1.1/Admin requires that the TSF shall restrict the ability to create the reference authentication data (RAD) to R.Admin. This is realized by TSF_Access and TSF_Auth.
- FMT_MTD.1.1/ Signatory requires that the TSF shall restrict the ability to modify [assignment: none] the reference authentication data (RAD, e.g. a PIN) to R.Sigy. This is realized by TSF_Access and TSF_Auth.
- FMT_SMR.1.1 requires that the TSF shall maintain the roles R.Admin and R.Sigy. This is realized by TSF_Access and TSF_Admin.

7.1.2 TSF_Admin: Administration

This Security Functionality manages the storage of manufacturing data, pre-personalization data and personalization data. This storage area is a write-only-once area and write access is subject to Manufacturer or Personalization Agent authentication. Management of manufacturing and pre-personalization data in the preparation phase – while the actual applet is not yet present – is based on platform functionality and on the card manager of the underlying SmartCafe Expert 7.0 C3 Java Card platform (SF.SecureManagement); also Audit functionality is based on SmartCafe functionality (SF.Audit). During Operational Use phase, read access is only possible after successful authentication.

TSF_Admin covers the following SFRs:

- FMT_SMR.1.1 requires that the TSF shall maintain the roles R.Admin and R.Sigy. This is realized by TSF_Access and TSF_Admin.
- FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. This is realized by TSF_Auth and TSF_Admin.
- FMT_SMF.1.1 requires that the TSF shall be capable of performing the following management functions: (1) Creation and modification of the reference authentication data (RAD), (2) Enabling the signature-creation function, (3) Modification of the security attribute SCD/SVD management, SCD operational, (4) Change the default value of the security attribute SCD Identifier, (5) none. This is realized by TSF_Admin.
- FMT_MSA.3.1 requires that the TSF shall enforce the SCD/SVD_Generation_SFP, SVD_Transfer_SFP and Signature Creation SFP to provide restrictive default values for security attributes that are used to enforce the SFP. This is realized by TSF_Admin and TSF_Crypto.
- FMT_MSA.3.2 requires that the TSF shall allow the R.Admin to specify alternative initial values to override the default values when an object or information is created. This is realized by TSF_Admin and TSF_Crypto.
- FMT_MSA.4.1 requires that the TSF shall use the following rules to set the value of security attributes: (1) if S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute “SCD operational of the SCD” shall be set to “no” as a single operation; (2) if S.Sigy successfully generates an SCD/SVD pair the security attribute “SCD operational of the SCD” shall be set to “yes” as a single operation. This is realized by TSF_Admin and TSF_Crypto.

7.1.3 TSF_Secret: Secret key management

This Security Functionality ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These functions make use of SF.CryptoKey of the underlying SmartCafe Expert 7.0 C3 Java Card OS.

TSF_Secret covers the following SFRs:

- FCS_CKM.1 requires that the TSF shall generate an SCD/SVD (Signature creation data / signature verification data) pair in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes: ECDSA or RSA key generation. This is realized by TSF_Secret (also using TSF_OS).
- FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method, i.e. overwriting the key value with zero values. This is realized by TSF_Secret (also using TSF_OS).

7.1.4 TSF_Crypto: Cryptographic operations

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

TSF_Crypto covers the following SFRs:

- FCS_COP.1/PACE requires that for variants with a contactless interface the TOE must provide the PACE authentication protocol with AES. This is covered by TSF_Crypto which itself uses the cryptographic mechanisms realized by TSF_OS.
- FCS_COP.1.1/SIG requires that the TSF shall perform electronic signature-generation in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes. This is covered by TSF_Crypto which itself uses the cryptographic mechanisms realized by TSF_OS.

7.1.5 TSF_ SecureMessaging: Secure Messaging

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

TSF_SecureMessaging covers the following SFRs:

- FIA_UAU.1.1 requires that the TSF shall allow (1) self test according to FPT_TST.1, (2) identification of the user by means of TSF required by FIA_UID.1, and (3) receiving DTBS on behalf of the user to be performed before the user is authenticated. This is realized by TSF_SecureMessaging, TSF_Access and TSF_Auth.

7.1.6 TSF_Auth: Authentication protocols

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

- **TSF_Auth_VERIFY_PIN**

  TSF_Auth_PIN performs the VERIFY PIN (RAD) authentication mechanism.

- **TSF_Auth_PACE**

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

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

The above two authentication mechanisms cover the following SFRs:

- FCS_COP.1/PACE requires that for variants with the contactless interface the TOE must provide the PACE authentication protocol.
- FDP_ACC.1.1/SCD/SVD_Generation requires that the TSF shall enforce the SCD/SVD_Generation_SFP on the (1) subjects: S.User, the (2) objects: signature creation data (SCD), signature verification data (SVD), and the (3) operations: generation of a SCD/SVD pair. This is realized by TSF_Auth and TSF_Access.
- FDP_ACF.1.1/SCD/SVD_Generation requires that the TSF shall enforce the SCD/SVD_Generation_SFP to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management ". This is realized by TSF_Auth and TSF_Access.
- FDP_ACF.1.2/SCD/SVD_Generation_ SFP requires that the TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute "SCD / SVD Management" set to "authorized" is allowed to generate a SCD/SVD pair. This is realized by TSF_Auth and TSF_Access.
- FDP_ACF.1.3/SCD/SVD_Generation requires that the TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none. This is realized by TSF_Auth and TSF_Access.
- FDP_ACF.1.4/SCD/SVD_Generation requires that the TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute "SCD / SVD management" set to "not authorized" is not allowed to generate SCD/SVD pair. This is realized by TSF_Auth and TSF_Access.
- FDP_ACC.1.1/SVD_Transfer requires that the TSF shall enforce the SVD_Transfer_SFP on (1) subjects: S.User, (2) objects: signature verification data (SVD), and (3) operations: export. This is realized by TSF_Auth and TSF_Access.
- FDP_ACF.1.1/ SVD_Transfer requires that the TSF shall enforce the SVD_Transfer_SFP to objects based on the following: (1) the S.User is associated with the security attribute Role, and (2) the signature verification data (SVD). This is realized by TSF_Auth and TSF_Access.
- FDP_ACF.1.2/ SVD_Transfer requires that the TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Admin is allowed to export the signature verification data (SVD). This is realized by TSF_Access and TSF_Auth.
- FDP_ACF.1.3/ SVD_Transfer requires that the TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none. This is realized by TSF_Access and TSF_Auth.
- FDP_ACF.1.4/SVD_Transfer requires that the TSF shall explicitly deny access of subjects to objects based on the following additional rules: none. This is realized by TSF_Auth and TSF_Access.
- FDP_ACC.1.1/Signature-creation requires that the TSF shall enforce the Signature Creation SFP on (1) subjects: S.User, (2) objects: DTBS/R, signature creation data (SCD), and (3) operations: signature-creation. This is realized by TSF_Auth and TSF_Access.
- FDP_ACF.1.1/Signature-creation requires that the TSF shall enforce the Signature Creation SFP to objects based on the following: (1) the user S.User is associated with the security attribute "Role" and (2) the signature creation data (SCD) with the security attribute "SCD Operational". This is realized by TSF_Auth and TSF_Access.
- FDP_ACF.1.2/Signature-creation requires that the TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Sigy is allowed to create electronic signatures for DTBS/R with signature creation data (SCD) which security attribute "SCD operational" is set to "yes". This is realized by TSF_Auth and TSF_Access.
- FDP_ACF.1.3/Signature-creation requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none. This is realized by TSF_Auth and TSF_Access.

- FDP_ACF.1.4/Signature-creation requires that the TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User is not allowed to create electronic signatures for DTBS/R with signature creation data (SCD) which security attribute “SCD operational” is set to “no”. This is realized by TSF_Auth and TSF_Access.
- FIA_UID.1.1 requires that the TSF shall allow (1) self test according to FPT_TST.1, and (2) receiving DTBS on behalf of the user to be performed before the user is identified. This is realized by TSF_Auth and TSF_Access.
- FIA_UID.1.2 requires that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. This is realized by TSF_Auth and TSF_Access.
- FIA_UAU.1.1 requires that the TSF shall allow (1) self test according to FPT_TST.1, (2) identification of the user by means of TSF required by FIA_UID.1, and (3) receiving DTBS on behalf of the user to be performed before the user is authenticated. This is realized by TSF_Auth, TSF_Access and TSF_SecureMessaging.
- FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. This is realized by TSF_Auth and TSF_Access.
- FIA_AFL.1.1 requires that the TSF shall detect when an administrator configurable positive integer within [assignment: 1-16] unsuccessful authentication attempts occur related to consecutive failed authentication attempts. This is realied by TSF_Admin and TSF_Auth.
- FIA_AFL.1.2 requires that when the defined number of unsuccessful authentication attempts has been met, the TSF shall block the reference authentication data (RAD). This is realized by TSF_Auth and TSF_Access.
- FMT_SMR.1.1 requires that the TSF shall maintain the roles R.Admin and R.Sigy. This is realized by TSF_Access and TSF_Admin.
- FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. This is realized by TSF_Auth and TSF_Admin.
- FMT_MSA.2.1 requires that the TSF shall ensure that only secure values are accepted for SCD / SVD Management and SCD operational. This is realized by TSF_Auth.
- FMT_MTD.1.1/Admin requires that the TSF shall restrict the ability to create the reference authentication data (RAD) to R.Admin. This is realized by TSF_Auth and TSF_Access.
- FMT_MTD.1.1/ Signatory requires that the TSF shall restrict the ability to modify [assignment: none] the reference authentication data (RAD, e.g. a PIN) to R.Sigy. This is realized by TSF_Auth and TSF_Access.

7.1.7 TSF_Integrity: Integrity protection

This Security Functionality protects the integrity of internal applet data like the Access control lists. This function makes use of SF.SecureManagement and SF.Transaction of the underlying SmartCafe Expert 7.0 C3 Java Card OS (cf. the according security target [ST_SmartCafe]).

TSF_Integrity covers the following SFRs:

- FDP_SDI.2.1/Persistent requires that the TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored data. This is realized by TSF_Integrity and TSF_OS.
- FDP_SDI.2.2/Persistent requires that upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data and (2) inform the S.Sigy about integrity error. This is realized by TSF_Integrity and TSF_OS.

- FDP_SDI.2.1/DTBS requires that the TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored DTBS. This is realized by TSF_Integrity and TSF_OS.
- FDP_SDI.2.2/DTBS requires that upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data and (2) inform the S.Sigy about integrity error. This is realized by TSF_Integrity and TSF_OS.
- FPT_PHP.1.1 requires that the TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. This is realized by TSF_Integrity and TSF_OS.
- FPT_PHP.1.2 requires that the TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. This is realized by TSF_Integrity and TSF_OS.

7.1.8 TSF_OS: Javacard OS security functions

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

- Enforcement of access control (SF.AccessControl)
- Audit functionality (SF.Audit)
- Cryptographic key management (SF.CryptoKey)
- Cryptographic operations (SF.CryptoOperation)
- Identification and authentication (SF.I&A)
- Secure management of TOE resources (SF.SecureManagement)
- Transaction management (SF.Transaction)

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

- FCS_CKM.1 requires that the TSF shall generate an SCD/SVD (Signature creation data / signature verification data) pair in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes. This is realized by TSF_OS.
- FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method. This is realized in the security functions provided by TSF_OS (and TSF_Secret).
- FCS_COP.1/PACE requires that for variants with the contactless interface the TOE must provide the PACE authentication protocol. This is realized using security functionality provided by TSF_OS.
- FCS_COP.1.1/SIG requires that the TSF shall perform electronic signature-generation in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes. This is realized by TSF_OS.
- FCS_RND.1 requires that the TSF should provide random numbers with a defined quality metric. This is provided by TSF_OS.
- FDP_SDI.2.1/DTBS requires that the TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored DTBS. This is realized by TSF_Integrity and TSF_OS.

- FDP_SDI.2.2/DTBS requires that upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data and (2) inform the S.Sigy about integrity error. This is realized by TSF_Integrity and TSF_OS.
- FPT_EMS.1.1 requires that the TOE shall not variations in power consumption or timing during command execution in excess of non-useful information enabling access to RAD and SCD. This is mainly realized by appropriate measures in TSF_OS together with the strict following of the security implementation guidelines of the Javacard platform.
- FPT_EMS.1.2 requires that the TSF shall ensure any users are unable to use the following interface: smart card circuit contacts or contactless interface to gain access to RAD and SCD. This is mainly realized by appropriate measures in TSF_OS together with the strict following of the security implementation guidelines of the Javacard platform.
- FPT_FLS.1.1 requires that the TSF shall preserve a secure state when the following types of failures occur: (1) self-test according to FPT_TST fails, or (2) exposure to out-of-range operating conditions where therefore a malfunction could occur. This is realized by TSF_OS (together with and TSF_Integrity).
- FPT_PHP.1.1 requires that the TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.
- FPT_PHP.1.2 requires that the TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.
- FPT_PHP.3.1 requires that the TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.
- FPT_TST.1.1 requires that the TSF shall run a suite of self-tests periodically during normal operation to demonstrate the correct operation of the TSF. This is realized by TSF_OS.
- FPT_TST.1.2 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF data. This is realized by TSF_OS.
- FPT_TST.1.3 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF. This is realized by TSF_OS.

7.2 TOE summary specification rationale

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

7.2.1 Mapping of TOE Security Requirements and TOE Security Functionalities

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

	TSF_Access	TSF_Admin	TSF_Secret	TSF_Crypto	TSF_SecureMessaging	TSF_Auth	TSF_Integrity	TSF_OS
FCS_CKM.1			x					x
FCS_CKM.4			x					x
FCS_COP.1/SIG				x		x		x
FCS_COP.1/PACE				x		x		
FCS_RND.1								x
FDP_ACC.1/SCD/SVD_Generation	x					x		
FDP_ACC.1/SVD_Transfer	x					x		
FDP_ACC.1/Signature-creation	x					x		
FDP_ACF.1/SCD/SVD_Generation	x					x		
FDP_ACF.1/SVD_Transfer	x					x		
FDP_ACF.1/Signature-creation	x					x		
FDP_RIP.1	x							
FDP_SDI.2/Persistent							x	x
FDP_SDI.2/DTBS							x	x
FIA_AFL.1	x					x		
FIA_UAU.1	x				x	x		
FIA_UID.1	x					x		
FMT_MOF.1	x							
FMT_MSA.1/Admin	x							
FMT_MSA.1/Signatory	x							
FMT_MSA.2						x		
FMT_MSA.3		x						
FMT_MSA.4		x						
FMT_MTD.1/Admin	x					x		
FMT_MTD.1/Signatory	x					x		
FMT_SMR.1	x	x				x		
FMT_SMF.1		x						
FPT_EMS.1								x
FPT_FLS.1								x
FPT_PHP.1							x	x
FPT_PHP.3								x
FPT_TST.1								x

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

8 References

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

Common Criteria

[CC_1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012; CCMB-2012-09-001.
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 4, September 2012; CCMB-2012-09-002.
[CC_3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, September 2012; CCMB-2012-09-003.
[CC_4]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 4, September 2012; CCMB-2012-09-004.

Protection Profiles

[PP0059]	Protection profiles for secure signature creation device – Part 2: Device with key generation; English version EN 419211-2:2013, English translation of DIN EN 419211-2:2013-12; PP Registration: BSI-CC-PP-0059-2009-MA-02; December 2013.
[PP_Javacard]	Java Card Protection Profile - Open Configuration, Version 3.0 (May 2012), Published by Oracle, Inc.
[PP0006]	Protection Profile Secure Signature-Creation Device Type 3, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0006-2002T, also short SSVG-PPs or CWA14169
[PP0084]	Security IC Platform Protection Profile, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Rev 1.0, 13 January 2014.

TOE and Platform References

[ST_SmartCafe]	Security Target Lite Sm@rtCafé® Expert 7.0 C3; Version 2.9/Status 16.08.2017
[ZertSmartCafe]	BSI: Certification Report BSI-DSZ-CC-1028-2017 for Sm@rtCafé® Expert 7.0 C3 from Veridos GmbH - Identity Solutions by G&D BDR; 08.09.2017 Assurance Continuity Maintenance Report BSI-DSZ-CC-1028-2017-MA-01 Sm@rtCafé® Expert 7.0 C3 from Giesecke+Devrient Mobile Security GmbH; 04.10.2018
[ST_IC]	Security Target Lite for BSI-DSZ-CC-0951-2015, Version 1.2, 2017-05-10, Infineon
[ZertIC]	Certification report BSI-DSZ-CC-0951-2015 for Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008,SHA-2 v1.01 and Toolbox v2.03.008 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 11.11.2015

	Assurance Continuity Reassessment Report BSI-DSZ-CC-0951-2015-RA-01, Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008,SHA-2 v1.01 and Toolbox v2.03.008 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 31.05.2017
[Guidance_PRE]	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing a Secure Signature Creation Device application with on-chip key generation (SSCD Type 3) and supporting PKI utilization; Preparation Guidance (AGD_PRE). For the exact version please refer to the certification report.
[Guidance_OPE]	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing a Secure Signature Creation Device application with on-chip key generation (SSCD Type 3) and supporting PKI utilization; Operational Guidance (AGD_PRE). For the exact version please refer to the certification report.
[Guidance_GEN]	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card Applet Suite providing Electronic ID Documents applications; Guidance Manual. For the exact version please refer to the certification report.
[GP_CIC]	GlobalPlatform Card Common Implementation Configuration Version 1.0, February 2014
[AGD_PRE]	Preparative procedures SmartCafé Expert 7.0 C3, Version 3.6/Status 10.08.17

EU regulation

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

The DIRECTIVE

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

Application and Cryptography standards

[CADES]	ETSI Technical Specification 101 733, CMS Advanced Electronic Signatures (CAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp
[XADES]	ETSI Technical Specification 101 903, XML Advanced Electronic Signatures (XAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp
[PADES]	ETSI Technical Specification 102 778: PDF Advanced Electronic Signatures (PAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp

[TR03110]	Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1, Version 2.20, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[AIS20]	Anwendungshinweise und Interpretationen zum Schema (AIS); AIS 20, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
[FIPS180-4]	Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD (SHS), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, March 2012
[FIPS186-3]	Digital Signature Standard (DSS) - FIPS PUB 186-3, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, June, 2009
[FIPS197]	Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001
[PKCS1]	PKCS #1: RSA Encryption Standard – An RSA Laboratories Technical Note Version 2.1
[RFC5639]	RFC 5639 ECC Brainpool Standard Curves & Curve Generation, March 2010; available at: http://tools.ietf.org/html/rfc5639
[TR03111]	Technical Guideline TR-03111, “Elliptic Curve Cryptography”, Version 2.0, BSI, 2012-06-28.
[SEC2]	Standards for efficient cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research, September 20, 2000, Version 1. http://www.secg.org/collateral/sec2_final.pdf

Glossary

The following glossary lists the main abbreviations and gives terms and definitions. It includes the terms and definitions given in [PP0059], chapter 3.2.3 and 4.

Administrator	User who performs TOE initialisation, TOE personalisation, or other TOE administrative functions
Advanced electronic signature	Electronic signature which meets specific requirements in [Directive]. According to the Directive a electronic signature qualifies as an electronic signature if it: • is uniquely linked to the signatory; • is capable of identifying the signatory; • is created using means that the signatory can maintain under his sole control, and • is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Authentication data	Information used to verify the claimed identity of a user
Authentication	Authentication defines a procedure that verifies the identity of the commu-nication partner. The most elegant method is based on the use of so called electronic signatures.
CA	Certification authority.
CC	Common criteria.
Certificate	Electronic signature used as electronic attestation binding an SVD to a person confirming the identity of that person as legitimate signer ([Directive]: 2.9).
Certificate info	Information associated with a SCD/SVD pair that may be stored in a secure signature creation device. Certificate info is either • a signer's public key certificate or, • one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values. Certificate info may be combined with information to allow the user to distinguish between several certificates.
Certificate generation application (CGA)	Collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a electronic signature of the certificate
Certificate revocation list	A list of revoked certificates issued by a certificate authority
Certification service provider (CSP)	Entity that issues certificates or provides other services related to electronic signatures ([Directive]: 2.11).
CGA	Certification generation application.
CRL	See Certificate Revocation List.
Data to be signed (DTBS)	All electronic data to be signed including a user message and signature attributes

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

Public key	Publicly known key in an asymmetric cipher which is used for encryption and verification of electronic signatures.
Public key infrastructure (PKI)	Combination of hardware and software components, policies, and different procedures used to manage electronic certificates.
Qualified certificate	Public key certificate that meets the requirements laid down in [Directive], Annex I and that is provided by a CSP that fulfils the requirements laid down in [Directive], Annex II.
Qualified electronic signature	advanced electronic signature that has been created with an SSCD with a key certified with a qualified certificate ([Directive]: 5.1).
RAD	Reference authentication data.
Random numbersa	Many cryptographic algorithms or protocols require a random element, mostly in form of a random number, which is newly generated in each case. In these cases, the security of the procedure depends in part on the suitability of these random numbers. As the generation of real random numbers within computers still imposes a problem (a source for real random events can in fact only be gained by exact observation of physical events, which is not easy to realize for a software), so called pseudo random numbers are used instead.
Reference authentication data (RAD)	Data persistently stored by the TOE for authentication of a user as authorised for a particular role.
SCA	Signature creation application.
SCD	Signature creation data.
SCS	Signature creation system.
SDO	Signed data object.
Secure messaging	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.
Secure signaturecreation device (SSCD)	Personalized device that meets the requirements laid down in [Directive], Annex III by being evaluated according to a security target conforming to this ST ([Directive]: 2.5 and 2.6).
SFP	Security function policy.
SFR	Security functional requirement.
Signatory	Legitimate user of an SSCD associated with it in the certificate of the signature-verification and who is authorized by the SSCD to operate the signature-creation function ([Directive]: 2.3).
Signature attributes	Additional information that is signed together with a user message.
Signature creation application (SCA)	Application complementing an SSCD with a user interface with the purpose to create an electronic signature. Note: A signature creation application is software consisting of a collection of application components configured to: • present the data to be signed (DTBS) for review by the signatory, • obtain prior to the signature process a decision by the signatory, • if the signatory indicates by specific unambiguous input or action its intent to sign send a DTBS/R to the TOE • process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.

Signature creation data (SCD)	Private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature ([Directive]: 2.4).
Signature creation system (SCS)	Complete system that creates an electronic signature consists of the SCA and the SSCD.
Signature verification data (SVD)	Public cryptographic key that can be used to verify an electronic signature ([Directive] 2.7).
Smart card	A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (ROM, EEPROM, Flash) memory, i.e. which can carry out its own calculations in contrast to a simple storage card. Sometimes a smart card has a numerical coprocessor (NPU) to execute public key algorithms efficiently. Smart cards have all of their functionality comprised on a single chip (in contrast to chip cards, which contain several chips wired to each other). Therefore, such a smart card is ideal for use in cryptography as it is almost impossible to manipulate its internal processes.
SSCD	Secure signature creation device.
SSCD provisioning service	Service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD.
ST	Security target.
SVD	Signature verification data.
TOE	Target of evaluation.
Travel document	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel.
TSF	TOE security functionality.
User	Entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User Message	Data determined by the signatory as the correct input for signing.
VAD	See Verification authentication data.
Verification authentication data (VAD)	Data provided as input to a secure signature creation device for authentication by cognition or by data derived from a user's biometric characteristics.
X.509	Standard for certificates, CRLs and authentication services. It is part of the X.500 standard of the ITU-T for realization of a worldwide distributed directory service realized with open system.