cryptoVision

cv act ePasslet/ePKI v3.6

Security Target

BSI-DSZ-CC-0804

Common Criteria / ISO 15408
EAL 4+

Document Version 1.05 • 2012-08-16

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
0.1	2010-11-19	Thomas Zeggel	Initial version (chapter 1-6) with marked assertions (to be made), glossary and references.
0.2	2010-11-23	Thomas Zeggel	Small corrections
0.3	2010-11-29	Thomas Zeggel	Added chapter 7.1; change of the internal structure of chapter 1 and 2. Additional minor changes and corrections.
0.4	2010-12-20	Thomas Zeggel	Changes of the TOE description in chapter 1.
0.5	2010-12-21	Thomas Zeggel	Extended chapter 7.
0.6	2011-01-05	Thomas Zeggel	Small corrections. TSFs and Objectives linked.
0.7	2011-01-07	Benjamin Drisch, Thomas Zeggel	Internal review with minor corrections
0.8	2011-01-21	Thomas Zeggel	Small corrections and changes in chapter 1 after review by NXP. CAdES/XadES paragraph in section 1.3.2 deleted.
0.9	2011-08-29	Benjamin Drisch	Changes from TÜViT review of BAC-ST included
0.91	2011-09-22	Thomas Zeggel	Changes according to TüvIT observation report, dated 2011-09-12.
0.92	2011-10-13	Thomas Zeggel	Integration of iterated cryptographic SFRs into one with an „or“ connection.
0.93	2011-11-10	Benjamin Drisch, Thomas Zeggel	Changes according to BSI evaluation kick-off meeting and TüvIT observation report.
0.94	2012-02-06	Thomas Zeggel	Changed product name in ePasslet/ePKI v3.6. Comments in SFR mappings of chapter 2.2 added. Change of name of chapter 1.1. Reference [ZertIC080] corrected. Certificates of Crypto Libs referenced. Additional references in chapters 1.1, 1.2 and 1.3.2. Names of hardware platforms corrected. Key lengths adjusted according to latest JCOP ST. Additional changes according to observation report No.5: • Introduced SFR FCS_RND.1 • Introduced SFR FCS_COP.1/PACE • Renamed SFR FCS_COP.1 in FCS_COP.1/SIG • Statements to application notes 12, 13 and 14 added
0.95	2012-02-09	Benjamin Drisch	Minor changes due to remarks by TÜViT: • Removed Secure Messaging requirement in FIA_UAU.1.1 • Repaired broken link to figures 1 and 2 in section 1.3.1 • Corrected “RNG.1” to “RND.1” in table 3 • Removed entry “Content” from TOC
0.96	2012-02-21	Benjamin Drisch	Changes due to remarks from BSI:

			• Added certification ID of platform and involved application in section 1.3.2 • Specified RSA variant in FCS_CKM.1.1 and FCS_COP.1.1/SIG • Added PKCS#1 to list of references
0.97	2012-02-23	Benjamin Drisch	Changes due to further remarks by BSI: • Added certification ID of crypto lib and hardware in section 1.3.2 • Further concretized applications involved in actual TOE in different mask variants in section 1.3.2 • Added remarks about EC parameters from JCOP guidance manual to FCS_CKM and FCS_COP • Added version and exact reference for PACE in FCS_COP1.1/PACE • Specified supported hash functions for FCS_COP.1/Sig • Included remark on added SFRs in PP conformance claim in section 2.1
0.98	2012-02-28	Benjamin Drisch	Corrected description of hash functions used in FCS_COP.1/Sig
0.99	2012-02-29	Benjamin Drisch	Aligned ECDSA standard reference with JCOP Security Target in FCS_COP.1/Sig
1.00	2012-03-01	Benjamin Drisch	• Futher clarified remark on applications involved in actual TOE section 1.3.2 • Corrected misspelling of the word “authorise” (various occurences) and incorrect SFR naming (due to erroneous search & replace operation)
1.01	2012-03-12	Benjamin Drisch, Thomas Zeggel	• Remark about fixed configuration and exclusion of code loading concretized in section 1.3.1 • Revised SFR definition (FCS_COP.1/SIG also without internal hashing) • Added remark about random number generation being provided by underlying platform • Update SHA reference from [FIPS180-2] to [FIPS180-4] • Changed role allowed to export SVD in FDP_ACF.1.2/ SVD_Transfer_SFP to R.Sigy and R.Admin.
1.02	2012-03-15	Benjamin Drisch, Thomas Zeggel	• Remark about MIFARE functionality added in section 1.3.2 • Life cycle definition clarified in section 1.3.6
1.03	2012-03-22	Benjamin Drisch	• TOE configuration clarified in section 1.3.2 • Performed minor corrections of mappings in Table 12
1.04	2012-04-16	Benjamin Drisch	• Clarified TOE definition and life-cycle description
1.05	2012-08-16	Benjamin Drisch	Revised TOE definition • corrected references to underlying certificates for

			Crypto Library and HW platform in 1.3.2 • explicitely stated contact-based interface Corrected reference to Guidance Manual

1 Introduction

1.1 ST/TOE Identification

Title:	cv act ePasslet/ePKI v3.6 Security Target
Version:	v1.05
Origin:	cv cryptovision GmbH
Compliant to:	Common Criteria Protection Profile - Protection profiles for Secure signature creation device — Part 2: Device with key generation (BSI-CC-PP0059) [PP0059]
Product identification:	cv act ePasslet/ePKI v3.6
ROM identification value:	P5Cx081UA: 8F80EC
	P5Cx080UA: 7C1970
	P5Cx040UA: F39353
Javacard OS platform:	NXP JCOP 2.4.1 R3 [ZertJCOP080], [ZertJCOP081], [ZertJCOP040]
Cryptographic library:	[ZertCL080], [ZertCL081], [ZertCL040]
Security controller:	[ZertIC080], [ZertIC081], [ZertIC040]
TOE identification:	cv act ePasslet/ePKI v3.6
TOE documentation:	Administration and user guide [Guidance]

1.2 ST overview

The aim of this document is to describe the Security Target for the SSCD compliant configurations of the cv act ePassslet Suite. The cv act ePasslet Suite is a set of Javacard applications intended to be used exclusively on the NXP JCOP Javacard OS platform, which is certified according to CC EAL 5+ [ZertJCOP080], [ZertJCOP081], [ZertJCOP040]. The JCOP Javacard OS platform is based on the NXP P5CD security controller, which is itself certified according to CC EAL 5+ [ZertIC080], [ZertIC081], [ZertIC040], and the certified cryptographic library [ZertCL080], [ZertCL081], [ZertCL040].

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-PP0059) [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 EAL4+.

1.3 TOE overview

1.3.1 Overview of cv act ePasslet Suite

The cv act ePasslet Suite is a modular multi-application solution for eID documents based on Java Card.

It provides the following applications:

Application name	Function	Standard
cv act ePasslet/BAC	Basic Access Control	ICAO Doc 9303
cv act ePasslet/EACv1.11	Extended Access Control, V1.11	BSI TR03110, V1.11
cv act ePasslet/EACv2-SAC	Extended Access Control, V2.05	BSI TR03110, V2.05
cv act ePasslet/GeID	German eID card	BSI TR03127, BSI TR03110
cv act ePasslet/ePKI	IAS with own PKCS#15 profile	PKCS#15
cv act ePasslet/IDL	International Driving License	ISO 18013
cv act ePasslet/eHIC	European Health Insurance	CWA 15974
cv act ePasslet/EuCCB	European Citizen Card - Base Profile	CEN/TS 15480
cv act ePasslet/EuCCF	European Citizen Card - French Profile	GIXEL IAS-ECC V1.01
cv act ePasslet/eVR	Electronic Vehicle Registration	EU Council Directive 1999/37/EC
cv act ePasslet/NIDS	Combination of EAC V1.11 and ePKI	BSI TR03110, V1.11, PKCS#15

Table 1: Customer view of the available applications in the cv act ePasslet Suite.

These applications are realized by configurations of one or more predefined applets; while each application has a distinct configuration, different applications might use the same underlying applet. For details on the relation between applets and applications please refer to Figure 1 and Figure 2 below.

While the whole applet code resides in ROM, the applets providing the different applications are instantiated into EEPROM. Multiple 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 EACv1 applet and an ePKI applet providing a travel application with LDS data and EAC authentication together with a signature application (offered as own standard product configuration "NIDS" as listed in Table 1, Figure 1 and Figure 2).

The product is available in two variants:

Variant 1

- available on P5Cx081 and P5Cx041
- covering all applications provided in Table 1
- certified products (on P5Cx081 only):
  - BAC certified according to PP0055
  - EACv1 certified according to PP0056
  - EACv2-SAC certified according to SAC/PACE-PP
  - ePKI certified as Secure Signature Creation Device (SSCD) according to PP0059 (contact interface and contactless interface with PACE)

The following Figure 1 gives an overview of the available applications and actual applets in variant 1.

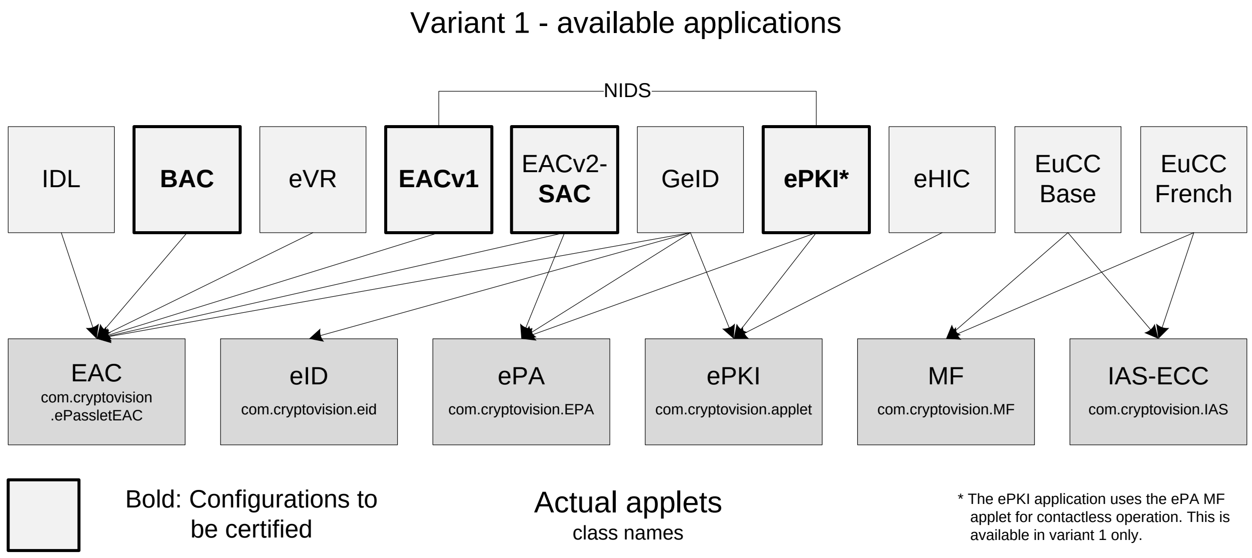

Figure 1: Available applications and actual applets in variant 1.

The other version (variant 2) contains a subset of these applications:

Variant 2

- available on P5Cx080 and P5Cx040
- Contains the applets and applications indicated in Figure 2
- certified products:
  - BAC certified according to PP0055
  - EACv1 certified according to PP0056
  - ePKI certified as Secure Signature Creation Device (SSCD) according to PP0059 (contact interface only)

The following Figure 2 gives an overview of the available applications and actual applets in variant 2.

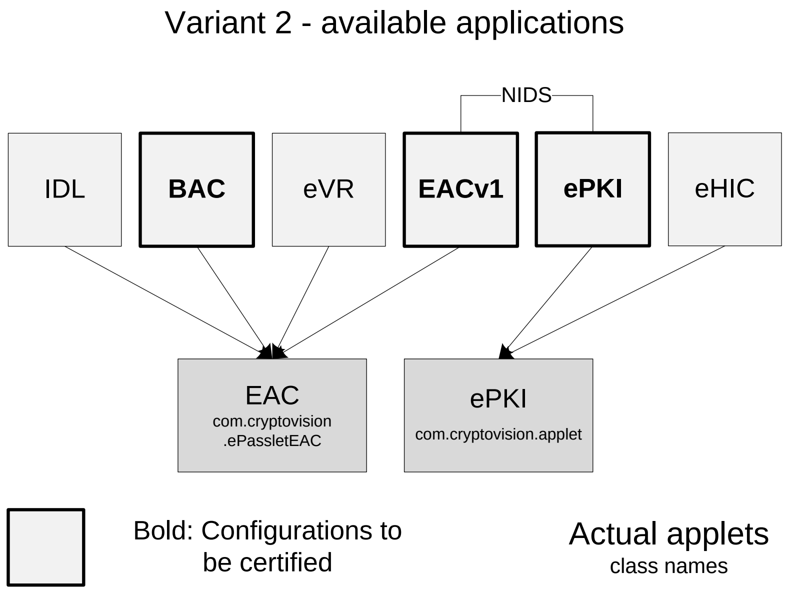
Variant 2 - available applications
NIDS
IDL
BAC
eVR
EACv1
ePKI
eHIC
EAC
com.cryptovision .ePassletEAC
ePKI
com.cryptovision.applet
Bold: Configurations to be certified
Actual applets
class names

Figure 2: Available applications and actual applets in variant 2.

Combinations of certified and non-certified applications are possible (as long as these applications use one of the above applets instantiated from ROM).

Via configuration the instanciated applets can be tied to the contactless and/or the contact interface, respectively. BAC, EACv1, EACv2-SAC require exclusive access to the contactless interface. Hence, if one of these applications is used (in certified configuration), further (certified or non-certified) applications have to be bound to the contact interface.

The configuration of the TOE claimed by this Security Target is fixed after personalization. Additional applications can be instanciated as specified above from ROM only. This explicitly excludes additional applet code being loaded and installed into EEPROM.

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, and the basic cryptographic software library,
- the platform with the Java Card operation system JCOP 2.4.1R3 by NXP, in the variants
  - JxA081, A, B1, B4, Certification ID BSI-DSZ-CC-0675-2011 ([ST_JCOP081], [ZertJCOP81]) with crypto library version 2.7, Certification ID BSI-DSZ-CC-0633-2010 ([ST_CL081], [ZertCL081]) and hardware P5Cx081V1A, Certification ID BSI-DSZ-CC-0555-2009 ([ST_IC081], [ZertIC081])
  - J2A080, Certification ID BSI-DSZ-CC-0674-2011 ([ST_JCOP080], [ZertJCOP80]) with crypto library version 2.6, Certification ID BSI-DSZ-CC-0709-2010 ([ST_CL080], [ZertCL080]) and hardware P5Cx080V0B, Certification ID BSI-DSZ-CC-0410-2010 ([ST_IC080], [ZertIC080]),
  - JxA040, A, B1, B4, Certification ID BSI-DSZ-CC-0730-2011 ([ST_JCOP040], [ZertJCOP40]) with crypto library version 2.6, Certification ID BSI-DSZ-CC-0710-2010 ([ST_CL040], [ZertCL040]) and hardware P5Cx040VOB, Certification ID BSI-DSZ-CC-0404-2007 ([ST_IC040], [ZertIC040]).
- cv act ePasslet/ePKI v3.6 as the only application that has access to the contactless interface,
- the associated Administrator and User Guidance [Guidance].

The TOE's functionality claimed by this Security Target is realized by cv act ePasslet/ePKI application as part of variant 1 (see Figure 1) on P5Cx081 and of variant 2 (see Figure 2) on P5Cx080 and P5Cx040. PACE is only available in variant 1. The cv act ePasslet/ePKI application provides a PKCS#15 compliant file structure and a separate DF for the SSCD functionality (D.Sig). While D.Sig provides the TOE's functionality claimed by this Security Target, the PKCS#15 part is out of scope of the certification.

Some of the underlying platform variants of this composite TOE provide MIFARE functionality; please note that this functionality is out of scope of the TOE's security functionality claimed by this Security Target.

1.3.3 TOE functions

This paragraph is directly based on the corresponding paragraph 5.4.2 in the protection profile [PP0059].

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 digital 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 digital 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 is directly based on the corresponding paragraph 5.4.1 in the protection profile [PP0059]. It presents a functional overview of the TOE in its distinct operational environments:

- 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 digital signature.
- 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 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 digital signature created with the TOE is a qualified electronic signature as defined in [Directive][1] if the certificate for the SVD is a qualified certificate ([Directive], Annex I). Determining the state of the certificate as qualified in beyond the scope of this standard.

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.

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 digital 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 [TR03110v2] 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.
- 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.

[1] 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.

- TSF_Crypto performs high level cryptographic operations. The implementation is mainly based on the Security Functionalities provided by TSF_OS.
- TSF_SecureMessaging realizes a secure communication channel.
- TSF_Auth realizes two authentication mechanisms: PIN verification and alternatively (not on the small-mask version) 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, crypto library, Javacard operation system). Besides some minor additions, the cryptographic operations are provided by this platform:
    - Digital signature-generation(and key generation) with ECDSA and key sizes of 224-320 bit according to ISO14888-3, or with RSA and key sizes of 1976 - 2048 bit according to PKCS#1v1.5.
    - Secure messaging with Triple-DES (112 bit key length) or AES (128, 192 or 256 bit key length).

1.3.6 TOE life cycle

This paragraph is based on the corresponding paragraph 5.4.3 in 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. 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 [2]). The functional integrity of the TOE shall be protected in delivering it to an SSCD-provisioning service provider.

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 key 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 the any stored corresponding certificate info.

1.3.6.2 Preparation stage

An SSCD-provisioning service provider having accepted it 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 enables if an SCD it holds 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).[2]
- 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.

[2] 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).

- 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 (third list item above) of an SSCD-provisioning service provider as specified in this PP 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;
- The name of the signatory either
  a) A legal name, or
  b) A pseudonym together with an indication of this fact.

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
- 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 shall assert 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 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 shall 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.

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, July 2009, version 3.1 revision 3, [CC_1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, July 2009, version 3.1 revision 3, [CC_2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, July 2009, version 3.1 revision 3, [CC_3],

as follows:

- Part 2 extended,
- Part 3 conformant,
- Package conformant to EAL4 augmented with AVA_VAN.5 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 NXP P5CD chip claiming conformance to the PP [PP0035]. The hardware part of the composite evaluation is covered by the certification report [ZertIC080], [ZertIC081], [ZertIC040]. In addition, the evaluation of the TOE uses the result of the CC evaluation of the crypto library and the JCOP 2.4.1R3 Javacard OS. The Javacard OS part of the composite evaluation is covered by the certification reports [ZertJCOP080], [ZertJCOP081], [ZertJCOP040], the crypto library by the certification reports [ZertCL080], [ZertCL081], [ZertCL040].

2.2 Statement of Compatibility concerning Composite Security Target

2.2.1 Assessment of the Platform TSFs

The following Table 2 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.

Relevant Platform TSF-group	Correspondence in this ST	References/Remarks
SF.AccessControl	TSF_Access	
SF.Audit	TSF_Admin	
SF.CryptoKey	TSF_Secret	
SF.CryptoOperation	TSF_Crypto	
SF.I&A	TSF_Access	
SF.SecureManagement	TSF_Admin, TSF_Integrity	
SF.Transaction	TSF_Integrity	
SF.Hardware	TSF_OS	Implicitly used via JCOP (TSF_OS)*
SF.CryptoLib	TSF_OS	Implicitly used via JCOP (TSF_OS)*

Table 2: Relevant platform TSF-groups and their correspondence

*** Remark:** The Platform TSF-groups “SF.Hardware” and “SF.CryptoLib” are not directly used by Security Functions of the TOE, they are (implicitly) invoked by calls to the JCOP operating system, though. These OS calls are grouped in the TSF_OS.

2.2.2 Assessment of the Platform SFRs

The following Table 3 provides an assessment of all relevant Platform SFRs.

Relevant Platform SFR	Correspondence in this ST	References/Remarks
FAU: Security Audit		
FAU_ARP.1/JCS	FPT_PHP.3	Internal counter for security violations complement JCOP mechanisms
FAU_SAA.1	FPT_PHP.3	Internal counter for security violations complement JCOP mechanisms
FAU_SAS.1	No correspondence	Out of scope (managed within JCOP)
FCS: CRYPTOGRAPHIC SUPPORT		
FCS_CKM.1	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 JCOP) No contradiction to this ST
FCS_CKM.3	No correspondence	Out of scope (managed within JCOP) No contradiction to this ST
FCS_CKM.4	FCS_CKM.4	The requirement in this ST leads to the fulfillment of the platform SFR.
FCS_COP.1	FCS_COP.1/SIG	The requirement of the ST targets digital signature generation and is fulfilled by the platform SFR targeting ECDSA and RSA signature generation (FCS_COP.1/RSASignatureISO9796, FCS_COP.1/RSASignaturePKCS#1, FCS_COP.1/ECSignature)

Relevant Platform SFR	Correspondence in this ST	References/Remarks
FCS_RNG.1	FCS_RND.1	The requirement in this ST is equivalent to the platform ST.
FDP: User Data Protection		
FDP_ACC.1/CMGR	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FDP_ACC.1/SCP	No correspondence	Out of scope (JCOP memory management) No contradiction to this ST
FDP_ACC.2/FIREWALL	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FDP_ACF.1/FIREWALL	No correspondence	Out of scope (JCOP access control mechanisms) No contradiction to this ST
FDP_ACF.1/CMGR	No correspondence	Out of scope (JCOP access control mechanisms) No contradiction to this ST
FDP_ACF.1/SCP	No correspondence	Out of scope (JCOP access control mechanisms) No contradiction to this ST
FDP_ETC.1	No correspondence	Out of scope (JCOP data control mechanisms) No contradiction to this ST
FDP_IFC.1/JCVM	No correspondence	Out of scope (refers to Virtual Machine) No contradiction to this ST
FDP_IFC.1/SCP	No correspondence	No contradiction to this ST
FDP_IFF.1/JCVM	No correspondence	Out of scope (refers to Virtual Machine) No contradiction to this ST
FDP_ITC.1	No correspondence	Out of scope (JCOP data control mechanisms) No contradiction to this ST
FDP_ITT.1/SCP	No correspondence	Out of scope (platform internal data transfer) No contradiction to this ST
FDP_RIP.1	FDP_RIP.1	The platform SFR leads to fulfillment of the SFR of this ST. No contradiction.
FDP_ROL.1/FIREWALL	No correspondence	Out of scope (refers to Virtual Machine)

Relevant Platform SFR	Correspondence in this ST	References/Remarks
		No contradiction to this ST
FDP_SDI.2	No correspondence	Out of scope (JCOP internal data integrity protection) No contradiction to this ST
FIA: Identification and Authentication		
FIA_AFL.1/PIN	FIA_AFL.1	The platform SFR leads to fulfillment of the SFR of this ST. No contradiction.
FIA_AFL.1/CMGR	No correspondence	Out of scope (refers to card manager) No contradiction to this ST
FIA_ATD.1/AID	No correspondence	Out of scope (JCOP AID management) No contradiction to this ST
FIA_UAU.1	FIA_UAU.1	Different level of detail in the SFRs; no contradiction.
FIA_UAU.3/CMGR	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FIA_UAU.4/CMGR	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FIA_UID.1/CMGR	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FIA_UID.2/AID	No correspondence	Out of scope (JCOP AID management) No contradiction to this ST
FIA_USB.1	No correspondence	Out of scope (JCOP applet management) No contradiction to this ST
FMT: Security Management		
FMT_LIM.1	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FMT_LIM.2	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FMT_MSA.1/JCRE	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FMT_MSA.1/CMGR	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FMT_MSA.2/JCRE	No correspondence	Out of scope (JCOP object handling)

Relevant Platform SFR	Correspondence in this ST	References/Remarks
		No contradiction to this ST
FMT_MSA.3/FIREWALL	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FMT_MSA.3/CMGR	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FMT_MSA.3/SCP	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FMT_MTD.1/JCRE	No correspondence	Out of scope (JCOP specific roles) No contradiction to this ST
FMT_MTD.3	No correspondence	Out of scope (JCOP LF state handling) No contradiction to this ST
FMT_SMF.1	FMT_SMF.1	Fullfillment of the platform SFR is used for fulfillment of the SFR of this ST.
FMT_SMR.1/JCRE	No correspondence	Out of scope (JCOP specific roles) No contradiction to this ST
FMT_SMR.1/CMGR	No correspondence	Out of scope (JCOP specific roles) No contradiction to this ST
FPR: Privacy		
FPR_UNO.1	No correspondence	Out of scope (JCOP package separation) No contradiction to this ST
FPT: Protection of the TSF		
FPT_EMSEC.1	FPT_EMSEC.1	The SFRs are equivalent. No contradiction.
FPT_FLS.1/JCS	FPT_FLS.1	Internal countermeasures for detecting security violations complement JCOP mechanisms No contradiction to this ST
FPT_FLS.1/SCP	FPT_FLS.1	Internal countermeasures for detecting security violations complement JCOP mechanisms
FPT_ITT.1/SCP	No correspondence	Out of scope (platform internal data transfer) No contradiction to this ST
FPT_PHP.1	FPT_PHP.1	The SFRs are identical.
FPT_PHP.3/SCP	No correspondence	No contradiction to this ST
FPT_RCV.3/SCP	No correspondence	No contradiction to this ST

Relevant Platform SFR	Correspondence in this ST	References/Remarks
FPT_RCV.4/SCP	No correspondence	No contradiction to this ST
FPT_TDC.1	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FPT_TST.1	FPT_TST.1	The SFRs are equivalent. No contradiction to the ST.
FRU: Resource Utilisation		
FRU_FLT.2/SCP	No correspondence	Out of scope (JCOP internal) No contradiction to this ST
FTP: Trusted Path/Channels		
FTP_ITC.1/CMGR	No correspondence	Out of scope (JCOP internal) No contradiction to this ST

Table 3: Relevant platform SFRs and their correspondence

2.2.3 Assessment of the Platform Objectives

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

Relevant Platform Oberctive	Correspondence in this ST	References/Remarks
O.PROTECT_DATA	OT.SCD_Secrecy, OT.DTBS_Integrity_TOE	
O.SIDE_CHANNEL	OT.EMSEC_Design	
O.OS_DECEIVE	No correspondence	Out of scope No contradiction to this ST
O.FAULT_PROTECT	OT.Prot_Malfunction	
O.PHYSICAL	OT.Tamper_ID, OT.Tamper_Resistance	
O.IDENTIFICATION	OT.SCD/SVD_Gen	
O.RND	No correspondence	Out of scope No contradiction to this ST
O.SID	No correspondence	Out of scope No contradiction to this ST
O.MF_FW	No correspondence	Out of scope No contradiction to this ST
O.OPERATE	No correspondence	Out of scope No contradiction to this ST
O.RESOURCES	No correspondence	Out of scope No contradiction to this ST
O.FIREWALL	No correspondence	Out of scope No contradiction to this ST

Relevant Platform Oberctive	Correspondence in this ST	References/Remarks
O.REALLOCATION	No correspondence	Out of scope No contradiction to this ST
O.SHRD_VAR_CONFID	No correspondence	Out of scope No contradiction to this ST
O.SHRD_VAR_INTEG	No correspondence	Out of scope No contradiction to this ST
O.ALARM	No correspondence	Out of scope No contradiction to this ST
O.TRANSACTION	No correspondence	Out of scope No contradiction to this ST
O.CIPHER	No correspondence	Out of scope No contradiction to this ST
O.PIN-MNGT	No correspondence	Out of scope No contradiction to this ST
O.KEY-MNGT	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.RECOVERY	No correspondence	Out of scope No contradiction to this ST
O.SCP.SUPPORT	No correspondence	Out of scope No contradiction to this ST
O.SCP.IC	No correspondence	Out of scope No contradiction to this ST

Table 4: Relevant platform objectives and their correspondence

2.2.4 Assessment of Platform Threats

The following Table 5 provides an assessment of all relevant Platform objectives.

Relevant Platform Oberctive	Correspondence in this ST	References/Remarks
T.ACCESS_DATA	T.SCD_Divulg, T.SCD_Derive	
T.OS_OPERATE	No correspondence	Out of scope No contradiction to this ST
T.OS_DECEIVE	No correspondence	Out of scope No contradiction to this ST
T.LEAKAGE	T.SCD_Divulg, T.SCD_Derive	
T.FAULT	T.SigF_Misuse	
T.RND	No correspondence	Out of scope

Relevant Platform Oberctive	Correspondence in this ST	References/Remarks
		No contradiction to this ST
T.PHYSICAL	T.Hack_Phys	
T.CONFID-JCSCODE	No correspondence	Out of scope No contradiction to this ST
T.CONFIDAPPLI-DATA	No correspondence	Out of scope No contradiction to this ST
T.CONFID-JCSDATA	No correspondence	Out of scope No contradiction to this ST
T.INTEG-APPLICODE	No correspondence	Out of scope No contradiction to this ST
T.INTEG-JCSCODE	No correspondence	Out of scope No contradiction to this ST
T.INTEG-APPLIDATA	T.DTBS_Forgery, T.Sig_Forgery	
T.INTEG-JCSDATA	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.RESOURCES	No correspondence	Out of scope No contradiction to this ST

Table 5: Relevant platform threats and their correspondence

2.2.5 Assessment of Platform Organisational Security Policies

The platform ST contains only the Organisational Security Policy “OSP.PROCESS-TOE” referring to accurate identification of each TOE instance. This policy will be fulfilled by a distinct product code for the platform and for the composite TOE each. 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 significant assumptions of the Platform ST. The last column provides an explanation of relevance for the Composite TOE.

Significant Platform Assumption	Relevance for Composite ST
A.USE_DIAG	A.USE_DIAG is required in the Platform ST to cover secure communication. There is no corresponding assumption in the Composite ST. Secure communication is enforced by TSF_Access and hence supports this assumption directly.

Table 6: Assessment of platform assumptions.

2.2.6.2 Assessment of Platform Security Objectives and SFRs for the Operational Environment

There are no significant Platform Security Objectives and no Platform SFRs for the Operational Environment to be considered.

3 Security problem definition

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

3.1 General

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

Assets and objects:

1. SCD: private key used to perform a digital 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 digital 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 digital signature must be maintained.
4. Signature-creation function of the TOE to create digital signature for the DTBS/R with the SCD.

User and subjects acting for users:

1. User: End user of the TOE who can be identified as Administrator or Signatory. In the TOE 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. In the TOE the subject S.Admin is acting in the role R.Admin for this user after successful authentication as Administrator.
3. Signatory: User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents. In the TOE the subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.

Threat agents:

1. Attacker as being a human or process acting on his behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the digital signature. An attacker has 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 presents a forged SVD 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 digital signature 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 digital signature

Without use of the SCD an attacker forges data with associated digital signature and the verification of the digital signature by the SVD does not detect the forgery. The signature generated 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 digital signature created with a SCD implemented in the SSCD that the signatory maintain under his 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 digital 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 his un-revoked certificate.

3.4 Assumptions

3.4.1 A.CGA: Trustworthy certification-generation application

The CGA protects the authenticity of the signatory's name or pseudonym and the SVD in the (qualified) certificate by 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 provide functionality to securely destroy the SCD.

PP application note 1: The TOE may contain more than one SCD. There is no need to destroy the SCD in case of re-generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after expiration of the (qualified) certificate for the corresponding SVD.

4.2.2 OT.SCD/SVD_Gen: SCD/SVD generation

The TOE provides security features to ensure that authorised users only 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 can practically occur only once and cannot be reconstructed 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 a digital signature creation with the SCD.

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

The secrecy of an SCD (used for signature creation) is 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 signing operation, storage and by destruction.

4.2.6 OT.Sig_Secure: Cryptographic security of the digital signature

The TOE generates digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the digital signatures or any other data exported 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 provides the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others to create a digital signature. 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 This objective does not conflict with a signature-creation process where the TOE applies a cryptographic hash function on the DTBS/R to prepare for signature creation algorithm.

4.2.9 OT.EMSEC_Design: Provide physical-emanation security

Design and build the TOE 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 provides 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 prevents or resists 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 ensures the integrity of the SVD exported by the TOE to the CGA. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

4.3.2 OE.CGA_QCert: Generation of qualified certificates

The CGA generates a qualified certificate that includes, inter alias

- the name of the signatory controlling the TOE,
- the SVD matching the SCD stored in the TOE and controlled by the signatory,
- the advanced signature of the CSP.

The CGA confirms with the generated 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 handles authentic devices that implement the TOE to be prepared for the legitimate user as signatory personalises and delivers the TOE 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 will 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.

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

The Signatory uses 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.

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

The operational environment ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE.

4.3.7 OE.Signatory: Security obligation of the Signatory

The Signatory checks that the SCD stored in the SSCD received from SSCD provisioning service is in non-operational state. The Signatory keeps his or her SVAD 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_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													
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						

	OT.Lifecycle_Security	OT.SCD/SVD_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
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 7: Mapping of threats, policies and assumptions to the security objectives.

4.4.2 Security Objectives Sufficiency

4.4.2.1 Policies and Security Objective Sufficiency

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

- the TOE security objective OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- the TOE security objective OT.SCD_SVD_Corresp, which requires the TOE to ensure the correspondence between the SVD and the SCD during their generation, and
- the security objective for the operational environment 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 generation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE generates digital signatures that 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. The 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 generation 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 [Directive], Annex III by the requirements to ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE;
- OT.Sigy_SigF meets the requirement in paragraph 1(c) of [Directive], Annex III by the requirements to ensure that the TOE provides the signature generation 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 [Directive], 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_Gen, which limits invoke the generation of the SCD and the SVD to authorised users only,
- OT.Sigy_SigF, which requires the TOE to provide the signature generation 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 a TOE sample as an authentic, 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 his 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 ensure the aspects of signatory's sole control over and responsibility for the digital signatures generated with the TOE. OE.SSCD_Prov_Service ensures that the signatory uses an authentic TOE, initialised and personalised for the signatory. OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure 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 his or her SVAD confidential. OE.DTBS_Intend, OE.DTBS_Protect and OT.DTBS_Integrity_TOE ensure that the TOE generates digital signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may generate a valid digital signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

4.4.2.2 Threats and Security Objective Sufficiency

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_Gen counters this threat by implementing cryptographic secure generation of the SCD/SVD-pair. OT.Sig_Secure ensures cryptographic secure digital 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 to generation a certificate. 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 a digital 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-generation 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 his or her SVAD 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 can not 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 digital signature) deals with non-detectable forgery of the digital signature. OT.Sig_Secure, OT.SCD_Unique and OE.CGA_Qcert address this threat in general. The OT.Sig_Secure (Cryptographic security of the digital signature) ensures by means of robust cryptographic techniques that the signed data and the digital signature are securely linked together. OT.SCD_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_Qcert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision on a forged signature.

4.4.2.3 Assumptions and Security Objective Sufficiency

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 for the data that has been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

A.CGA (Trustworthy certification-generation application) establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert (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 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_EMSEC

The additional family FPT_EMSEC (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_EMSEC 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_EMSEC is taken from the Protection Profile Secure Signature Creation Device [PP0006], chapter 6.6.1

5.1.1 FPT_EMSEC TOE Emanation

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC.1 TOE Emanation has two constituents:

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

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

FPT_EMSEC.1: TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.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_EMSEC.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 5 describes the extended component FPT_EMSEC.1. 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 3: 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:

- **ECDSA key generation* or RSA CRT key generation** [3]

and specified cryptographic key sizes:

- **224 - 320 bit or 1976 - 2048 bit** [4]

that meet the following:

- **ANSI X9.62 or PKCS#1v1.5**[5, 6]

[3] [assignment: cryptographic key generation algorithm]

[4] [assignment: cryptographic key sizes]

PP application note 4: <applied>

***Remark:** For ECDSA key generation please also note the remark in the JCOP user guidance manual [JCOP_UGM], section 2.2.1 on EC domain parameters.

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 value with zero values**[7] that meets the following: **none**[8]**.**

PP application note 5: <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-generation*** in accordance with a specified cryptographic algorithm

- **ECDSA* or RSA (straight and CRT variant) without internal hash calculation, with SHA-224 or SHA-256**[9]

and specified cryptographic key sizes:

- **224 – 320 bit or 1976 – 2048 bit** [10]

that meet the following:

- **ISO14888-3, section 6.4 or PKCS#1v1.5, sections 5.1.1 and 5.1.2 and FIPS 180-4**[11, 12]

[5] [assignment: list of standards]

[6] 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.

[7] [assignment: cryptographic key destruction method]

[8] [assignment: list of standards]

[9] [assignment: cryptographic algorithm]

[10] [assignment: cryptographic key sizes]

[11] [assignment: list of standards]

PP application note 6: <applied>

***Remark:** For ECDSA signature operation please also note the remark in the JCOP user guidance manual [JCOP_UGM], section 2.2.1 on EC domain parameters.

The following SFR is only required for variant 1 (cf. section 1.3) 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:

- **224 – 320 bit**

that meet the following:

- **BSI-TR-03110 [TR03110v2], section 4.2.**

Application note: It must be underlined that the SFR FCS_COP.1/PACE SFR is only required for variant 1 (cf. section 1.3) with a contactless interface.

***Remark:** For PACE operation please also note the remark in the JCOP user guidance manual [JCOP_UGM], section 2.2.1 on EC domain parameters.

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 K3 quality metric**[13]**.**

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 JCOP platform.

[12] 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.

[13] [assignment: a defined quality metric]

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 – S.User acts as S.Admin R.Sigy – S.User acts as S.Sigy
S.User	SCD / SVD Management	Authorised, not authorised
SCD	SCD Operational	No, yes
SCD	SCD identifier	Arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

Table 8: Security attributes and related status.

PP application note 7: <not applicable>

6.2.3.1 FDP_ACC.1/SCD/SVD_Generation_SFP: Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SCD/SVD_Generation_SFP

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_SFP: 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_ SFP

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_ SFP

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_SFP

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

FDP_ACF.1.4/ SCD/SVD_Generation_SFP

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_SFP Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SVD_Transfer_SFP

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_SFP: 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_SFP

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_SFP

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**[14] ***is allowed to export SVD.***

FDP_ACF.1.3/ SVD_Transfer_SFP

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

FDP_ACF.1.4/ SVD_Transfer_SFP

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

PP application note 8: <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 EN14169-3 "Protection Profiles for Secure signature creation device – Part 3: Device

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

with key generation and trusted channel between SSCD and CGA" 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_SFP: Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Signature-creation_SFP

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_SFP: Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Signature-creation_SFP

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_SFP

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 digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes".

FDP_ACF.1.3/Signature-creation_SFP

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

FDP_ACF.1.4/Signature-creation_SFP

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

S.User is not allowed to create digital 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 9: 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**[15]

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 10: <applied>

6.2.4.2 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1

The TSF shall allow

(1) ***Self test according to FPT_TST.1,***

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

(3) **Receiving DTBS**[16]

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 11: <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**[17] 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 12: <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.

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

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

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

6.2.5 Security management (FMT)

6.2.5.1 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1

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

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.5.2 FMT_SMF.1 Security management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1

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) <u>none</u>[18]

PP application note 13: <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***.

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

6.2.5.5 FMT_MSA.1/Signatory Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Signatory

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

6.2.5.6 FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
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 14: <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 15: 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 16: 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_EMSEC.1 TOE Emanation

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

FPT_EMSEC.1.1

The TOE shall not emit **variations in power consumption or timing during command execution**[19] in excess of **non-useful information**[20] enabling access to ***RAD*** and ***SCD***.

FPT_EMSEC.1.2

The TSF shall ensure **any users**[21] are unable to use the following interface: **smart card circuit contacts or contactless interface**[22] to gain access to ***RAD*** and ***SCD***.

PP application note 17: 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

[19] [assignment: types of emissions]

[20] [assignment: specified limits]

[21] [assignment: type of users]

[22] [assignment: type of connection]

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

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

(1) Self-test according to FPT_TST fails,

(2) <u>none</u>[23]

PP application note 18: <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 **<u>physical manipulation and physical probing</u>**[24] to the **<u>security IC</u>**[25] by responding automatically such that the SFRs are always enforced.

PP application note 19: 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.

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

[24] [assignment: physical tampering scenarios]

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

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.

FPT_TST.1.1

The TSF shall run a suite of self-tests **during initial start-up**[26] 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 20: <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.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage

[26] [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
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 9: Assurance Requirements: EAL4 augmented with AVA_VAN.5.

6.4 Rationale

6.4.1 Security Requirements Rationale

6.4.1.1 Security Requirement Coverage

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.1	x		x	x	x						
FCS_CKM.4	x				x						
FCS_COP.1/SIG	x					x					
FCS_COP.1/PACE							x				

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_RND.1							x				
FDP_ACC.1/ SCD/SVD_Generation_SFP	x	x									
FDP_ACC.1/ SVD_Transfer_SFP	x										
FDP_ACC.1/Signature-creation_SFP	x						x				
FDP_AFC.1/ SCD/SVD_Generation_SFP	x	x									
FDP_AFC.1/ SVD_Transfer_SFP	x										
FDP_AFC.1/Signature-creation_SFP	x						x				
FDP_RIP.1					x		x				
FDP_SDI.2/Persistent				x	x	x					
FDP_SDI.2/DTBS							x	x			
FIA_AFL.1							x				
FIA_UAU.1		x					x				
FIA_UID.1		x					x				
FMT_MOF.1	x						x				
FMT_MSA.1/Admin	x	x									
FMT_MSA.1/Signatory	x						x				
FMT_MSA.2	x	x					x				
FMT_MSA.3	x	x					x				
FMT_MSA.4	x	x					x				
FMT_MTD.1/Admin	x						x				
FMT_MTD.1/Signatory	x						x				
FMT_SMR.1	x						x				
FMT_SMF.1	x						x				
FPT_EMSEC.1					x				x		
FPT_FLS.1					x						
FPT_PHP.1										x	
FPT_PHP.3					x						x
FPT_TST.1	x				x	x					

Table 10: 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_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer_SFP and FDP_ACF.1/SVD_Transfer_SFP. The SCD usage is ensured by access control FDP_ACC.1/Signature-creation_SFP, FDP_AFC.1/Signature-creation_SFP 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_Gen (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_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP 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_EMSEC.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 digital 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_SFP and FDP_ACF.1/Signature-creation_SFP 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 variant 1 (cf. section 1.3) 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_EMSEC.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/RSA and FCS_CKM.1/ECDSA
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 juistification No. 1 for non-satisfied dependencies
FCS_RND.1	No dependencies	n. a.
FDP_ACC.1/ SCD/SVD_Generation_SFP	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation_SFP
FDP_ACC.1/ Signature-creation_SFP	FDP_ACF.1	FDP_ACF.1/Signature-Creation_SFP
FDP_ACC.1/ SVD_Transfer_SFP	FDP_ACF.1	FDP_ACF.1/SVD_Transfer_SFP
FDP_ACF.1/	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation_SFP

Requirement	Dependencies	Fulfilled
SCD/SVD_Generation_SFP		, FMT_MSA.3
FDP_ACF.1/ Signature-creation_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature-creation_SFP, FMT_MSA.3
FDP_ACF.1/ SVD_Transfer_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer_SFP, FMT_MSA.3
FDR_RIP.1	No dependencies	n. a.
FDP_SDI.2/Persistent	No dependencies	n. a.
FDP_SDI.2/DTBS	No dependencies	n. a.
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/ Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation_SFP, 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_SFP, 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_SFP, FDP_ACC.1/ Signature-creation_SFP
FMT_MTD.1/ Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/ Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No dependencies	n. a.
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_FLS.1	No dependencies	n. a.
FPT_PHP.1	No dependencies	n. a.
FPT_PHP.3	No dependencies	n. a.
FPT_TST.1	No dependencies	n. a.

Table 11: Functional Requirements Dependencies.

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

- No. 1: The PACE authentication protocol uses the RAD (e.g. the 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 4 Augmented

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

AVA_VAN.5 Advanced methodical vulnerability analysis

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

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. 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 EAL4 assurance package.

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 Phase 2 – while the actual applet is not yet present – is based on the card manager of the underlying JCOP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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 digital 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_SFP 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_SFP 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 digital 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, (3) erstablishing a trusted secure messaging channel be-tween the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD, and (4) 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 Phase 2 – while the actual applet is not yet present – is based on the card manager of the underlying JCOP Java Card platform (SF.SecureManagement); also Audit functionality is based on JCOP 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 JCOP 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 key generation with key sizes of 224-320 bit according to ANSI X9.62, or RSA key generation with key sizes of 1976 – 2048 bit according to PKCS#1v1.5. 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 variant 1 (cf. section 1.3) and use of the contactless interface the TOE must provide the PACE authentication protocol. This is covered by TSF_Crypto which itself is realized by TSF_OS.
- FCS_COP.1.1/SIG requires that the TSF shall perform digital signature-generation in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes: ECDSA key generation with key sizes of 224-320 bit according to ANSI X9.62, or RSA key generation with key sizes of 1976 – 2048 bit according to PKCS#1v1.5. This is covered by TSF_Crypto which itself is 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, (3) erstablishing a trusted secure messaging channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD, and (4) 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 [TR03110v2]. It is used for secure PIN entry especially over contactless interface. To prevent denial ove service attacks on the PACE PIN (that could be performed unnoticed via contactless interface), the suspend mode as defined in TR03110 [TR03110v2] is used. After two consecutive unseccussul 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 variant 1 (cf. section 1.3) and use of the contactless interface the TOE must provide the PACE authentication protocol.
- FDP_ACC.1.1/SCD/SVD_Generation_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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_SFP 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 digital 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_SFP 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_SFP 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 digital 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, (3) erstablishing a trusted secure messaging channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD, and (4) 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_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 JCOP Java Card OS (cf. the according security targets [ST_JCOP080], [ST_JCOP081], [ST_JCOP040]).

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 targets [ST_JCOP080], [ST_JCOP081], [ST_JCOP040]; the realization is partly based on the security functions of the certified cryptographic library and 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: ECDSA key generation with key sizes of 224-320 bit according to ANSI X9.62, or RSA key generation with key sizes of 1976 – 2048 bit according to PKCS#1v1.5. 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). The only exceptions are the CMAC Sub-Keys (for Secure Messaging), where the security function is provided by TSF_Crypto.
- FCS_COP.1.1/SIG requires that the TSF shall perform digital signature-generation in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes: ECDSA key generation with key sizes of 224-320 bit according to ANSI X9.62, or RSA key generation with key sizes of 1976 – 2048 bit according to PKCS#1v1.5. This is realized by TSF_OS, which itself is partly based on TSF_CryptoLib and TSF_Hardware. TSF_OS provides the basic cryptographic mechanisms.
- 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_EMSEC.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_EMSEC.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 during initial start-up 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_Hardware.
- 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_Hardware.

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_SFP	x					x		
FDP_ACC.1/SVD_Transfer_SFP	x					x		
FDP_ACC.1/Signature-creation_SFP	x					x		
FDP_AFC.1/SCD/SVD_Generation_SFP	x					x		
FDP_AFC.1/SVD_Transfer_SFP	x					x		
FDP_AFC.1/Signature-creation_SFP	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								
FMT_MSA.3		x						

	TSF_Access	TSF_Admin	TSF_Secret	TSF_Crypto	TSF_SecureMessaging	TSF_Auth	TSF_Integrity	TSF_OS
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_EMSEC.1								x
FPT_FLS.1								x
FPT_PHP.1							x	x
FPT_PHP.3								x
FPT_TST.1								x

Table 12: 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 3, July 2009; CCMB-2009-07-001.
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 3, July 2009; CCMB-2009-07-002.
[CC_3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 3, July 2009; CCMB-2009-07-003.
[CC_4]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009

Protection Profiles

[PP0059]	Protection profiles for Secure signature creation device – Part 2: Device with key generation; prEN 14169-1:2009, CEN/TC 224, December 2009
[PP0002]	PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001
[PP0035]	Security IC Platform Protection Profile, Version 1.0, June 2007; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007
[PP_Javacard]	Java Card System – Minimal Configuration Protection Profile, Version 1.1, May 2006, part of: Java Card Protection Profile Collection, Version 1.1, May 2006
[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

TOE and Platform References

[Guidance]	cv act ePasslet/ePKI – cv act ePasslet Suite Java Card applet for PKI applications, Secure Signature Creation Device (SSCD) Configuration, Guidance Manual, Version 1.0.1; cryptovision, June 2012
[ZertIC040]	Certification Report BSI-DSZ-CC-0404-2007 for NXP Secure Smart Card Controller P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B each with specific IC Dedicated Software from NXP Semiconductors Germany GmbH Business Line Identification; BSI, July 2007.
[ZertIC080]	Certification Report BSI-DSZ-CC-0410-2007 for NXP Secure Smart Card Con-troller P5CD080V0B, P5CN080V0B and P5CC080V0B, each with specific IC Dedicated Software from NXP Semiconductors Germany GmbH; BSI, July 2007.
[ZertIC081]	Certification Report BSI-DSZ-CC-0555-2009 for NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A, each with IC dedicated Software from NXP Semi-

	conductors Germany GmbH Business Line Identification; BSI, November 2009.
[ZertJCOP040]	Certification Report BSI-DSZ-CC-0730-2011 for NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH; BSI, May 2011.
[ZertJCOP080]	Certification Report BSI-DSZ-CC-0674-2011 for NXP J3A080 and J2A080 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH; BSI, March 2011.
[ZertJCOP081]	Certification Report BSI-DSZ-CC-0675-2011 for NXP J3A081, J2A081 and J3A041 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH; BSI, April 2011.
[ZertCL040]	Certification Report BSI-DSZ-CC-0710-2010 for Crypto Library V2.6 on P5CD040V0B /P5CC040V0B / P5CD020V0B / P5CC021V0B /P5CD012V0B from NXP Semiconductors Germany GmbH; BSI, January 2011.
[ZertCL080]	Certification Report BSI-DSZ-CC-0709-2010 for Crypto Library V2.6 on P5CD080V0B /P5CN080V0B / P5CC080V0B / P5CC073V0B from NXP Semiconductors Germany GmbH; BSI, December 2010.
[ZertCL081]	Certification Report BSI-DSZ-CC-0633-2010 for Crypto Library V2.7 on P5CD081V1A /P5CC081V1A / P5CN081V1A / P5CD041V1A /P5CD021V1A / P5CD016V1A from NXP Semiconductors Germany GmbH; BSI, November 2010.
[ST_JCOP040]	Security Target Lite „NXP J3A040 and J2A040 Secure Smart Card Controller Rev. 3“, Rev. 01.03; NXP, 13 May 2011.
[ST_JCOP080]	Security Target Lite „NXP J3A080 and J2A080 Secure Smart Card Controller Rev. 3“, Rev. 01.02; NXP, December 2010.
[ST_JCOP081]	Security Target Lite „NXP J3A081, J2A081 and J3A041 Secure Smart Card Controller Rev. 3“, Rev. 01.02; NXP, December 2010.
[ST_CL040]	Security Target Lite “Crypto Library V2.6 on P5CD040V0B / P5CC040V0B / P5CD020V0B / P5CC021V0B / P5CD012V0B”, Rev. 2.4; NXP, 14 December 2010.
[ST_CL080]	Security Target Lite “Crypto Library V2.6 on P5CD080V0B / P5CN080V0B / P5CC080V0B / P5CC073V0B”, NXP, Rev. 2.3; NXP, 12 November 2010.
[ST_CL081]	Security Target Lite “Crypto Library V2.7 on P5CD081V1A / P5CC081V1A / P5CN081V1A / P5CD041V1A / P5CD021V1A / P5CD016V1A”, NXP, Rev. 1.2; 9 November 2010.
[ST_IC040]	Security Target Lite “P5CD040/P5CC040/P5CD020/P5CC021 V0B”, Rev. 1.0, NXP, 21 March 2007.
[ST_IC080]	Security Target Lite “P5CD080/P5CN080/P5CC080 V0B”, Rev. 1.0, NXP, 21 March 2007.
[ST_IC081]	Security Target Lite “NXP Secure Smart Card Controllers P5CD016/021/041V1A and P5Cx081V1A”, Rev. 1.3, NXP, 21 September 2009.
[JCOP_UGM]	NXP JCOP V2.4.1 Revision 3 secure smart card controller, Rev. 3.0--9 March 2011 – User manual, Doc No. 188830

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

[TR-03110v2]	Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 2.05, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI), November 2010.
[EuCC]	Identification card systems – European Citizen Card – Part 2: Logical data structures and card services, CEN/TS 15480-2:2007
[ISO7816-4]	ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004
[AIS20]	Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20; Bundesamt für Sicherheit in der Informationstechnik, Version 2.1, 2.12.2011
[AIS31]	Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik
[ISO14888-3]	ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999
[FIPS46-3]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Techn logy
[NIST800-20]	NIST Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm, US Department of Commerce, October 1999
[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
[FIPS186-2]	Federal Information Processing Standards Publication 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1
[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
[ANSIX9.19]	ANSI X9.19, AMERICAN NATIONAL STANDARD, Financial Institution Retail Message Authentication, 1996
[ANSIX9.62]	AMERICAN NATIONAL STANDARD X9.62-1999: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©, September 20, 1998
[ISO9796-2]	ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002
[ISO15946-1]	ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002.
[ISO15946-2]	ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.
[ISO15946-3]	ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002
[PKCS3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993

[NIST800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, May 2005
[RFC4493]	Request for Comments: 4493, The AES-CMAC Algorithm, JH. Song et al. University of Washington, Category: Informational, June 2006
[Gixel]	EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS, IAS ECC Identification Authentication Signature – European Citizen Card, Technical Specifications, Revision: 1.0.1, GIXEL, 21.03.2008
[PKCS#1]	PKCS #1: RSA Encryption Standard – An RSA Laboratories Technical Note Version 1.5, Revised November 1, 1993

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 Digital signature which meets specific requirements in [Directive]. According to the Directive a digital signature qualifies as an electronic signature if it:

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

Authentication data Information used to verify the claimed identity of a user

Authentication Authentication defines a procedure that verifies the identity of the communication partner. The most elegant method is based on the use of so called digital signatures.

CA Certification authority.

CC Common criteria.

Certificate Digital 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 digital 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 Data received by a secure signature creation device as input in a single signature-creation operation. Note: DTBS/R is either

DTBS/R

- a hash-value of the data to be signed (DTBS), or
- an intermediate hash-value of a first part of the DTBS complemented with a remaining part of the DTBS, or
- the DTBS.

DTBS Data to be signed.

DTBS/R Data to be signed or its unique representation.

EAL Evaluation assurance level.

ECC (Elliptic Curve Cryptography) class of procedures providing an attractive alternative for the probably most popular asymmetric procedure, the RSA algorithm.

Hash function A function which forms the fixed-size result (the hash value) from an arbitrary amount of data (which is the input). These functions are used to generate the electronic equivalent of a fingerprint. The significant factor is that it must be impossible to generate two entries which lead to the same hash value (so called collisions) or even to generate a matching message for a defined hash value.

Integrity The test on the integrity of data is carried out by checking messages for changes during the transmission by the receiver. Common test procedures employ Hashfunctions, MACs (Message Authentication Codes) or – with additional functionality – digital 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 digital 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 digital signatures.

Public key infrastructure (PKI) Combination of hardware and software components, policies, and different procedures used to manage digital 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 PP ([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 sys- Complete system that creates an electronic signature consists of the SCA and

tem (SCS) 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) 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.