MORPHO

SECURITY TARGET LITE
FOR
ID.ME ON IDEAL CITIZ V2.1

Reference: 2016_2000019402

Table of contents

Table of figures

Table of tables

1 TOE Overview

This document is the Security Target Lite for the ID.me Applet on IdealCitiz Platform which is a MORPHO specific Java Card implementation of the Identification Authentication Signature for European Citizen Card v1.0.1 [IAS ECC].

ID.me is designed to be compliant with the IAS ECC v1.0.1 specification [IAS ECC], taking into account the addendum [IAS ADD].

The TOE addressed by the current ST is a SSCD device with PACE Authentication that may:

1) generate signing keys internally [PP-SSCD2],
2) import signing keys [PP-SSCD3]
3) export the public key in protected manner: SSCD with key generation and trusted communication with CGA [PP-SSCD4]
4) communicate with the SCA in protected manner: SSCD with key generation and key import, and trusted communication with SCA [PP-SSCD5] and [PPSSCD6].

The ID.me applet is a set of Java card services intended to be used exclusively on the IdealCitiz v2.1 Java card Platform, which is certified according to CC EAL 5+ [ST-PL]. The IdealCitiz v2.1 Java card Platform is based on the Infineon M7892 B11 IC security controller, which is itself certified according to CC EAL 5+ [ST-IC].

This ST has been conceived to prepare a Common Criteria evaluation following the "compositional approach" described in [COMP]. This approach consists in starting from a Platform that has been independently certified, and performing an evaluation of the product resulting from embedding an Application into it, which makes use of some of the results issued from the evaluation of the IdealCitiz Java card Platform.

This document provides a list of security requirements for the ID.me Applet embedded in a Java Card platform.

This Security Target describes:

- The Target of Evaluation (TOE)
- The assets to be protected, the threats (T) to be countered by the TOE itself during the usage of the TOE,
- The organizational security policies (OSP), and the assumptions (A),
- The security objectives (OT) for the TOE and its environment (OE),
- The security functional requirements (SFR) for the TOE and its IT environment,
- The TOE security assurance requirements (SAR).

The assurance level for the TOE is CC EAL5+.

1.1 ST Identification

Title	Security Target Lite for ID.me on IDeal Citiz v2.1
Reference	2016_2000019402
Version	1.0
Certification Body	ANSSI
Author	MORPHO
CC Version	3.1 Revision 4
Assurance Level	EAL5 augmented with ALC_DVS.2 and AVA_VAN.5
Protection Profiles	PP SSCD-Part 2 Key Generation [PP-SSCD2], PP SSCD-Part 3 Key Import [PP-SSCD3], PP SSCD-Part 4 Key Generation and Trusted Channel with CGA [PP-SSCD4] PP SSCD-Part 5 Key Generation and Trusted Channel with SGA [PP-SSCD5] PP SSCD-Part 6 Key Import and Trusted Channel with SGA [PP-SSCD6]

1.2 TOE Reference

TOE name	ID.me Applet on IDeal Citiz v2.1
TOE version number	1.12
Name of Platform	IDealCitiz v2.1 open platform
IC Identifiers	Infineon M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)

1.3 TOE documentation

TOE documentation is described in the table below:

Reference	Description
[AGD_PRE]	2014_2000002907 – ID.me – AGD_PRE
[AGD_OPE]	2014_2000002909 – ID.me – AGD_OPE
[AGD_USR]	2014_2000000211 - ID.me - Applet User Manual
[AGD_ADM]	2014_0000001563 - ID.me - Application Personalization Specification

2 Technical terms, Abbreviation and Associated references

2.1 Technical terms

Term	Definition
Application note	*Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.*
Administrator	*user who performs TOE initialization, TOE personalization, or other TOE administrative functions*
Advanced electronic signature	*An electronic signature which meets the following requirements [DIRECTIVE]:* *(i) it is uniquely linked to the signatory,* *(ii) it is capable of identifying the signatory,* *(iii) it is created using means that the signatory can maintain under his sole control,* *(iv) it 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.*
Card Access Number (CAN)	*A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Identification Card), semi-static (e.g. printed on a label on the Identification Card) or dynamic (randomly chosen by the Card and displayed by it using e.g. ePaper, OLED or similar technologies), see [D03110], sec. 3.3*
Certificate	*digital signature used as electronic attestation binding signature-verification data to a person confirming the identity of that person as legitimate signer*
Certificate info	*information associated with an SCD/SVD pair that may be stored in a secure signature creation device* *NOTE 1: 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.* *NOTE 2: Certificate info may contain 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*

Term	Definition
Certification service provider (CSP)	*entity that issues certificates or provides other services related to electronic signatures*
Data to be signed (DTBS)	*all of the electronic data to be signed including a user message and signature attributes*
Data to be signed or its unique representation (DTBS/R)	*data received by a secure signature creation device as input in a single signature creation operation* *NOTE: Examples of DTBS/R are* - *a hash value of the data to be signed (DTBS), or* - *an intermediate hash value of a first part of the DTBS complemented with a remaining part of the DTBS, or* - *the DTBS.*
ECC	*(Elliptic Curve Cryptography) class of procedures providing an attractive alternative for the probably most popular asymmetric procedure, the RSA algorithm.*
Hash function	*A function which forms the fixed-size result (the hash value) from an arbitrary amount of data (which is the input). These functions are used to generate the electronic equivalent of a fingerprint. The significant factor is that it must be impossible to generate two entries which lead to the same hash value (so called collisions) or even to generate a matching message for a defined hash value.*
Integrity	*The test on the integrity of data is carried out by checking messages for changes during the transmission by the receiver. Common test procedures employ Hash functions, MACs (Message Authentication Codes) or – with additional functionality – digital signatures.*
Javacard	*A smart card with a Javacard operation system.*
Legitimate user	*An user of a secure signature creation device who gains possession of it from an SSCD provisioning service provider and who may 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.*
Notified body	*An organizational entity designated by a member state of the European Union as responsible for accreditation and supervision of the evaluation process for products conforming to [PP-SSCD2], [PP-SSCD5] and for determining admissible algorithms and algorithm parameters.*
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.*

Term	Definition
PACE Terminal (PCT)	*A technical system verifying correspondence between the stored password and the related value presented to the terminal. PCT implements the terminal's part of the PACE protocol and authenticates itself to the Card using a shared password (CAN, PIN or PUK). The PCT is not allowed reading User Data (see sec. 4.2.2 in [D03110]).* *See [D03110], chap. 3.3, 4.2, table 1.2 and G.2.*
Password Authenticated Connection Establishment (PACE)	*A communication establishment protocol defined in [D03110], sec. 4.2. The PACE Protocol is a password authenticated DiffieHellman key agreement protocol providing implicit password based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.*
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 Annex I and that is provided by a CSP that fulfils the requirements laid down in Annex II (the directive: 2.10) [DIRECTIVE]*
Qualified electronic signature	*advanced electronic signature that has been created with an SSCD with a key certified with a qualified certificate ([DIRECTIVE]: 5.1).*
Random numbers	*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 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.*
Secure messaging	*Secure messaging using encryption and message authentication code ac-cording to ISO/IEC 7816-4.*
Secure signature creation 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).*

Term	Definition
Signatory	*legitimate user of an SSCD associated with it in the certificate of the signature-verification data and who is authorized by the SSCD to operate the signature-creation function*
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 in-tent 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*
Signature creation system (SCS)	*complete system that creates an electronic signature consisting of an SCA and an SSCD*
Signature verification data (SVD)	*public cryptographic key that can be used to verify an electronic signature*
Signed data object	*The electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.*
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). There-fore, such a smart card is ideal for use in cryptography as it is almost impossible to manipulate its internal processes.*
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*
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*
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*

2.2 Abbreviation

Acronym	Definition
ADF	*Application Dedicated File*
CA	*Certification authority*
CAD	*card acceptance device*
CAN	*Card Access Number*
CC	*Common Criteria*
CGA	*Certification generation application*
CPU	*Central Processing Unit*
CSP	*certification service provider*
DPA	*differential power analysis*
DTBS	*Data to be signed*
DTBS/R	*Data to be signed or its unique representation*
EAL	*Evaluation assurance level*
ECC	*Elliptic Curve Cryptography*
EEPROM	*electrically erasable programmable read only memory*
GP	*GlobalPlatform*
HID	*human interface device*
IT	*Information technology*
JCVM	*java card virtual machine*
MAC	*Message Authentication Code*
MPU	*Memory Protection Unit*
NVM	*Non Volatile Memory*
OID	*object identifier*
OS	*Operating System*
OSP	*Organizational security policy*
PACE	*Password Authenticated Connection Establishment*
PIN	*Personal Identification Number*
PP	*Protection profile*
PUK	*PIN Unblocked Key*
RAD	*Reference authentication data*
RAM	*random access memory*
RF	*Radio Frequency*
RNG	*random number generation*
ROM	*read only memory*
SAR	*Security Assurance Requirements*
SCA	*Signature creation application*

Acronym	Definition
SCD	*Signature creation data*
SCS	*Signature creation system*
SDO	*Security data object*
SF	*security function*
SFP	*Security function policy*
SFR	*Security functional requirement*
SPA	*simple power analysis*
SSCD	*Secure signature creation device*
ST	*Security target*
SVD	*Signature verification data*
TOE	*Target of evaluation*
TSF	*TOE security functionality*
VAD	*Verification authentication data*

2.3 Associated references

Ref.	Document title
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 4. September 2012. CCMB-2012-09-001.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 4. September 2012. CCMB-2012-09-002.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 4. September 2012. CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 4. September 2012. CCMB-2012-09-004.
[COMP]	Common Criteria mandatory technical document – Composite product evaluation for smart cards and similar devices, CCDB-2012-04-001, Version 1.2, April 2012.
[PP-IC]	Security IC platform protection profile, version 1.0, 15th June 2007. Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035.
[PP-SSCD2]	Protection profiles for secure signature creation device — Part 2: Device with key Generation BSI-CC-PP-0059-2009-MA-01, Version 2.0.1, February 2012.
[PP-SSCD3]	Protection profiles for secure signature creation device – Part3: Device with key import BSI-CC-PP-0075-2012, Version 1.0.2, September 2012
[PP-SSCD4]	Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application BSI-CC-PP-0071-2012, Version 1.0.1, December 2012.
[PP-SSCD5]	Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application BSI-CC-PP-0072-2012, Version 1.0.1, December 2012.
[PP-SSCD6]	Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application BSI-CC-PP-0076-2013, Version 1.0.4, April 2013
[PP-PL]	JavaCard Protection Profile – Open Configuration, Version 3.0, May, 2012. Certified by ANSSI under the reference ANSSI-CC-PP-2010/03-M01
[ST-PL]	2014_0000002183 Security Target-IDeal Citiz v2.1 open platform
[ST-IC]	Security Target Lite M7892 B11 Recertification including optional software libraries RSA – EC – SHA-2 - Toolbox, Version 0.3, 2015-10-13
[ICAO]	International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.0.1, November 2010.

Ref.	**Document title**
[D03110]	Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE) and Restricted Identification (RI), TR-03110, version 2.02, 09.11.2009, Bundesamt für Sicherheit in der Informationstechnik (BSI).
[D14890-2]	Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services.
[IAS ECC]	Identification Authentication Signature - European Citizen Card Technical Specifications Revision: 1.0.1.
[IAS ADD]	0000098587-01 Addendum IAS-ECC v1.0.1UK.
[DIRECTIVE]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.
[Note10]	CERTIFICATION OF APPLICATIONS ON "OPEN AND ISOLATING PLATFORM Paris, the 27th July 2012. Reference: ANSSI-CCNOTE/10EN.02deW10
[JCRE]	JavaCard Platform, version 3.0.1 (, Classic Edition, including Specification Errata, October 2010, Updated February 2011. Runtime Environment (JavaCard RE) Specification. March 2008. Published by Sun Microsystems, Inc.
[JCAPI]	JavaCard Platform, versions 3.0 (March 2008) and 3.0.1, Classic Edition, including Specification Errata, October 2010, Updated February 2011, Application Programming Interface, March 2008. Published by Sun Microsystems, Inc.
[GP]	GlobalPlatform, Card Specification, Version 2.1.1, March 2003.

3 Conformance Claims

3.1 CC Conformance

This Security Target claims conformance to the following documents defining the ISO/IEC 15408:2005 standard:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [CC1].
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [CC2].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [CC3].
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012 [CEM].

Conformance to ISO/IEC 15408:2005 is claimed as follows:

- Part 1: conformant
- Part 2: extended with
  - FPT_EMS.1 TOE Emanation
  - FCS_RND Quality metric for random numbers
  - FIA_API Authentication proof of identity

  All the other security requirements have been drawn from the catalogue of requirements in [CC2].
- Part 3: conformant, compliant to EAL5 augmented with
  - ALC_DVS.2 (Sufficiency of security measures)
  - AVA_VAN.5 (Advanced methodical vulnerability analysis)

The TOE also includes:

- Integrated Circuit IC: Infineon M7892 B11 [ST-IC]. The IC ST claims strict conformance to the security IC platform PP [PP-IC]. The assets, threats, objectives, SFR and security functions specific to the Infineon M7892 B11 are described in [ST-IC] and are not repeated in the current ST.
- Java Card Platform: Ideal Citiz V2.1 open platform [ST-PL]. The PL ST claims demonstrable conformance to the security JC platform PP [PP-PL]. The assets, threats, objectives, SFR and security functions specific to the Platform are described in [ST-PL] and are not repeated in the current ST.

3.2 PP Claims

This security target is compliant with the following PPs:

- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation" [PP-SSCD2].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 3: Device with key import" [PP-SSCD3].

- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 4: Extension for device with key generation and trusted communication with certificate generation application" [PP-SSCD4].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 5: Extension for device with key generation and trusted communication with signature creation application" [PP-SSCD5].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 6: Extension for device with key import and trusted communication with signature creation application" [PP-SSCD6].

To cover the additional PACE functionality, the following SFR has been added in this ST:
FCS_RND.1

3.3 Conformance Rationale

[PP-SSCD4] and [PP-SSCD5] are strictely conforming to the core PP-SSCD2 [PP-SSCD2].
[PP-SSCD6] is strictely conforming to the core PP-SSCD3 [PP-SSCD3].
This ST is claimed to be conformant to the above mentioned PPs [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6].
A detailed justification is given in the following:

1) The SPD of this ST contains the security problem definition [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]. The SPD for this ST is described by the same threats, organisational security policies and assumptions as for the TOE in the PPs.

2) The security objectives for the TOE in this ST include all the security objectives for the TOE of the core PPs [PP-SSCD2] and [PP-SSCD3] and add
   a. the security objectives OT.TOE_TC_VAD_Imp and OT.TOE_TC_DTBS_Imp from [PP-SSCD5] and [PP-SSCD6],
   b. the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp from [PP-SSCD4],

3) The assumptions in this ST include A.CSP from [PP-SSCD3] and [PP-SSCD6]. This assumption doesn't mitigate any threat and doesn't fulfil any OSP meant to be addressed by security objectives for the TOE in the other PPs.

4) The security objectives for the operational environment in this ST include all security objectives for the operational environment of the core PPs [PP-SSCD2] and [PP-SSCD3] except OE.HI_VAD, OE.DTBS_Protect and OE.SSCD_Prov_Service. This ST adapts OE.HI_VAD and OE.DTBS_Protect to the support provided by the TOE by new security functionality (cf. OT.TOE_TC_VAD_Imp, OT.TOE_TC_DTBS_Imp) provided by the TOE and changes them into OE.HID_TC_VAD_Exp and OE.SCA_TC_DTBS_Exp ([PP-SSCD5] and [PP-SSCD6] for details).
   OE.SSCD_Prov_Service is replaced by OE.Dev_Prov_Service from [PP-SCCD4].
   This ST also includes security objectives for the operational environment OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp from [PP-SSCD4]

5) The SFRs specified in this ST includes all security functional requirements (SFRs) specified in the core PPs [PP-SSCD2] and [PP-SSCD3]. Additional SFRs address :

a. Trusted channel between the TOE and the SCA from [PP-SSCD5] and [PP-SSCD6]: FDP_UIT.1/DTBS, FTP_ITC.1/VAD and FTP_ITC.1/DTBS.
b. Trusted communication with CGA from [PP-SSCD4] : FIA_API.1 and FDP_DAU.2/SVD, FTP_ITC.1/SVD

6) This ST provides refinements for the SFR FIA_UAU.1 according to [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6].

7) To cover the additional PACE functionality, the following SFR have been added in this ST FCS_RND.1. This SFR does not come from any of the PP-SSCD.

8) The security assurance requirements (SARs) are originally taken from SARs of CC 3.1 Part 3 according to the package conformance EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5 (the Evaluation Assurance Level EAL5+ of the current ST exceeds the EAL4+ defined by [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]).

The document [COMP] shall be used in addition to the CC part 3 [CC3] and to the CEM [CEM]. This document specifies the additional information to be provided by a developer, and the additional checks to be performed by the ITSEF (Information Technology Security Evaluation Facility) when performing a "composite evaluation".

This security target is compliant with the SPD of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE SPDs	**PP SSCD2**	**PP SSCD3**	**PP SSCD4**	**PP SSCD5**	**PP SSCD6**	**Included**
	Assumptions					
A.CGA	×		x	×		×
A.SCA	×		x	×		×
A.CSP		x			x	x
	Threats					

TOE SPDs	**PP SSCD2**	**PP SSCD3**	**PP SSCD4**	**PP SSCD5**	**PP SSCD6**	**Included**
T.SCD_Divulg	x	x	x	×	x	×
T.SCD_Derive	×	x	x	×	x	×
T.Hack_Phys	×	x	x	×	x	×
T.SVD_Forgery	×	x	x	×	x	×
T.SigF_Misuse	×	x	x	×	x	×
T.DTBS_Forgery	×	x	x	×	x	×
T.Sig_Forgery	×	x	x	×	x	×
	Organisational Security Policies					
P.CSP_QCert	×	x	x	×	x	×
P.QSign	×	x	x	×	x	×
P.Sigy_SSCD	×	x	x	×	x	×
P.Sig_Non-Repud	×	x	x	×	x	×

Table 1 PP SPDs vs. ST

This security target is compliant with the security objectives of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE Objectives	**PP SSCD2**	**PP SSCD3**	**PP SSCD4**	**PP SSCD5**	**PP SSCD6**	**Included**
	Objectives for the TOE					

TOE Objectives	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
OT.Lifecycle_Security	x	x	x	x	x	×
OT.SCD/SVD_Auth_Gen	x		x	x		×
OT.SCD_Unique	x		x	x		×
OT.SCD_SVD_Corresp	x		x	x		×
OT.SCD_Secrecy	x	x	x	x	x	×
OT.Sig_Secure	x	x	x	x	x	×
OT.Sigy_SigF	x	x	x	x	x	×
OT.DTBS_Integrity_TOE	x	x	x	x	x	×
OT.EMSEC_Design	x	x	x	x	x	×
OT.Tamper_ID	x	x	x	x	x	×
OT.Tamper_Resistance	x	x	x	x	x	×
OT.TOE_TC_VAD_Imp				×	x	×
OT.TOE_TC_DTBS_Imp				×	x	×
OT.TOE_SSCD_Auth			x			×
OT.TOE_TC_SVD_Exp			x			×
OT.SCD_Auth_Imp		x			x	x
	Objectives for the Operational Environment					

TOE Objectives	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
OE.SVD_Auth	×	×	×	×	×	×
OE.CGA_QCert	×	×	×	×	×	×
OE.SSCD_Prov_Service	×	×		×	×	
OE.SCD/SVD_Auth_Gen		×			×	×
OE.SCD_Unique		×			×	×
OE.SCD_SVD_Corresp		×			×	×
OE.SCD_Secrecy		x			x	×
OE.HID_VAD	×	×	×			
OE.DTBS_Intend	×	×	×	×	x	×
OE.DTBS_Protect	×	×	×			
OE.Signatory	×	×	×	×	×	×
OE.HID_TC_VAD_Exp				×	×	×
OE.SCA_TC_DTBS_Exp				×	×	×
OE.Dev_Prov_Service			x			x
OE.CGA_SSCD_Auth			x			×
OE.CGA_TC_SVD_Imp			x			×

Table 2 PP Security Objectives vs. ST

This security target is compliant with the security functional requirements of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE SFRs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
FCS_CKM.1	×		×	×		×
FCS_CKM.4	×	×	×	×	×	×
FCS_COP.1	×	×	×	×	×	×
FDP_ACC.1/SCD/SVD_Generation	×		×	×		×
FDP_ACF.1/SCD/SVD_Generation	×		×	×		×
FDP_ACC.1/SVD_Transfer	×		×	×		×
FDP_ACF.1/SVD_Transfer	×		×	×		×
FDP_ACC.1/Signature_Creation	×	×	×	×	×	×
FDP_ACF.1/Signature_Creation	×	×	×	×	×	×
FDP_ACC.1/SCD_Import		×			×	×
FDP_ACF.1/SCD_Import		×			×	×
FDP_RIP.1	×	×	×	×	×	×
FDP_SDI.2/Persistent	×	×	×	×	×	×
FDP_SDI.2/DTBS	×	×	×	×	×	×
FIA_UID.1	×	×	×	×	×	×
FIA_UAU.1	×	×	×	×	×	×
FIA_AFL.1	×	×	×	×	×	×
FMT_SMR.1	×	×	×	×	×	×
FMT_SMF.1	×	×	×	×	×	×
FMT_MOF.1	×	×	×	×	×	×
FMT_MSA.1/Admin	×	×	×	×	×	×
FMT_MSA.1/Signatory	×	×	×	×	×	×
FMT_MSA.2	×	×	×	×	×	×
FMT_MSA.3	×	×	×	×	×	×

TOE SFRs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
FMT_MSA.4	×	×	×	×	×	×
FMT_MTD.1/Admin	×	×	×	×	×	×
FMT_MTD.1/Signatory	×	×	×	×	×	×
FPT_EMS.1	×	×	×	×	×	×
FPT_FLS.1	×	×	×	×	×	×
FPT_PHP.1	×	×	×	×	×	×
FPT_PHP.3	×	×	×	×	×	×
FPT_TST.1	×	×	×	×	×	×
FIA_API.1			×			×
FTP_ITC.1/SVD			×			×
FDP_DAU.2/SVD			×			x
FDP_UIT.1/DTBS				×	×	×
FTP_ITC.1/VAD				×	×	×
FTP_ITC.1/DTBS				×	×	×
FDP_ITC.1/SCD		×				×
FDP_UCT.1/SCD		×				×
FTP_ITC.1/SCD		×				×
FCS_RND.1						×

Table 3 PP SFRs vs. ST

4 Statement of Compatibility

In this section, the compatibility between the Composite ST and the Platform ST [ST-PL] is examined. In other words, it will be shown that there is no conflict between the security environment, the security objectives, and the security requirements of the Composite Security Target and the Platform Security Target.

4.1 Compatibility between SFRs

The following table lists the relevant SFRs of the Ideal Citiz v2.1 open platform given in [ST-PL], and provides the link to the SFRs on the composite-product, showing that there is no contradiction between the two.

Platform SFR	Composite SFR	Compatibility
FAU_ARP.1	Indirectly supports FPT_FLS.1, FPT_PHP.3	Internal counter for security violations complement IdealCitiz mechanisms
FCS_CKM.1	FCS_CKM.1 (used EC, RSA)	The requirement in this ST is equivalent to parts of the platform ST. See SF.APP_CRYPTO
FCS_CKM.2	No correspondence	managed within IdealCitiz No contradiction to this ST
FCS_CKM.3	No correspondence	managed within IdealCitiz No contradiction to this ST
FCS_CKM.4	FCS_CKM.4	The requirement in this ST leads to the fulfillment of the platform SFR. See SF.APP_CRYPTO
FCS_COP.1	FCS_COP.1	The requirement of the ST targets digital signature generation, PACE authentication, Ciphering and deciphering. It is fulfilled by the platform SFR. See SF.AUTHENTICATION, SF.APP_CRYPTO, SF.TRUSTED_CHANNEL
FDP_ACC.2/FIREWALL FDP_ACC.2/ADEL	No correspondence	managed within IdealCitiz: access control mechanisms No contradiction to this ST
FDP_ACF.1/FIREWALL FDP_ACF.1/ADEL	No correspondence	IdealCitiz access control mechanisms No contradiction to this ST
FDP_IFC.1/JCVM	No correspondence	refers to IdealCitiz Virtual Machine No contradiction to this ST
FDP_IFF.1/JCVM	No correspondence	refers to IdealCitiz Virtual Machine No contradiction to this ST

Platform SFR	Composite SFR	Compatibility
FDP_RIP.1/OBJECTS FDP_RIP.1/ABORT FDP_RIP.1/APDU FDP_RIP.1/bArray FDP_RIP.1/KEYS FDP_RIP.1/TRANSIENT FDP_RIP.1/ADEL FDP_RIP.1/ODEL	FDP_RIP.1	The platform SFR leads to fulfillment of the SFR of this ST. No contradiction.
FDP_ROL.1/FIREWALL	No correspondence	refers to IdealCitiz Virtual Machine No contradiction to this ST
FDP_SDI.2	No correspondence	IdealCitiz: internal data integrity protection No contradiction to this ST
FDP_ITC.2/Installer	No correspondence	IdealCitiz: data control mechanisms No contradiction to this ST
FCO_NRO.2/CM	No correspondence	IdealCitiz: PACKAGE LOADING information flow control No contradiction to this ST
FDP_IFC.2/CM	No correspondence	IdealCitiz: PACKAGE LOADING information flow control No contradiction to this ST
FDP_IFF.1/CM	No correspondence	IdealCitiz: PACKAGE LOADING information flow control No contradiction to this ST
FDP_UIT.1/CM	No correspondence	IdealCitiz: PACKAGE LOADING information flow control No contradiction to this ST
FIA_ATD.1/AID	No correspondence	IdealCitiz AID management No contradiction to this ST
FIA_UID.2/AID	No correspondence	IdealCitiz AID management No contradiction to this ST

Platform SFR	Composite SFR	Compatibility
FIA_USB.1/AID	No correspondence	IdealCitiz AID management No contradiction to this ST
FIA_UID.1/CM	No correspondence	IdealCitiz Card Identification No contradiction to this ST
FMT_MSA.1/JCRE FMT_MSA.1/JCVM	No correspondence	IdealCitiz Firewall mechanism No contradiction to this ST
FMT_MSA.2/FIREWALL_JCVM	No correspondence	IdealCitiz Firewall mechanism and JCVM information No contradiction to this ST
FMT_MSA.3/FIREWALL	No correspondence	IdealCitiz Firewall mechanism No contradiction to this ST
FMT_MSA.3/JCVM	No correspondence	IdealCitiz JCVM information 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	No correspondence	IdealCitiz specific roles No contradiction to this ST
FMT_MTD.1/JCRE	No correspondence	IdealCitiz specific roles No contradiction to this ST
FMT_MTD.3/JCRE	No correspondence	IdealCitiz: secure values for the registered applets' AIDs No contradiction to this ST
FMT_MSA.1/ADEL	No correspondence	IdealCitiz: Firewall management and Applet deletion management No contradiction to this ST
FMT_MSA.3/ADEL	No correspondence	IdealCitiz: Firewall management and Applet deletion management No contradiction to this ST
FMT_SMF.1/ADEL	No correspondence	IdealCitiz: Applets'AIDs management No contradiction to this ST

Platform SFR	Composite SFR	Compatibility
FMT_SMR.1/ADEL	No correspondence	IdealCitiz: Applet deletion management No contradiction to this ST
FMT_MSA.1/CM	No correspondence	IdealCitiz: Package loading, security attributes and security domain management No contradiction to this ST
FMT_MSA.3/CM	No correspondence	IdealCitiz: Package loading, security attributes and security domain management No contradiction to this ST
FMT_SMF.1/CM	No correspondence	IdealCitiz: management functions specified in GP No contradiction to this ST
FMT_SMR.1/CM	No correspondence	IdealCitiz: Card Administrator roles management No contradiction to this ST
FMT_SMR.1/Installer	No correspondence	IdealCitiz: Card Administrator roles management No contradiction to this ST
FPR_UNO.1	No correspondence	IdealCitiz: Firewall management and package separation No contradiction to this ST
FPT_FLS.1 FPT_FLS.1/Installer FPT_FLS.1/ADEL FPT_FLS.1/ODEL FPT_FLS.1/OS	FPT_FLS.1	Internal countermeasures for detecting security violations complement IdealCitiz mechanisms
FPT_TDC.1	No correspondence	IdealCitiz: JCVM specification, interpretation of CAP files, bytecode and data arguments No contradiction to this ST

Platform SFR	Composite SFR	Compatibility
FPT_RCV.3/Installer	No correspondence	IdealCitiz: package loading and applet installation management No contradiction to this ST
FPT_RCV.3/OS	No correspondence	IdealCitiz: memory management and memory access control No contradiction to this ST
FPT_RCV.4/OS	No correspondence	IdealCitiz: memory management, memory access control, preservation of secure state when power loss No contradiction to this ST
FPT_PHP.3/OS	FPT_PHP.3	Fullfillment of the platform SFR is used for fulfillment of the SFR of this ST.
FTP_ITC.1/CM	No correspondence	IdealCitiz: trusted channel for loading/installing a new application package on the card No contradiction to this ST
FDP_ACC.1/CardLifeCycleManagement	No correspondence	refers to IdealCitiz card life cycle management No contradiction to this ST
FDP_ACF.1/CardLifeCycleManagement	No correspondence	refers to IdealCitiz card life cycle management No contradiction to this ST
FMT_MSA.1/CardLifeCycleManagement	No correspondence	refers to IdealCitiz card life cycle management No contradiction to this ST
FMT_MSA.3/CardLifeCycleManagement	No correspondence	refers to IdealCitiz card life cycle management No contradiction to this ST
FTP_ITC.1/CardLifeCycleManagement	No correspondence	refers to IdealCitiz card life cycle management No contradiction to this ST
FCS_CKM.2/PACE	No correspondence	refers to IdealCitiz PACE key management No contradiction to this ST

Platform SFR	Composite SFR	Compatibility
FCS_CKM.3/PACE	No correspondence	refers to IdealCitiz PACE key management No contradiction to this ST
FCS_COP.1/PACE	No correspondence	refers to IdealCitiz PACE key management No contradiction to this ST

4.2 Compatibility between OTs

The following table lists the relevant Security Objectives (O) of the IdealCitiz platform given in [ST-PL], and provides the link to the Security Objectives (OT) on the composite-product, showing that there is no contradiction between the two.

Platform Security Objectives	Composite Security Objectives	Compatibility
O.SID	No correspondence	No contradiction to this ST
O.FIREWALL	No correspondence	No contradiction to this ST
O.GLOBAL_ARRAYS_CONFID	No correspondence	No contradiction to this ST
O.GLOBAL_ARRAYS_INTEG	No correspondence	No contradiction to this ST
O.NATIVE	No correspondence	No contradiction to this ST
O.OPERATE	OT.SCD_Unique	No contradiction to this ST
O.REALLOCATION	No correspondence	No contradiction to this ST
O.RESOURCES	No correspondence	No contradiction to this ST
O.ALARM	No correspondence	No contradiction to this ST
O.CIPHER	OT.SCD_Unique, OT.Sig_Secure	No contradiction to this ST
O.KEY-MNGT	OT.SCD_Secrecy, OT.SCD/SVD_Auth_Gen, OT.SCD_Unique	No contradiction to this ST
O.PIN-MNGT	No correspondence	No contradiction to this ST
O.BIO-MNGT	No correspondence	No contradiction to this ST
O.TRANSACTION	No correspondence	No contradiction to this ST
O.OBJ-DELETION	No correspondence	No contradiction to this ST
O.DELETION	No correspondence	No contradiction to this ST
O.LOAD	OT.Lifecycle_Security	No contradiction to this ST
O.INSTALL	OT.Lifecycle_Security	No contradiction to this ST
O.SCP.IC	OT.Tamper_Resistance	No contradiction to this ST
O.SCP.RECOVERY	OT.EMSEC_Design	No contradiction to this ST
O.SCP.SUPPORT	No correspondence	No contradiction to this ST
O.CARD-MANAGEMENT	OT.Lifecycle_Security	No contradiction to this ST

4.3 Compatibility between OEs

The following table lists the relevant Security Objectives for the environments (OE) of the IdealCitiz platform given in [ST-PL], and provides the link to the OEs on the composite-product, showing that there is no contradiction between the two.

Platform OE	Composite OE	Compatibility
OE.APPLET	No correspondence	No contradiction to this ST
OE.VERIFICATION	Applet is loaded pre issuance on platform. Same organizational measures than for platform apply.	No contradiction to this ST
OE.CODE-EVIDENCE	Applet code is delivered with Platform code to the founder. Same measures apply.	No contradiction to this ST
OE.SECURITY-DOMAINS	No correspondence	No contradiction to this ST
OE.QUOTAS	No correspondence	No contradiction to this ST
OE.SHARE-CONTROL	No correspondence	No contradiction to this ST
OE.KEY_GENERATION	No correspondence	No contradiction to this ST
OE.PRODUCTION	Platform guidance documents have to be taken into account	No contradiction to this ST

4.4 Compatibility between As

The following table lists the relevant assumptions (A) of the IdealCitiz platform given in [ST-PL], and provides the link to the assumptions on the composite-product, showing that there is no contradiction between the two.

Platform A	Composite A	Compatibility
A.APPLET	Guidance of the Platform-Developer for the Applet Developer has to be applied	No contradiction to this ST
A.VERIFICATION	Guidance of the Platform-Developer for the Applet Developer has to be applied	No contradiction to this ST
A.PRODUCTION	Guidance of the Platform-Developer for the Applet Developer has to be applied	No contradiction to this ST

4.5 Compatibility between OSPs

The following table lists the relevant OSPs of the IdealCitiz platform given in [ST-PL], and provides the link to the OSPs on the composite-product, showing that there is no contradiction between the two.

Platform OSP	Composite OSP	Compatibility
OSP.VERIFICATION	Guidance of the Platform-Developer for the Applet-Developer and recommandations related to the isolation property of the platform have to be applied in the application code	No contradiction to this ST
OSP.SECURITY_DOMAINS	No correspondence	No contradiction to this ST
OSP.QUOTAS	No correspondence	No contradiction to this ST
OSP.KEY_GENERATION	Guidance of the Platform-Developer for the Applet-Developer and recommandations related to the Key Generation have to be applied in the application code	No contradiction to this ST
OSP.SHARE-CONTROL	Guidance of the Platform-Developer for the Applet-Developer and recommandations related to the Shareable interface functionality have to be applied in the application code	No contradiction to this ST

4.6 Compatibility between Ts

The following table lists the relevant threats (T) of the IdealCitiz platform given in [ST-PL], and provides the link to the threats on the composite-product, showing that there is no contradiction between the two.

Platform T	Composite T	Compatibility
T.CONFID-APPLI-DATA	No correspondence	No contradiction to this ST
T.CONFID-JCS-CODE	No correspondence	No contradiction to this ST
T.CONFID-JCS-DATA	No correspondence	No contradiction to this ST
T.INTEG-APPLI-CODE	No correspondence	No contradiction to this ST
T.INTEG-APPLI-CODE.LOAD	No correspondence	No contradiction to this ST
T.INTEG-APPLI-DATA	T.DTBS_Forgery, T.Sig_Forgery, T.SCD_Divulg, T.SCD_Derive, T.SVD_Forgery	
T.INTEG-APPLI-DATA.LOAD	No correspondence	No contradiction to this ST
T.INTEG-JCS-CODE	No correspondence	No contradiction to this ST
T.INTEG-JCS-DATA	No correspondence	No contradiction to this ST
T.SID.1	No correspondence	No contradiction to this ST
T.SID.2	No correspondence	No contradiction to this ST
T.EXE-CODE.1	No correspondence	No contradiction to this ST
T.EXE-CODE.2	No correspondence	No contradiction to this ST
T.NATIVE	No correspondence	No contradiction to this ST
T.RESOURCES	No correspondence	No contradiction to this ST
T.DELETION	No correspondence	No contradiction to this ST
T.INSTALL	No correspondence	No contradiction to this ST
T.OBJ-DELETION	No correspondence	No contradiction to this ST
T.PHYSICAL	T.Hack_Phys	No contradiction to this ST
T.APP_DATA_INTEGRITY	No correspondence	No contradiction to this ST
T.UNAUTH_CARD_MNGT	No correspondence	No contradiction to this ST
T.LIFE_CYCLE	No correspondence	No contradiction to this ST
T.UNAUTH_ACCESS	No correspondence	No contradiction to this ST

4.7 Separation and Compatibility of SFs

This section describes the separation of relevant TSF described in the Security Target of the underlying platform being used by this Security Target.

Platform TSF	**Usage by TOE**
F.OPEN	Not relevant
F.CARD_MANAGER	Not relevant
F.JAVA_CARD_SYSTEM	Not relevant
F.JAVA_API	Relevant SF Used by SF.TRUSTED_CHANNEL, SF.MANAGEMENT
F.AUTHENTICATION	Relevant SF Used by SF.AUTHENTICATION, SF.TRUSTED_CHANNEL
F.MEMORY_PROGRAMMING	Not relevant
F.SECURE_DATA_MANAGER	Relevant SF Used by SF.RATIF, SF.AUTHENTICATION, SF.MANAGEMENT
F.SECRET_DATA_MANAGER	Relevant SF Used by SF.RATIF, SF.AUTHENTICATION, SF.MANAGEMENT
F.SYSTEM_MANAGER	Not relevant
F.CRYPTOGRAPHIC_OPERATIONS	Relevant SF Used by SF.APP_CRYPTO
F.MEMORY_ACCESS	Not relevant
F.MEMORY_CONTROLLER	Not relevant
F.INPUT/OUTPUT_LAYER	Not relevant
F.TRANSPORT_LAYER	Not relevant

Platform TSF	Usage by TOE
F.CRYPTOGRAPHY_SERVICES	Relevant SF Used by SF.APP_CRYPTO
F.SECURITY_CONFIGURATION	Not relevant
F.CPU_MANAGER	Not relevant
F.INTEGRATED_CIRCUIT	Relevant SF Used by SF.APP_INTEGRITY

4.8 Compatibility of Assurance Requirements

The level of assurance of the:

- TOE is EAL5 augmented with ALC DVS.2 and AVA_VAN.5
- Platform is EAL5 augmented with ALC DVS.2 and AVA VAN.5

This shows that the Assurance Requirements of the TOE matches the Assurance Requirements of the underlying Platform.

5 TOE Description

5.1 Product Presentation

The CC IDeal Citiz product is the DUAL integrated circuit chip embedding

- An Operating system providing:
  - Java Card interfaces, as specified in [JCAPI]
  - Extended interfaces for targeted applications needs
- A Set of applications:
  - An ID.me application compliant with the IAS ECC v1.0.1 specification [IAS ECC],
  - A SAC-EAC ePassport application compliant with International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL specifications [ICAO] and
  - A card manager application compliant with the GlobalPlatform v2.1.1 specifications [GP] standard. This application enables the card issuer to add functionality to the product by loading and executing new applets, even in the evaluated configuration. This functionality is out of the scope of the evaluation.

All applications are protected against post issuance Java Card applet loading and execution thanks to a firewall mechanism.

5.2 Overview of ID.me Package

The ID.me is an European Card for e-Services and national e-ID Applications based on Java Card. ID.me is designed to be compliant with the IAS ECC v1.0.1 specification [IAS ECC], taking into account the addendum [IAS ADD]. It provides the following services:

1) SSCD containing data needed for generating electronic signatures on behalf of the Card Holder as well as for user authentication; this application is intended to be used in the context of official and commercial services, where an electronic signature of the Card Holder is required: to be certified according to [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6].
2) PACE authentication to ensure a trusted channel secure communication with a SCA and a CGA.

The TOE comprises of

- The Infineon M7892 B11 integrated circuit,
- The Crypto Libraries: RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries
- The IdealCitiz v2.1 Java Card open platform,
- The applet containing the SSCD functionality and,
- The associated guidance documentation [AGD_OPE], [AGD_PRE].

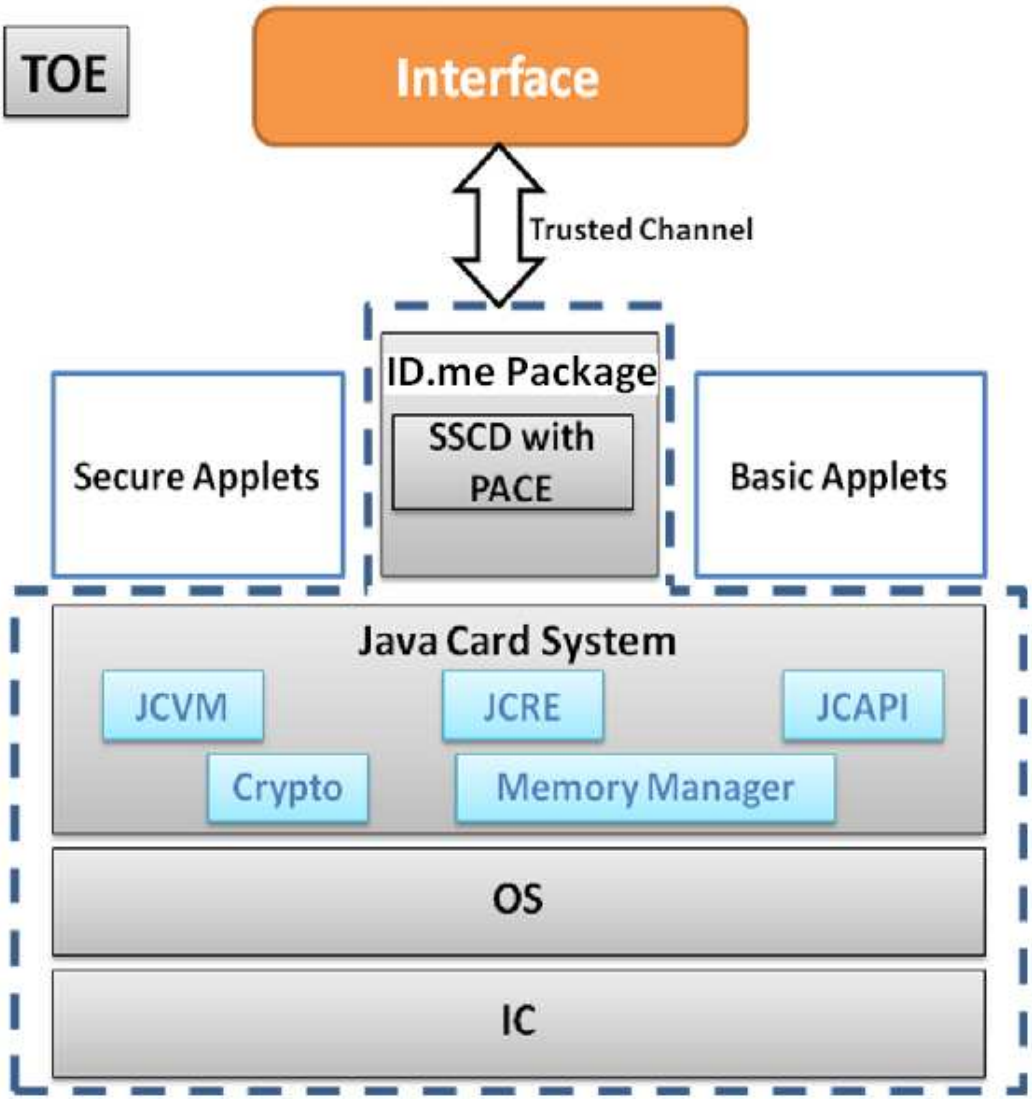

Figure 1: TOE physical scope

Beside the TOE, the product can include other Java Card applications (out of scope of the TOE). IdealCitiz Operating System enforces separation of the data between the applets and associated packages imposing logical separation of data using the Java Card™ Firewall [JCRE].

5.3 TOE Functions

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

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

The TOE provides the following functions:

- generation of the SCD and the correspondent SVD,
- importation of the SCD and, optionally, the correspondent signature verification data (SVD)
- export the SVD for certification through a trusted channel to the CGA,
- prove the identity as SSCD to external entities
- optionally, receive and store certificate info,
- switch the TOE from a non operational state to an operational state, and
- if in an operational state, create digital signatures for data with the following steps:
  - select an SCD if multiple are present in the SSCD,
  - receive DTBS or a unique representation thereof DTBS/R through a trusted channel with SCA.
  - authenticate the signatory and determine its intent to sign,
  - apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R
- identification and authentication of trusted users and applications,
- data storage and protection from modification or disclosures, as needed,
- secure exchange of sensitive data between the TOE and a trusted applications,
- secure exchange of sensitive data between the TOE and a trusted human interface device.

The TOE is prepared for the signatory's use by

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

After preparation or import 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, PIN or a biometric template, providing this information shall protect the confidentiality of the corresponding RAD.

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

5.4 Operation of the TOE

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

1) The preparation environment, where it interacts with a certification service provider through a SCD/SVD generation application to import, if applicable, a signature creation data (SCD) and a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with the SCD the TOE or the CSP has generated. In case of SCD/SVD generation by the CSP, the SCD/SVD generation application transmits the SVD to the CGA. The initialization environment interacts further with the TOE to personalize it with the initial value of the reference

authentication data (RAD). Optionally, the TOE may export the SVD through a trusted channel allowing the CGA to check the authenticity of the SVD.

2) The signing environment where it interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation application provides the data to be signed (DTBS), or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting digital signature. Optionally, the TOE and the SCA may communicate through a trusted channel to ensure the confidentiality and the integrity of the DTBS/R.
3) The management environments where it interacts with the user or an SSCD-provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

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

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case the TOE 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 and integrity of the SCD and restricts its use in signature creation to its signatory. The digital signature created by the TOE is a qualified electronic signature as defined in Article 5.1 of the directive [DIRECTIVE]. Determining the state of the certificate as qualified is 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. Optionally, the TOE and the SCA may communicate through a trusted channel in order to protect the integrity of the DTBS/R.

The TOE stores signatory RAD to authenticate a user as its signatory. The RAD is a password e.g. PIN, a biometric template or a combination of these. The TOE protects the confidentiality and integrity of the RAD. The TOE receives the VAD from the signature creation application. The signature creation application protects the confidentiality of this data.

A certification service provider and a SSCD-provisioning service provider interact with the TOE in the secure preparation environment to perform any preparation function of the TOE required before control of the TOE is given to the legitimate user. These functions include but are not limited to:

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

Optionally, the TOE and the CGA communicate through a trusted channel in order to protect the integrity and authenticity of the SVD exported from the TOE.

The TOE is a SSCD with PACE on a smart card. A smart card terminal shall 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 initiates the digital signature creation function of the smart card through the terminal.

This TOE does not implement, in addition to the functions of the SSCD, the signature creation application (SCA). The SCA presents the data to be signed (DTBS) to the signatory and prepares the DTBS representation the signatory wishes to sign for performing the cryptographic function of the signature. The SCA is considered as part of the environment of the TOE.

The TOE allows implementing a Human Interface (HI) for user authentication:

1) by the TOE itself or
2) by a trusted human interface device connected via a trusted channel with the TOE.

The human interface device is used for the input of VAD for authentication by knowledge or for the generation of VAD for authentication by biometric characteristics.

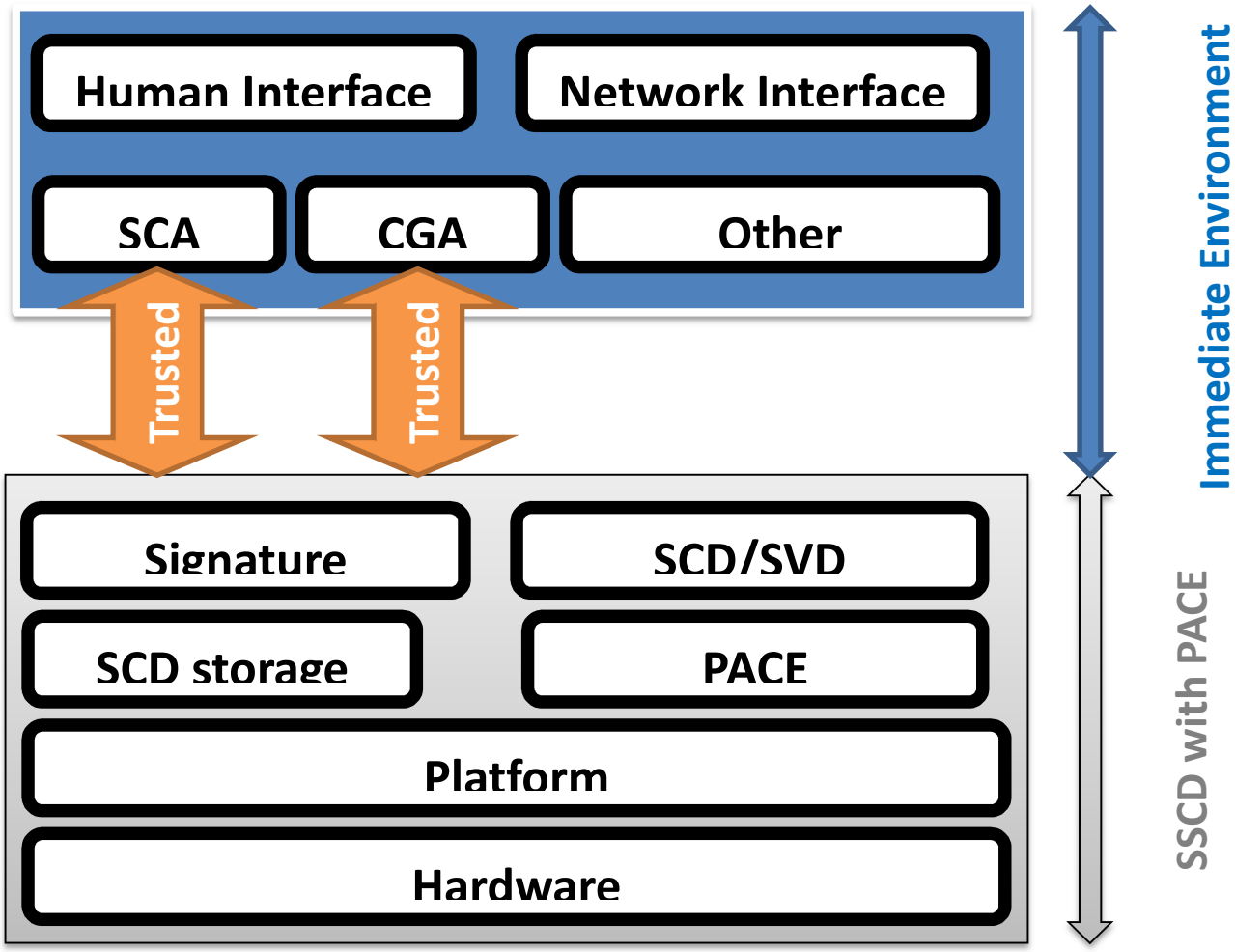

Figure 2: Scope of the SSCD

The security functionality of the TOE will be externally available to the user by APDU commands according to the access conditions specified by the appropriate policies considering the life cycle state, user role and security state.

5.5 Open and isolating Platform

This security target claims conformance to the Application Note 10 on Open and Isolating platform, issued by ANSSI [Note10].

An "open platform" can host new applications:

- Before its delivery to the end user (during phases 4, 5 or 6 of the traditional smartcard lifecycle). Such loadings are called "pre-issuance".
- After its delivery to the end user (phase 7). Such loadings are called "post-issuance".

An "isolating platform" is a platform that maintains the separation of the execution domains of all embedded applications on a platform, as of the platform itself. "Isolation" refers here to domain separation of applications as well as protection of application's data.

5.6 Major security features of the TOE

The TOE provides the following TOE security features:

5.6.1 Authentication mechanisms

This feature realizes three authentication mechanisms: PIN verification, biometric characteristic verification and alternatively authentication with the PACE protocol. It also ensures that only authenticated terminals can get access to the user data stored on the TOE.

5.6.2 Cryptographic

This feature performs high level cryptographic operations (key generation, Signature Creation, destruction of cryptographic keys and random number generation). The implementation is mainly based on the Security Functionalities provided by the platform.

5.6.3 Trusted Channels

This feature realizes a secure communication channel to verify authenticity and integrity as well as securing confidentiality of user data between the TOE and other devices connected. The TOE provides:

- Secure messaging with external applications as CGA and SCA
- PACE used to establish session keys for secure messaging
- TDES for encryption/decryption and MAC generation/verification

This feature is provided by the platform and used for secure messaging.

5.6.4 Access Control

This feature manages the access to objects (files, directories, data and secrets) stored in the ID.me file system. It ensures secure management of secrets such as cryptographic keys. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification.

5.6.5 Data Storage

This feature manages the storage of manufacturing data, pre-personalization data and personalization data. This covers secure key storage.

5.6.6 Integrity

This feature monitors the integrity of sensitive user data and the integrity of the DTBS/R.

5.6.7 Features from the Platform

This contains all security functionalities provided by the certified platform (IC and Java Card operation system):

- Protection against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.
- Protection against physical attack and perform self tests as described in [ST-PL].
- Security domains are supported by the Java Card platform.
- Cryptographic operations: Signature generation, signature creation and secure messaging.

5.7 TOE Life Cycle

5.7.1 General

The TOE life cycle in Figure 3 distinguishes stages for development, production, preparation and operational use. The development and production of the TOE (cf. CC part 1 [CC1], 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 a SSCD-provisioning service provider. The functional integrity of the TOE shall be protected in delivering it to a SSCD-provisioning service provider: before any delivery occurs, the TOE is secured with a Transport Key. The SSCD-provisioning service will be able to unlock the card with the Transport Key before the preparation phase.

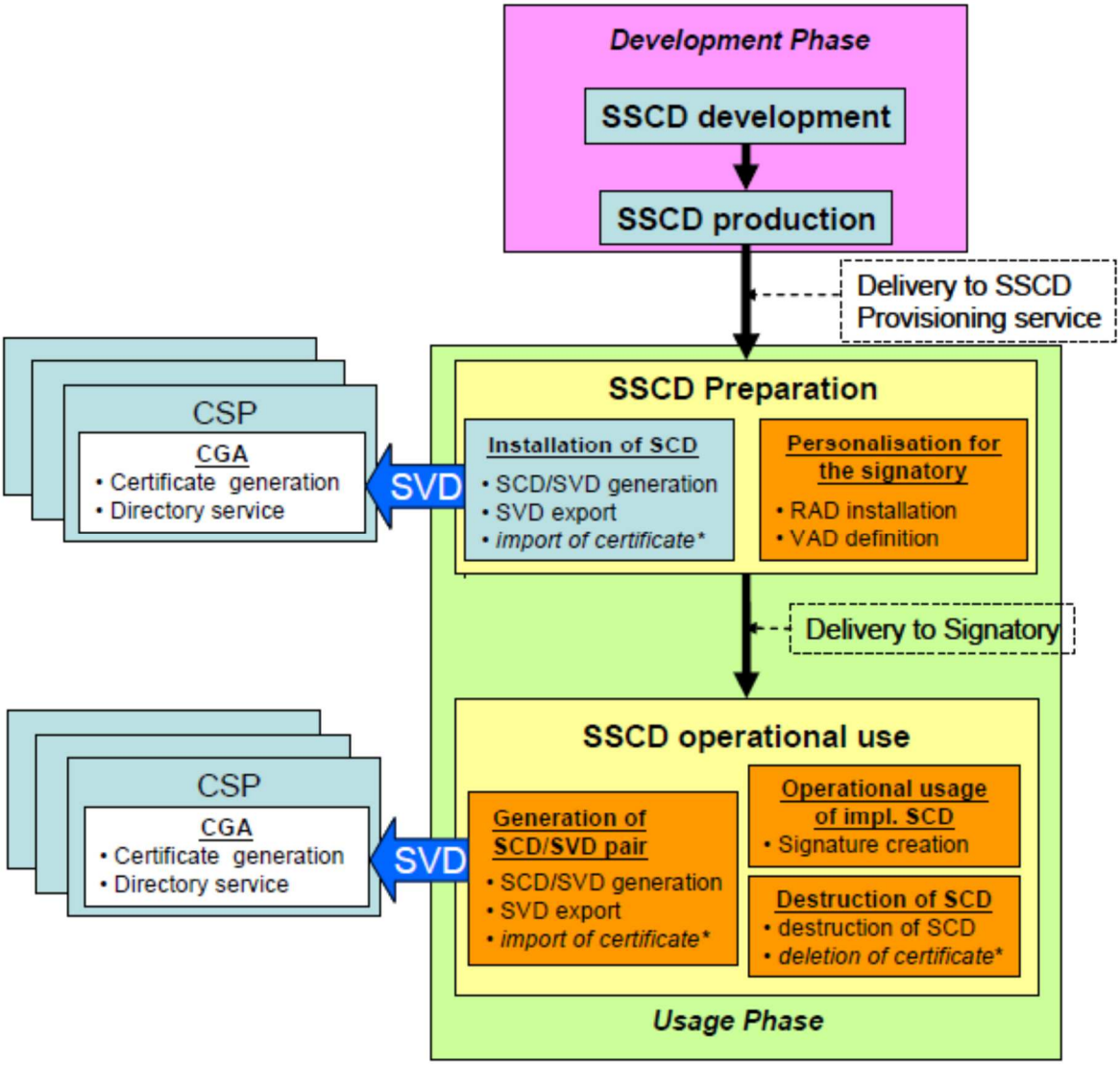

Figure 3: TOE Life Cycle (SCD Generation by TOE)

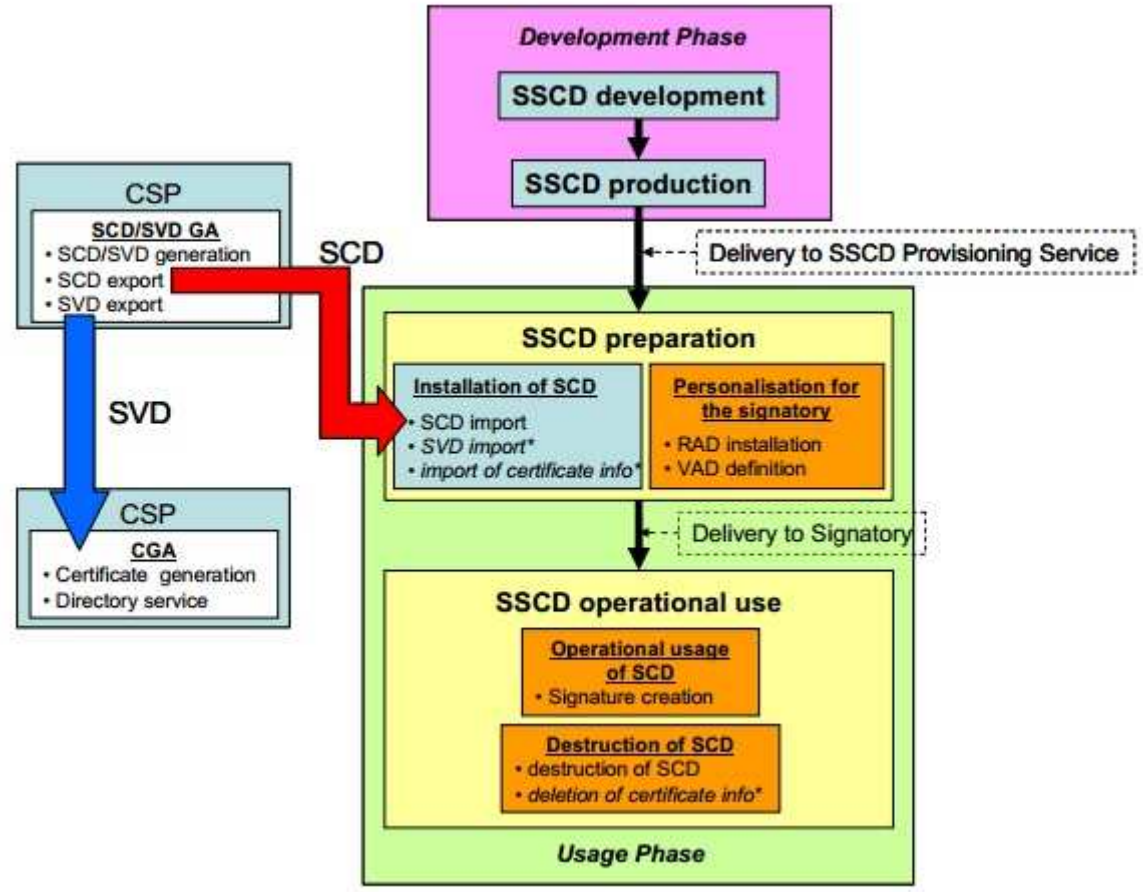

Figure 4: TOE Life Cycle (SCD import by TOE)

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 shall include deletion of the any stored corresponding certificate info.

5.7.2 Development phase (Phases 1 & 2 of the IC life cycle [PP-IC])

This phase is composed of two stages:

- IC embedded software development
- IC development

The IC Embedded Software Developer is in charge of:

- Specification, development and validation of the software (IC operating system & ID.me Package).
- Specification of IC initialization requirements.

The IC Developer:

- Designs the IC, develops the IC dedicated software and provides information, software or tools to the IC embedded software developer.

- Receives the smartcard embedded software from the developer, through trusted delivery and verification procedures.

From the IC design, IC Dedicated Software and Smartcard Embedded Software, the IC Developer constructs the smartcard IC database, necessary for the IC photo mask fabrication.

Actors :

IC Embedded Software Developer	Infineon, Morpho
IC Developer	Infineon

5.7.3 Production phase (Phases 3, 4 & 5 of the Platform life cycle)

This phase is composed of three stages:

- IC manufacturing and testing
- IC Packaging
- Smartcard Prepersonalization & testing

The IC Manufacturer is responsible for producing the IC through three main steps:

- IC manufacturing,
- IC testing,
- IC Initialization.

The IC Packaging Manufacturer is responsible for IC packaging and testing.

The smartcard prepersonalizer is responsible for prepersonalizing the smartcard

Actors :

IC Manufacturer	Infineon or Morpho
IC Packaging Manufacturer	Infineon or Morpho
Smartcard prepersonalizer	Infineon or Morpho

5.7.4 Preparation phase (Phases 6 of the Platform life cycle)

This phase consists of:

1) Finishing process of the product (Composite product integration)
2) Personalization: RAD storage and VAD delivery processes
3) SCD initialization by the generation of SCD/SVD pair :
    a. By the TOE through the SCD/SVD generation functionality.
    b. By the CSP which loads the SCD to the TOE
4) export of SVD to CGA.

The IC contains in its ROM the following applets:

The ID.me package composed of:

a. ID.me SSCD providing the SSCD functionality (Service to be certified in this ST)
b. ID.me ID providing a general purpose file system

During this phase, creation of ID.me SSCD applet instance is mandatory. This phase may also include the following additional activities:

- loading additional applets into the IC EEPROM,
- creating instances of additional applets.

These additional applets will be tested before loading and they verifiably will not interfere with the ID.me SSCD applet.

The instances of additional applets (ID.me ID…) are out of the scope of this certification and should not be used together with ID.me SSCD.

5.7.5 Operational phase (Phase 7 of the Platform life cycle)

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

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

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

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

The TOE supports 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 certificate. If the conditions to obtain a qualified certificate are met the new key can also be used to create advanced electronic signatures. The optional TOE functions for additional key generation and certification may require additional security functions in the TOE and an interaction with the SSCD-provisioning service provider in an environment that is secure.

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

6 Security Problem Definition

6.1 Assets

D.SCD

Signature Creation Data

Private key used to perform an electronic signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.

D.SVD

Signature Verification Data

Public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported must be maintained.

D.DTBS/R

Data to be signed or its unique Representation

set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.

6.2 Users / Subjects

6.2.1 Threat agents

S.Attacker

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

6.2.2 Miscellaneous

S.User

End user of the TOE who can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

S.Admin

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

S.Signatory

User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

6.3 Threats

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.

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.

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.

T.SVD_Forgery

Forgery of the signature verification data

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

T.SigF_Misuse

Misuse of the signature creation function of the TOE

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

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.

T.Sig_Forgery

Forgery of the electronic signature

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

6.4 Organisational Security Policies

P.CSP_QCert

Qualified certificate

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

P.QSign

Qualified electronic signatures

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

P.Sigy_SSCD

TOE as secure signature creation device

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

P.Sig_Non-Repud

Non-repudiation of signatures

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

6.5 Assumptions

A.CGA

Trustworthy certificate generation application

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

A.SCA

Trustworthy signature creation application

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

A.CSP

Secure SCD/SVD management by CSP

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

7 Security Objectives

7.1 Security Objectives for the TOE

7.1.1 OTs common to PP SSCD-KG and PP SSCD-KI

OT.Lifecycle_Security

Lifecycle security

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

OT.SCD_Secrecy

Secrecy of the signature-creation data

The secrecy of the SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential. Application Note: The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and secure destruction.

OT.Sig_Secure

Cryptographic security of the electronic signature

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

OT.Sigy_SigF

Signature creation function for the legitimate signatory only

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

OT.DTBS_Integrity_TOE

DTBS/R integrity inside the TOE

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

OT.Tamper_ID

Tamper detection

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

OT.EMSEC_Design

Provide physical emanations security

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

OT.Tamper_Resistance

Tamper resistance

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

7.1.2 Specific OTs from PP SSCD-KG

OT.SCD/SVD_Auth_Gen

Authorized SCD/SVD generation

The TOE shall provide security features to ensure that authorised users only may invoke the generation of the SCD and the SVD. Application Note: PoP code is used as proof or authorised user if user initiates key generation

OT.SCD_Unique

Uniqueness of the signature creation data

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

OT.SCD_SVD_Corresp

Correspondence between SVD and SCD

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

7.1.3 Specific OTs from PP SSCD-KI

OT.SCD_Auth_Imp

Authorized SCD import

The TOE shall provide securityfeatures to ensurethat authorised users only may invoke the import of the SCD.

7.1.4 Additional OTs - Trusted Communication with CGA

OT.TOE_SSCD_Auth

Authentication proof as SSCD

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

OT.TOE_TC_SVD_Exp

TOE trusted channel for SVD export

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

7.1.5 Additional OTs - Trusted Communication with SCA

OT.TOE_TC_DTBS_Imp

Trusted channel of TOE for DTBS import

The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS representation received from the SCA. The TOE must not generate digital signatures with the SCD for altered DTBS. Application Note: This security objective for the TOE is partly covering OE.DTBS_Protect from the PP [PP-SSCD2]. While OE.DTBS_Protect in the PP [PP-SSCD2] requires only the operational environment to protect DTBS, this ST requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp.

OT.TOE_TC_VAD_Imp

Trusted channel of TOE for VAD import

The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed. Application Note: This security objective for the TOE is partly covering OE.HID_VAD from the PP [PP-SSCD2]. While OE.HID_VAD in the PP [PP-SSCD2] requires only the operational environment to protect VAD, this ST requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp.

7.2 Security Objectives for the Operational Environment

7.2.1 OEs common to PP SSCD-KG and PP SSCD-KI

OE.SVD_Auth

Authenticity of the SVD

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

OE.CGA_QCert

Generation of qualified certificates

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

- the name of the signatory controlling the TOE,
- the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
- the advanced signature of the CSP. The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a SSCD.

OE.DTBS_Intend

SCA sends data intended to be signed

The signatory shall use a trustworthy SCA that

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

Application Note:

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

OE.Signatory

Security obligation of the signatory

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

7.2.2 Specific OEs from PP SSCD-KI

OE.SCD/SVD_Auth_Gen

Authorized SCD/SVD generation

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

OE.SCD_Secrecy

SCD Secrecy

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

OE.SCD_Unique

Uniqueness of the signature creation data

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

OE.SCD_SVD_Corresp

Correspondence between SVD and SCD

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

7.2.3 Additional OEs - Trusted Communication with CGA

OE.Dev_Prov_Service

Authentic SSCD provided by SSCD Provisioning Service

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

OE.CGA_SSCD_Auth

Preinitialisation of the TOE for SSCD authentication

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

OE.CGA_TC_SVD_Imp

CGA trusted channel for SVD import

The CGA shall detect alteration of the SVD imported from the TOE. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the certificate.

7.2.4 Additional OEs - Trusted Communication with SCA

OE.SCA_TC_DTBS_Exp

Trusted channel of SCA for DTBS export

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS-representation cannot be altered undetected in transit between the SCA and the TOE. Application Note: This security objective for the TOE is partly covering OE.DTBS_Protect from the PP [PP-SSCD2]. While OE.DTBS_Protect in the PP [PP-SSCD2] requires only the operational environment to protect DTBS, this ST requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp.

OE.HID_TC_VAD_Exp

Trusted channel of HID for VAD export

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel. Application Note: This security objective for the TOE is partly covering OE.HID_VAD from the PP [PP-SSCD2]. While OE.HID_VAD in the PP [PP-SSCD2] requires only the operational environment to protect VAD, this ST requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp.

7.3 Security Objectives Rationale

7.3.1 Threats

T.SCD_Divulg addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in recital (18) of the directive. This threat is countered by

OE.SCD_Secrecy, whichassures the secrecy of the SCD in the CSP environment, and

OT.SCD_Secrecy, which assures the secrecy of the SCD during use by the TOE for signature creation. Furthermore, generation and/or import of SCD known by an attacker is countered by OE.SCD/SVD_Auth_Gen, which ensures that only authorized SCD generation in the environment is possible, and OT.SCD_Auth_Imp, which ensures that only authorised SCD import is possible.

T.SCD_Derive deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. OT.SCD/SVD_Auth_Gen and OE.SCD_Unique counter this threat by implementing cryptographically secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographically secure electronic signatures.

T.Hack_Phys 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 deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the 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 and verification of the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP. Additionally T.SVD_Forgery is addressed by OT.TOE_TC_SVD_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA_TC_SVD_Imp, which provides verification of SVD authenticity by the CGA.

T.SigF_Misuse addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create an electronic signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of Annex III [DIRECTIVE]. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. OT.Sigy_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign. The combination of OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission form the SCA to the TOE. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) requires the HID to protect the confidentiality and the integrity of the VAD as needed by the authentication method employed. The HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD). OE.Signatory (Security obligation of the 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 (Security obligation of the signatory) ensures also that the signatory keeps their VAD confidential.

T.DTBS_Forgery addresses the threat arising from modifications of the DTBS/R sent to the TOE for signing which than does not correspond to the DTBS/R corresponding to the DTBS the signatory intends to sign. The threat T.DTBS_Forgery is addressed by the security objectives OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS), which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE. The TOE counters internally this threat by the means of OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensuring the integrity of the DTBS/R inside the TOE. The TOE IT environment also addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE.

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

7.3.2 Organisational Security Policies

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

P.QSign provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

P.Sigy_SSCD requires the TOE to meet Annex III of the directive. The paragraph 1(a) of Annex III is ensured by OT.SCD_Unique and OE.SCD_Unique requiring that the SCD used for signature creation can practically occurs only once. The OT.SCD_Secrecy, OE.SCD_Secrecy, OT.Sig_Secure and OT.EMSEC_Design and OT.Tamper_Resistance address the secrecy of the SCD (cf. paragraph 1(a) of Annex III). OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE. OT.Sigy_SigF and OE.SCD_Secrecy meets the requirement in paragraph 1(c) of Annex III by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others. OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of Annex III as the TOE must not alter the DTBS/R. The usage of SCD under sole control of the signatory is ensured by OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen, OE.SCD/SVD_Auth_Gen, OT.SCD_Auth_Imp, OE.SCD_Secrecy and OT.Sigy_SigF. OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised TOE from an SSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD In the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA_SSCD_Auth and the received SVD is sent by this SSCD as required by OE.CGA_TC_SVD_Imp. Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

P.Sig_Non-Repud deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, that ensure the aspects of signatory's sole control over and responsibility for the electronic signatures generated with the TOE. OE.Dev_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 stored 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). The TOE security feature addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp supported by OE.Dev_Prov_Service enables the verification whether the device presented by the applicant is a SSCD as required by OE.CGA_SSCD_Auth and the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA_TC_SVD_Imp. OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory ensures that the signatory keeps their VAD confidential. The confidentiality of VAD is protected during the transmission between the HI device and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD). OE.DTBS_Intend, OT.DTBS_Integrity_TOE, OE.SCA_TC_DTBS_Exp and OT.TOE_TC_DTBS_Imp ensure that the TOE generates electronic 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 electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature creation data), OT.EMSEC_Design (Provide physical emanations

security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

7.3.3 Assumptions

A.CGA establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert (Generation of qualified certificates), which ensures the generation of qualified certificates, and by OE.SVD_Auth (Authenticity of the SVD), which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

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

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

7.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.SCD_Divulg	OT.SCD_Secrecy, OT.SCD_Auth_Imp, OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy	Section 6.3.1
T.SCD_Derive	OT.SCD/SVD_Auth_Gen, OT.Sig_Secure, OE.SCD_Unique	Section 6.3.1
T.Hack_Phys	OT.SCD_Secrecy, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance	Section 6.3.1
T.SVD_Forgery	OT.SCD_SVD_Corresp, OE.SVD_Auth, OT.TOE_TC_SVD_Exp, OE.CGA_TC_SVD_Imp	Section 6.3.1
T.SigF_Misuse	OT.Lifecycle_Security, OT.Sigy_SigF, OE.DTBS_Intend, OT.TOE_TC_DTBS_Imp, OE.SCA_TC_DTBS_Exp, OT.DTBS_Integrity_TOE, OE.HID_TC_VAD_Exp, OT.TOE_TC_VAD_Imp, OE.Signatory	Section 6.3.1
T.DTBS_Forgery	OT.TOE_TC_DTBS_Imp, OE.SCA_TC_DTBS_Exp, OT.DTBS_Integrity_TOE, OE.DTBS_Intend	Section 6.3.1
T.Sig_Forgery	OT.Sig_Secure, OT.SCD_Unique, OE.CGA_QCert	Section 6.3.1

Table 4 Threats and Security Objectives - Coverage

Security Objectives	Threats
OT.Lifecycle_Security	T.SigF_Misuse
OT.SCD_Secrecy	T.SCD_Divulg, T.Hack_Phys
OT.Sig_Secure	T.SCD_Derive, T.Sig_Forgery
OT.Sigy_SigF	T.SigF_Misuse
OT.DTBS_Integrity_TOE	T.SigF_Misuse, T.DTBS_Forgery
OT.Tamper_ID	T.Hack_Phys
OT.EMSEC_Design	T.Hack_Phys
OT.Tamper_Resistance	T.Hack_Phys
OT.SCD/SVD_Auth_Gen	T.SCD_Derive
OT.SCD_Unique	T.Sig_Forgery
OT.SCD_SVD_Corresp	T.SVD_Forgery
OT.SCD_Auth_Imp	T.SCD_Divulg
OT.TOE_SSCD_Auth	
OT.TOE_TC_SVD_Exp	T.SVD_Forgery
OT.TOE_TC_DTBS_Imp	T.SigF_Misuse, T.DTBS_Forgery
OT.TOE_TC_VAD_Imp	T.SigF_Misuse
OE.SVD_Auth	T.SVD_Forgery
OE.CGA_QCert	T.Sig_Forgery
OE.DTBS_Intend	T.SigF_Misuse, T.DTBS_Forgery
OE.Signatory	T.SigF_Misuse
OE.SCD/SVD_Auth_Gen	T.SCD_Divulg
OE.SCD_Secrecy	T.SCD_Divulg
OE.SCD_Unique	T.SCD_Derive
OE.SCD_SVD_Corresp	
OE.Dev_Prov_Service	
OE.CGA_SSCD_Auth	
OE.CGA_TC_SVD_Imp	T.SVD_Forgery
OE.SCA_TC_DTBS_Exp	T.SigF_Misuse, T.DTBS_Forgery
OE.HID_TC_VAD_Exp	T.SigF_Misuse

Table 5 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.CSP_QCert	OE.CGA_QCert, OT.TOE_SSCD_Auth, OE.CGA_SSCD_Auth, OT.SCD_SVD_Corresp, OT.Lifecycle_Security, OT.SCD_Auth_Imp, OE.SCD/SVD_Auth_Gen	Section 6.3.2
P.QSign	OT.Sigy_SigF, OT.Sig_Secure, OE.CGA_QCert, OE.DTBS_Intend	Section 6.3.2
P.Sigy_SSCD	OT.SCD_Unique, OT.SCD_Secrecy, OT.Sig_Secure, OT.EMSEC_Design, OT.Tamper_Resistance, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen, OT.TOE_SSCD_Auth, OT.TOE_TC_SVD_Exp, OE.CGA_SSCD_Auth, OE.CGA_TC_SVD_Imp, OT.SCD_Auth_Imp, OE.Dev_Prov_Service, OE.SCD_Unique, OE.SCD_Secrecy, OE.SCD/SVD_Auth_Gen	Section 6.3.2
P.Sig_Non-Repud	OE.CGA_QCert, OE.SVD_Auth, OT.SCD_SVD_Corresp, OT.SCD_Unique, OE.Signatory, OT.TOE_SSCD_Auth, OT.TOE_TC_SVD_Exp, OE.CGA_SSCD_Auth, OE.CGA_TC_SVD_Imp, OT.Sigy_SigF, OE.HID_TC_VAD_Exp, OT.TOE_TC_VAD_Imp, OE.DTBS_Intend, OT.DTBS_Integrity_TOE, OE.SCA_TC_DTBS_Exp, OT.TOE_TC_DTBS_Imp, OT.Sig_Secure, OT.Lifecycle_Security, OT.SCD_Secrecy, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, OE.Dev_Prov_Service	Section 6.3.2

Table 6 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
OT.Lifecycle_Security	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud
OT.SCD_Secrecy	P.Sigy_SSCD, P.Sig_Non-Repud
OT.Sig_Secure	P.QSign, P.Sigy_SSCD, P.Sig_Non-Repud
OT.Sigy_SigF	P.QSign, P.Sigy_SSCD, P.Sig_Non-Repud
OT.DTBS_Integrity_TOE	P.Sigy_SSCD, P.Sig_Non-Repud
OT.Tamper_ID	P.Sig_Non-Repud
OT.EMSEC_Design	P.Sigy_SSCD, P.Sig_Non-Repud
OT.Tamper_Resistance	P.Sigy_SSCD, P.Sig_Non-Repud
OT.SCD/SVD_Auth_Gen	P.Sigy_SSCD
OT.SCD_Unique	P.Sigy_SSCD, P.Sig_Non-Repud
OT.SCD_SVD_Corresp	P.CSP_QCert, P.Sig_Non-Repud
OT.SCD_Auth_Imp	P.CSP_QCert, P.Sigy_SSCD
OT.TOE_SSCD_Auth	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud
OT.TOE_TC_SVD_Exp	P.Sigy_SSCD, P.Sig_Non-Repud
OT.TOE_TC_DTBS_Imp	P.Sig_Non-Repud
OT.TOE_TC_VAD_Imp	P.Sig_Non-Repud
OE.SVD_Auth	P.Sig_Non-Repud
OE.CGA_QCert	P.CSP_QCert, P.QSign, P.Sig_Non-Repud
OE.DTBS_Intend	P.QSign, P.Sig_Non-Repud
OE.Signatory	P.Sig_Non-Repud
OE.SCD/SVD_Auth_Gen	P.CSP_QCert, P.Sigy_SSCD
OE.SCD_Secrecy	P.Sigy_SSCD
OE.SCD_Unique	P.Sigy_SSCD
OE.SCD_SVD_Corresp	
OE.Dev_Prov_Service	P.Sigy_SSCD, P.Sig_Non-Repud
OE.CGA_SSCD_Auth	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud
OE.CGA_TC_SVD_Imp	P.Sigy_SSCD, P.Sig_Non-Repud
OE.SCA_TC_DTBS_Exp	P.Sig_Non-Repud
OE.HID_TC_VAD_Exp	P.Sig_Non-Repud

Table 7 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.CGA	OE.CGA_QCert, OE.SVD_Auth	Section 6.3.3
A.SCA	OE.DTBS_Intend	Section 6.3.3
A.CSP	OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OE.SCD_SVD_Corresp	Section 6.3.3

Table 8 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions
OE.SVD_Auth	A.CGA
OE.CGA_QCert	A.CGA
OE.DTBS_Intend	A.SCA
OE.Signatory	
OE.SCD/SVD_Auth_Gen	A.CSP
OE.SCD_Secrecy	A.CSP
OE.SCD_Unique	A.CSP
OE.SCD_SVD_Corresp	A.CSP
OE.Dev_Prov_Service	
OE.CGA_SSCD_Auth	
OE.CGA_TC_SVD_Imp	
OE.SCA_TC_DTBS_Exp	
OE.HID_TC_VAD_Exp	

Table 9 Security Objectives for the Operational Environment and Assumptions - Coverage

8 Extended Requirements

8.1 Extended Families

8.1.1 Extended Family FPT_EMS - TOE Emanation

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

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS TOE Emanation	1

FPT_EMS.1 TOE Emanation has two constituents:

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

Management:

There are no management activities foreseen.

Audit:

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

Definition:

FPT_EMS.1 TOE Emanation

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

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

Dependencies: No dependencies.

8.1.2 Extended Family FIA_API - Authentication Proof of Identity

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

Family behaviour:

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

Component levelling:

FIA_API Authentication Proof of Identity	**1**

FIA_API.1 Authentication Proof of Identity

Management:

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

Audit:

There are no actions defined to be auditable.

Definition :

FIA_API.1 Authentication Proof of Identity

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

Dependencies: No dependencies.

8.1.3 Extended Family FCS_RND - Quality Metric for Random Numbers

To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

Family behaviour:

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

Component levelling:

FCS_RND Generation of random numbers	**1**

FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management:

There are no management activities foreseen

Audit:

There are no actions defined to be auditable.

Definition:

FCS_RND.1 Quality Metric for Random Numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].

Dependencies: No dependencies.

9 Security Requirements

9.1 Security Functional Requirements

This section describes the requirements imposed on the TOE in order to achieve the security objectives laid down in the previous chapter.

9.1.1 Cryptographic support (FCS)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 [Editorially Refined] The TSF shall generate **SCD/SVD** pair in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[cryptographic key sizes]** that meet the following: **[list of standards]**.

The assignments of the cryptographic operations are described in the table below:

cryptographic key generation algorithm	cryptographic key sizes	list of standards
EC key pair generation	256, 384, 512 and 521 bits	ANS X9.62
RSA CRT key pair generation	1024, 1536, 2048, 2560 and 3072 bits	RSA PKCS1 v2.1

Refinement:

substitution of cryptographic keys by SCD/SVD pairs.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Key overwriting** that meets the following: **the method of the underlying platform**.

Application Note:

The destruction method is provided by the underlying platform. The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 [Editorially Refined] The TSF shall perform **[cryptographic operations]** in accordance with a specified cryptographic algorithm **[cryptographic algotithm]** and cryptographic key sizes **[key sizes]** that meet the following: **[Norms]**.

Refinement:

The assignments of the cryptographic operations are described in the table below:

Cryptographic operation	Algorithms	Key size	Norms
Digital signature computation	RSA PKCS#1v1.5, RSA-PSS PKCS#1 v2.1, with SHA-1 SHA-224 SHA-256 SHA-384 or SHA-512	1024, 1536, 2048, 2560, and 3072 bits	RSA PKCS1 v2.1
Digital signature computation	ECDSA with SHA-1 SHA-224 SHA-256 SHA-384 or SHA-512	256, 384, 512, 521 bits	Signature Creation: ANSI_X9.62-2005, Public key cryptography for the financial services Industry: The elliptic curve digital signature algorithm (ECDSA), ANSI, 2005-11-16, section 7.3
Symmetric Mutual authentication for secure messaging	3DES with SHA-1, SHA-256	128 bits	Addendum IAS-ECC v1.0.1
Symmetric Mutual authentication for secure messaging	AES with SHA-256	128, 192, 256 bits	Addendum IAS-ECC v1.0.1
PACE Authentication	PACE IM and GM with DH, ECDH, DES, AES	256, 384, 512, 521 bits AES: 128 192 256, DES:128	ICAO Technical Report- Supplemental Access Control for Machine Readable Travel Documents Release: 1.01 November 2010
Symmetric Role Authentication	3DES CBC EDE 128 bits (encipherment) + Retail MAC or AES CBC 128 bits (encipherment) + C-MAC	128 bits	Addendum IAS-ECC v1.0.1
Secure messaging - Encryption/decryption	3DES in CBC mode or AES in CBC mode	3DES: 128 bits, AES::128, 192, 256 bits	Addendum IAS-ECC v1.0.1

secure messaging - MAC generation and verification	ISO/IEC 9797-1 algorithm 3 padding 2 (3DES) or CMAC (AES)	3DES: 128 bits, AES::128, 192, 256 bits	DES: ISO9797 - AES: NIST SP 800-38B
Hash calculation within the digital signature sequence	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	none	NIST FIPS PUB 180-2
Ciphering key encryption	RSA PKCS#1v1.5	1024, 1536, 2048, 2560, and 3072 bits	RSA PKCS1 v2.1
Ciphering key decryption	RSA-OAEP, PKCS#1 v2.1, RSA PKCS#1v1.5	1024, 1536, 2048, 2560, and 3072 bits	RSA PKCS1 v2.1
Random number generation	ANSI X9.31	none	NIST-Recommended Random Number Generator Based on ANSI X9.31

Application Note:

The operations in the element FCS_COP.1.1 shall be appropriate for the SCD/SVD pairs generated according to FCS_CKM.1. Note that for some cryptographic algorithm like RSA padding is important part of the signature creation algorithm.

FCS_RND.1 Quality Metric for Random Numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **AIS31 Class P2 quality metric**.

Application Note:

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 platform.

9.1.2 User data protection (FDP)

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

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

FDP_ACC.1/SCD/SVD_Generation Subset access control

FDP_ACC.1.1/SCD/SVD_Generation The TSF shall enforce the **SCD/SVD Generation SFP** on

subjects: S.User,

objects: SCD, SVD,

operations: generation of SCD/SVD pair.

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

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

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

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

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

FDP_ACC.1/SVD_Transfer Subset access control

FDP_ACC.1.1/SVD_Transfer The TSF shall enforce the **SVD Transfer SFP** on

subjects: S.User,

objects: SVD,

operations: export.

Application Note:

When SCD is generated in the TOE, FDP_ACC.1/SVD Transfer SFP will be required to export the SVD to the CGA for certification.

FDP_ACF.1/SVD_Transfer Security attribute based access control

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

the S.User is associated with the security attribute Role,

the SVD.

FDP_ACF.1.2/SVD_Transfer The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **R.Admin and R.Sigy are allowed to export SVD**.

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

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

FDP_ACC.1/Signature_Creation Subset access control

FDP_ACC.1.1/Signature_Creation The TSF shall enforce the **Signature Creation SFP** on **Sending of DTBS/R by SCA and Signing of DTBS/R by Signatory:**

subjects: S.User,

objects: DTBS/R, SCD,

operations: signature creation.

FDP_ACF.1/Signature_Creation Security attribute based access control

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

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

the SCD with the security attribute "SCD Operational".

FDP_ACF.1.2/Signature_Creation The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is

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

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

FDP_ACF.1.4/Signature_Creation The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no"**.

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **SCD**.

FDP_SDI.2/Persistent Stored data integrity monitoring and action

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

prohibit the use of the altered data

inform the S.Sigy about integrity error.

Application Note:

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

SCD,

SVD (if persistent stored by TOE).

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

FDP_SDI.2/DTBS Stored data integrity monitoring and action

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
prohibit the use of the altered data
inform the S.Sigy about integrity error.

Application Note:

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

FDP_ACC.1/SCD_Import Subset access control

FDP_ACC.1.1/SCD_Import The TSF shall enforce the **SCD Import SFP** on
subjects: S.User,
objects: SCD,
operations: import of SCD.

FDP_ACF.1/SCD_Import Security attribute based access control

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

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

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

FDP_ACF.1.4/SCD_Import The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to import SCD**.

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

FDP_ITC.1.1/SCD The TSF shall enforce the **SCD Import SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/SCD [Editorially Refined] The TSF shall ignore any security attributes associated with the **SCD** when imported from outside the TOE.

FDP_ITC.1.3/SCD The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

FDP_UCT.1/SCD Basic data exchange confidentiality

FDP_UCT.1.1/SCD [Editorially Refined] The TSF shall enforce the **SCD Import SFP** to **receive SCD** in a manner protected from unauthorised disclosure.

FDP_DAU.2/SVD Data Authentication with Identity of Guarantor

FDP_DAU.2.1/SVD The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **SVD**.

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

FDP_UIT.1/DTBS Data exchange integrity

FDP_UIT.1.1/DTBS The TSF shall enforce the **signature creation SFP** to **receive** user data in a manner protected from **modification and insertion** errors.

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

9.1.3 Identification and authentication (FIA)

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

Self-test according to FPT_TST.1,

Identification of the user by means of TSF required by FIA_UID.1,

establishing a trusted channel between CGA and the TOE by means of TSF required by FTP_ITC.1/SVD (additional requirement allowed by [PP-SSCD2] and [PP-SSCD5]),

establishing a trusted channel between SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS ([PP-SSCD5]),

establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD ([PP-SSCD5]),

none

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

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

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

Self-test according to FPT_TST.1,

Identification of the user by means of TSF required by FIA_UID.1,

establishing a trusted channel between CGA and the TOE by means of TSF required by FTP_ITC.1/SVD (additional requirement allowed by [PP-SSCD2] and [PP-SSCD5]),

establishing a trusted channel between SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS ([PP-SSCD5]),

establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD ([PP-SSCD5]),

none

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.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer within 1 byte [0 - 255]**

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**.

Application Note:

The administrator configurable positive integer shall be defined during the personalization phase.

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a

- **3DES Symmetric Mutual Authentication Authentication according to Addendum IAS-ECC v1.0.1**
- **AES Symmetric Mutual Authentication Authentication according to Addendum IAS-ECC v1.0.1**
- **PACE Authentication according to [ICAO]**
- **3DES Symmetric Role Authentication according to Addendum IAS-ECC v1.0.1**
- **AES Symmetric Role Authentication according to Addendum IAS-ECC v1.0.1**
- **RSA Digital Signature computation according to RSA PKCS1 v2.1**
- **ECDSA Digital Signature computation according to Signature Creation: ANSI_X9.62-2005, Public key cryptography for the financial services Industry: The elliptic curve digital signature algorithm (ECDSA), ANSI, 2005-11-16, section 7.3**

to prove the identity of the **SSCD**.

9.1.4 Security management (FMT)

FMT_SMR.1 Security roles

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.

FMT_SMF.1 Specification of Management Functions

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

- **Creation and modification of RAD,**
- **Enabling the signature creation function,**
- **Modification of the security attribute SCD/SVD management, SCD operational,**
- **Change the default value of the security attribute SCD Identifier,**
- **none**.

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **enable** the functions **signature creation function** to **R.Sigy**.

FMT_MSA.1/Admin Management of security attributes

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**.

FMT_MSA.1/Signatory Management of security attributes

FMT_MSA.1.1/Signatory The TSF shall enforce the **Signature Creation SFP** to restrict the ability to **modify** the security attributes **SCD operational** to **R.Sigy**.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for **SCD/SVD Management and SCD operational**.

FMT_MSA.3 Static attribute initialisation

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.

FMT_MSA.4 Security attribute value inheritance

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

Application Note:

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

FMT_MTD.1/Admin Management of TSF data

FMT_MTD.1.1/Admin The TSF shall restrict the ability to **create** the **RAD** to **R.Admin**.

FMT_MTD.1/Signatory Management of TSF data

FMT_MTD.1.1/Signatory The TSF shall restrict the ability to **modify** the **RAD** to **R.Sigy**.

9.1.5 Protection of the TSF (FPT)

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **side channel** in excess of **state of the art** enabling access to **SCD** and **RAD**.

FPT_EMS.1.2 The TSF shall ensure **that unauthorized users** are unable to use the following interface **external contacts** to gain access to **RAD** and **SCD**.

Application Note:

The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission. Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state of the art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

self-test according to FPT_TST fails (1),
power shortage,
over and under voltage,
over and under clock frequency,
over and under temperature,
integrity problems,
unexpected abortion of the execution of the TSF due to external events,
none.

Application Note:

The assignment (1) addresses failures detected by a failed self-test and requiring appropriate action to prevent security violation. When the TOE is in a secure state the TSF shall not perform any cryptographic operations and all data output interfaces shall be inhibited by the TSF.

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **resist physical manipulation and physical probing** to the **TSF** by responding automatically such that the SFRs are always enforced.

Application Note:

The TOE implements appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here:

assuming that there might be an attack at any time,

countermeasures are provided at any time.

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up** to demonstrate the correct operation of **the TSF**.

FPT_TST.1.2 The TSF shall provide 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 **stored TSF executable code**.

9.1.6 Trusted Path/Channel (FTP)

FTP_ITC.1/SVD Inter-TSF trusted channel

FTP_ITC.1.1/SVD [Editorially Refined] The TSF shall provide a communication channel between itself and another trusted IT product **CGA** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SVD [Editorially Refined] The TSF shall permit another trusted IT product **CGA** to initiate communication via the trusted channel.

FTP_ITC.1.3/SVD [Editorially Refined] The TSF **or the CGA** shall initiate communication via the trusted channel for:

according to FIA_UAU.1

none.

FTP_ITC.1/SCD Inter-TSF trusted channel

FTP_ITC.1.1/SCD The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SCD The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/SCD The TSF shall initiate communication via the trusted channel for

Data exchange integrity according to FDP_UCT.1/SCD,

none.

FTP_ITC.1/DTBS Inter-TSF trusted channel

FTP_ITC.1.1/DTBS [Editorially Refined] The TSF shall provide a communication channel between itself and another trusted IT product **SCA** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/DTBS [Editorially Refined] The TSF shall permit another trusted IT product **SCA** to initiate communication via the trusted channel.

FTP_ITC.1.3/DTBS [Editorially Refined] The TSF **or the SCA** shall initiate communication via the trusted channel for:

user authentication according to FIA_UAU.1

signature creation

none.

FTP_ITC.1/VAD Inter-TSF trusted channel

FTP_ITC.1.1/VAD [Editorially Refined] The TSF shall provide a communication channel between itself and another trusted IT product **HID** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/VAD [Editorially Refined] The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/VAD [Editorially Refined] The TSF **or the HID** shall initiate communication via the trusted channel for:

user authentication according to FIA_UAU.1

signature creation
none.

Application Note:

Note the VAD needs protection depending on the authentication methods employed: VAD for authentication by knowledge needs protection in confidentiality; VAD for biometric authentication may need protection in integrity only.

9.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL5 augmented with AVA_VAN.5 and ALC_DVS.2.

9.3 Security Requirements Rationale

9.3.1 Objectives

9.3.1.1 Security Objectives for the TOE

OTs common to PP SSCD-KG and PP SSCD-KI

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

OT.SCD_Secrecy OT.SCD_Secrecy is provided by the security functions specified by the following SFR. FDP_UCT.1/SCD and FTP_ITC.1/SCD ensures the confidentiality for SCD import. FCS_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information. The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the

security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA). SFR FPT_EMS.1 and

FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

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

OT.Sigy_SigF OT.Sigy_SigF is provided by an SFR for identification authentication and access control. FIA_UAU.1 and FIA_UID.1 ensure that no signature creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process). The security functions specified by FDP_ACC.1/Signature_Creation and FDP_ACF.1/Signature_Creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory. FMT_MOF.1 restricts the ability to enable the signature creation function to the signatory. FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

OT.DTBS_Integrity_TOE OT.DTBS_Integrity_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.Tamper_ID OT.Tamper_ID is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

OT.EMSEC_Design OT.EMSEC_Design covers that no intelligible information is emanated. This is provided by FPT_EMS.1.1.

OT.Tamper_Resistance OT.Tamper_Resistance is provided by FPT_PHP.3 to resist physical attacks.

Specific OTs from PP SSCD-KG

OT.SCD/SVD_Auth_Gen OT.SCD/SVD_Auth_Gen addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The SFR FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation provide access control for the SCD/SVD generation. The security attributes of

the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute initialisation. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute 'SCD operational' of the SCD.

OT.SCD_Unique OT.SCD_Unique implements the requirement of practically unique SCD as laid down in Annex III, paragraph 1(a) [DIRECTIVE], which is provided by the cryptographic algorithms specified by FCS_CKM.1. FCS_RND.1 contributes to OT.SCD_Unique, because a random number generator with the required qualitiy of metric used by the key generation algorithms will ensure the uniqueness of the SCD.

OT.SCD_SVD_Corresp OT.SCD_SVD_Corresp 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.

Specific OTs from PP SSCD-KI

OT.SCD_Auth_Imp OT.SCD_Auth_Imp (Authorized SCD import) is provided by the security functions specified by the following SFR. FIA_UID.1 and FIA_UAU.1 ensure that the user is identified and authenticated before SCD can be imported. FDP_ACC.1/SCD_Import and FDP_ACF.1/SCD_Import ensure that only authorised users can import SCD.

Additional OTs - Trusted Communication with CGA

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

OT.TOE_TC_SVD_Exp OT.TOE_TC_SVD_Exp requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA, which is directly provided by: o the SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer; o FTP_ITC.1/SVD inter-TSF trusted channel, which requires the TOE to provide a trusted channel to the CGA. o FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor), which requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.

Additional OTs - Trusted Communication with SCA

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

OT.TOE_TC_VAD_Imp OT.TOE_TC_VAD_Imp is provided by FTP_ITC.1/VAD to provide a trusted channel to protect the VAD provided by the HID to the TOE.

9.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.Lifecycle_Security	FCS_CKM.1, FCS_COP.1, FCS_CKM.4, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FDP_ACC.1/SVD_Transfer, FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, FDP_ACF.1/SVD_Transfer, 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_SMR.1, FMT_SMF.1, FPT_TST.1, FDP_ITC.1/SCD, FDP_UCT.1/SCD, FTP_ITC.1/SCD, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import	Section 8.3.1
OT.SCD_Secrecy	FCS_CKM.1, FCS_CKM.4, FDP_RIP.1, FDP_SDI.2/Persistent, FPT_FLS.1, FPT_PHP.3, FPT_TST.1, FPT_EMS.1, FDP_UCT.1/SCD, FTP_ITC.1/SCD	Section 8.3.1
OT.Sig_Secure	FDP_SDI.2/Persistent, FCS_COP.1, FPT_TST.1	Section 8.3.1
OT.Sigy_SigF	FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, FDP_RIP.1, FDP_SDI.2/DTBS, FIA_AFL.1, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMR.1, FMT_SMF.1	Section 8.3.1
OT.DTBS_Integrity_TOE	FDP_SDI.2/DTBS	Section 8.3.1
OT.Tamper_ID	FPT_PHP.1	Section 8.3.1
OT.EMSEC_Design	FPT_EMS.1	Section 8.3.1
OT.Tamper_Resistance	FPT_PHP.3	Section 8.3.1
OT.SCD/SVD_Auth Gen	FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FIA_UAU.1, FIA_UID.1, FMT_MSA.1/Admin, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4	Section 8.3.1
OT.SCD_Unique	FCS_CKM.1, FCS_RND.1	Section 8.3.1

OT.SCD_SVD_Corresp	FCS_CKM.1, FDP_SDI.2/Persistent, FMT_MSA.4, FMT_SMF.1	Section 8.3.1
OT.SCD_Auth_Imp	FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FIA_UAU.1, FIA_UID.1	Section 8.3.1
OT.TOE_SSCD_Auth	FIA_UAU.1, FIA_API.1	Section 8.3.1
OT.TOE_TC_SVD_Exp	FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer, FTP_ITC.1/SVD, FDP_DAU.2/SVD	Section 8.3.1
OT.TOE_TC_DTBS_Imp	FTP_ITC.1/DTBS, FDP_UIT.1/DTBS	Section 8.3.1
OT.TOE_TC_VAD_Imp	FTP_ITC.1/VAD	Section 8.3.1

Table 10 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FCS_CKM.1	OT.Lifecycle_Security, OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.SCD_Secrecy
FCS_CKM.4	OT.Lifecycle_Security, OT.SCD_Secrecy
FCS_COP.1	OT.Lifecycle_Security, OT.Sig_Secure
FCS_RND.1	OT.SCD_Unique
FDP_ACC.1/SCD/SVD_Generation	OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen
FDP_ACF.1/SCD/SVD_Generation	OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen
FDP_ACC.1/SVD_Transfer	OT.TOE_TC_SVD_Exp, OT.Lifecycle_Security
FDP_ACF.1/SVD_Transfer	OT.TOE_TC_SVD_Exp, OT.Lifecycle_Security
FDP_ACC.1/Signature_Creation	OT.Lifecycle_Security, OT.Sigy_SigF
FDP_ACF.1/Signature_Creation	OT.Lifecycle_Security, OT.Sigy_SigF
FDP_RIP.1	OT.SCD_Secrecy, OT.Sigy_SigF
FDP_SDI.2/Persistent	OT.SCD_SVD_Corresp, OT.SCD_Secrecy, OT.Sig_Secure
FDP_SDI.2/DTBS	OT.Sigy_SigF, OT.DTBS_Integrity_TOE
FDP_ACC.1/SCD_Import	OT.SCD_Auth_Imp, OT.Lifecycle_Security
FDP_ACF.1/SCD_Import	OT.SCD_Auth_Imp, OT.Lifecycle_Security
FDP_ITC.1/SCD	OT.Lifecycle_Security
FDP_UCT.1/SCD	OT.Lifecycle_Security, OT.SCD_Secrecy
FDP_DAU.2/SVD	OT.TOE_TC_SVD_Exp
FDP_UIT.1/DTBS	OT.TOE_TC_DTBS_Imp
FIA_UID.1	OT.SCD/SVD_Auth_Gen, OT.Sigy_SigF, OT.SCD_Auth_Imp
FIA_UAU.1	OT.TOE_SSCD_Auth, OT.SCD/SVD_Auth_Gen, OT.Sigy_SigF, OT.SCD_Auth_Imp

FIA_AFL.1	OT.Sigy_SigF
FIA_API.1	OT.TOE_SSCD_Auth
FMT_SMR.1	OT.Lifecycle_Security, OT.Sigy_SigF
FMT_SMF.1	OT.Lifecycle_Security, OT.SCD_SVD_Corresp, OT.Sigy_SigF
FMT_MOF.1	OT.Lifecycle_Security, OT.Sigy_SigF
FMT_MSA.1/Admin	OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen
FMT_MSA.1/Signatory	OT.Lifecycle_Security, OT.Sigy_SigF
FMT_MSA.2	OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen, OT.Sigy_SigF
FMT_MSA.3	OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen, OT.Sigy_SigF
FMT_MSA.4	OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen, OT.SCD_SVD_Corresp, OT.Sigy_SigF
FMT_MTD.1/Admin	OT.Lifecycle_Security, OT.Sigy_SigF
FMT_MTD.1/Signatory	OT.Lifecycle_Security, OT.Sigy_SigF
FPT_EMS.1	OT.SCD_Secrecy, OT.EMSEC_Design
FPT_FLS.1	OT.SCD_Secrecy
FPT_PHP.1	OT.Tamper_ID
FPT_PHP.3	OT.SCD_Secrecy, OT.Tamper_Resistance
FPT_TST.1	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure
FTP_ITC.1/SVD	OT.TOE_TC_SVD_Exp
FTP_ITC.1/SCD	OT.Lifecycle_Security, OT.SCD_Secrecy
FTP_ITC.1/DTBS	OT.TOE_TC_DTBS_Imp
FTP_ITC.1/VAD	OT.TOE_TC_VAD_Imp

Table 11 SFRs and Security Objectives

9.3.3 Dependencies

9.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1
FCS_COP.1	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_RND.1	No Dependencies	
FDP_ACC.1/SCD/SVD_Generation	(FDP_ACF.1)	FDP_ACF.1/SCD/SVD_Generation
FDP_ACF.1/SCD/SVD_Generation	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACC.1/SVD_Transfer	(FDP_ACF.1)	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SVD_Transfer	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDP_ACC.1/Signature_Creation	(FDP_ACF.1)	FDP_ACF.1/Signature_Creation
FDP_ACF.1/Signature_Creation	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_RIP.1	No Dependencies	
FDP_SDI.2/Persistent	No Dependencies	
FDP_SDI.2/DTBS	No Dependencies	
FDP_ACC.1/SCD_Import	(FDP_ACF.1)	FDP_ACF.1/SCD_Import
FDP_ACF.1/SCD_Import	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SCD_Import, FMT_MSA.3

FDP_ITC.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_UCT.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/SCD_Import, FTP_ITC.1/SCD
FDP_DAU.2/SVD	(FIA_UID.1)	FIA_UID.1
FDP_UIT.1/DTBS	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FIA_UID.1	No Dependencies	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FIA_AFL.1	(FIA_UAU.1)	FIA_UAU.1
FIA_API.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FMT_SMF.1	No Dependencies	
FMT_MOF.1	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_SMF.1

FMT_MSA.2	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.4	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FPT_EMS.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_PHP.1	No Dependencies	
FPT_PHP.3	No Dependencies	
FPT_TST.1	No Dependencies	
FTP_ITC.1/SVD	No Dependencies	
FTP_ITC.1/SCD	No Dependencies	
FTP_ITC.1/DTBS	No Dependencies	
FTP_ITC.1/VAD	No Dependencies	

Table 12 SFRs Dependencies

9.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	(ADV_IMP.1) and (ADV_TDS.1)	ADV_IMP.1, ADV_TDS.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4, ALC_TAT.2
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	(ADV_FSP.5)	ADV_FSP.5
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.5
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.5, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.2	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	(ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3

Table 13 SARs Dependencies

9.3.4 Rationale for the Security Assurance Requirements

The assurance level for this ST is EAL5+ augmented. The TOE is semiformally designed and tested. EAL5+ allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. The TOE is intended to operate in open environments, where attackers can easily exploit vulnerabilities. According to the usage of the TOE, it represents a significant value to perform attacks. In some malicious usages, of the TOE the statistical or probabilistic mechanisms in the TOE, for instance, may be subjected to analysis and attack in the normal course of operation. This level seems to be the reasonable minimum level for card hosting sensitive operations.

9.3.5 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.

9.3.6 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. Due to the nature of the TOE, there is a need to justify the sufficiency of these procedures to protect the confidentiality and the integrity of the TOE. The TOE shall be protected in confidentiality and integrity during its development to meet the security objective OT.Lifecycle_Security.

10 TOE Summary Specification

10.1 TOE Summary Specification

This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The summary is structured in security functions. The security functionalities concerning the IC and the JC Platform are described in [ST-IC], [ST-PL] and are not redefined in this security target, although they must be considered for the TOE.

10.1.1 Chip security functionalities

The following functionalities of the product are directly addressed by the chip. The complete list the chip security functionality can be check in the chip Security Target [ST-IC].

SF.IC_INTEGRITY

This SF is responsible for:

- correcting single bit fails upon a read operation on each NVM byte,
- verifying valid CPU usage,
- checking integrity loss when accessing NVM, ROM or RAM,
- providing a sign engine to check code and/or data integrity loss,
- monitoring various manifestations of fault injection attempts,
- providing a security timeout feature (watchdog timer),
- providing the embedded software developer with the traceability information of the TOE.

SF.PHYSICAL_TAMPERING

This SF ensures that:

- The TOE detects clock and voltage supply operating changes by the environment,
- The TOE detects attempts to violate its physical integrity, and glitch attacks,
- The TOE is always clocked with shape and timing within specified operating conditions.

SF.SECURITY_ADMIN

This SF ensures the management of the following security violation attempts:

- Incorrect CPU usage,
- Integrity loss in NVM, ROM or RAM
- Code signature alarm,
- Fault injection attempt,
- access attempt to unavailable or reserved memory areas,
- MPU errors,
- Clock and voltage supply operating changes,

- o TOE physical integrity abuse.

SF.UNOBSERVABILITY

This SF prevents the disclosure of user data and of TSF data when it is transmitted between separate parts of the TOE (the different memories, the CPU and other functional units of the TOE such as a cryptographic co-processor are seen as separated parts of the TOE). This SF provides protection mechanism of the TOE towards observation and physical tampering, such as random delay and desynchronisation capability.

SF.SYM_CRYPTO

This SF provides AES and TDES data encryption/decryption capability, in order to compute Message Authentication code (MAC) or the encrypted data.

SF.ASYM_CRYPTO

This SF provides:

- o RSA verification (encryption),
- o RSA signature (decryption),
- o RSA private and public keys computation,
- o Prime number generation up to 3200 bits, with Rabin-Miller primality tests. This functionality implements also the following standard hash function:
- o SHA-1 hash function,
- o SHA-224 hash function,
- o SHA-256 hash function,
- o SHA-384 hash function,
- o SHA-512 hash function. This security function provides also the following basic functions for Elliptic Curves Cryptography over prime fields:
- o general point addition,
- o point expansion and compression,
- o public scalar multiplication,
- o private scalar multiplication.

SF.ALEAS

This SF provides a hardware Random Number Generator (RNG) to support security operations performed by cryptographic applications. The RNG complies with the AIS31 Class P2 quality metric.

10.1.2 Platform security functionalities

SF.RNG

This SF manages random number generation in compliance with X9.31. This function calls SF.ALEAS to initialise the seed key.

SF.ACCESS

This SF manages the access to objects (files, directories, data and secrets) stored in EEPROM.

SF.INIT

This SF is called after each reset of the card.

SF.MEMORY

This SF manages memory erasure.

SF.CHECK

This SF tests the integrity of the different items.

SF.TEST

This SF runs tests at start-up.

SF.AUDIT

This SF reacts when a fault or an anomaly is detected.

10.1.3 Application manager security functions

SF.GESTION

At start-up of the card, this SF calls SF.INIT and then waits for a command sent by the terminal. This command is then executed or transmitted to another module or application.

10.1.4 Application security functionalities

SF.AUTHENTICATION

Only authenticated terminals can get access to the user data stored on the TOE.

SF.APP_CRYPTO

This SF performs high level cryptographic operations.

SF.APP_INTEGRITY

This security functionality monitors the integrity of sensitive user data and the integrity of the DTBS/R.

SF.RATIF

A counter is associated to a secret key, to a password and to the VAD, which is used to count the number of successive unsuccessful authentication attempts.

SF.TRUSTED_CHANNEL

This SF realizes a secure communication channel to verify authenticity and integrity as well as securing confidentiality of user data between the TOE and other devices connected.

SF.MANAGEMENT

This SF manages the access to objects stored in the ID.me file system. It also controls write access to specific data as personalization data. This SF controls the RAD/VAD management, including the Cardholder (signatory) authentication.