IDEMIA

ID-One CNS V2

Public Security Target

About IDEMIA

OT-Morpho is now IDEMIA, the global leader in trusted identities for an increasingly digital world, with the ambition to empower citizens and consumers alike to interact, pay, connect, travel and vote in ways that are now possible in a connected environment.

Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, we reinvent the way we think, produce, use and protect this asset, whether for individuals or for objects. We ensure privacy and trust as well as guarantee secure, authenticated and verifiable transactions for international clients from Financial, Telecom, Identity, Security and IoT sectors.

With close to €3bn in revenues, IDEMIA is the result of the merger between OT (Oberthur Technologies) and Safran Identity & Security (Morpho). This new company counts 14,000 employees of more than 80 nationalities and serves clients in 180 countries.

| For more information, visit www.idemia.com / Follow @IdemiaGroup on Twitter

DOCUMENT MANAGEMENT

Business Unit – Department	**CI – R&D**
Document type	**FQR**
Document Title	**ID-One CNS V2 Public Security Target**
FQR No	**550 0012**
FQR Issue	**1**

DOCUMENT REVISION

Date	Revision	Modification
2019/02/14	1.0	Creation of the document
2019/03/05	1.1	Update following BRS comments
2019/04/12	1.2	Update of ST for QSCD
2019/04/15	1.3	Update after review of QSCD related changes

Table of contents

TABLE OF FIGURES

TABLE OF TABLES

1 Technical terms, Abbreviation and Associated references

1.1 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 [DIR] and [REG]:* *(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.*
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.*

Term	Definition
Certificate-generation application (CGA)	*collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate*
Certificate revocation list	*A list of revoked certificates issued by a certificate authority*
Certification service provider (CSP)	*entity that issues certificates or provides other services related to electronic signatures*
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.*
Java Card	*A smart card with a Java Card operation system.*
Legitimate user	*A 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.*

Term	Definition
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.*
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.*
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) [DIR]*
Qualified electronic signature	*Advanced electronic signature that has been created with an SSCD with a key certified with a qualified certificate ([DIR]: 5.1).*
Qualified signature creation device (QSCD)	*Personalized device that meets the requirements laid down in [REG], Annex II.*
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)	*ersonalized device that meets the requirements laid down in [DIR], Annex III by being evaluated according to this security target ([DIR]: 2.5 and 2.6).*
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.*

Term	Definition
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*
Smart card	*A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (FLASH) memory, i.e. which can carry out its own calculations in contrast to a simple storage card. Sometimes a smart card has a numerical coprocessor (NPU) to execute public key algorithms efficiently. Smart cards have all of their functionality comprised on a single chip (in contrast to chip cards, which contain several chips wired to each other). 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*

1.2 Abbreviation

Acronym	Definition
CC	*Common Criteria*
CGA	*Certification generation application*
CNS	*Carta Nazionale dei Servizi*
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*
OS	*Operating System*
OSP	*Organizational security policy*
PIN	*Personal Identification Number*
PP	*Protection profile*
PUK	*PIN Unblocked Key*
QSCD	*Qualified Signature Creation Device*
RAD	*Reference authentication data*
RAM	*random access memory*
RNG	*random number generation*
ROM	*read only memory*
SAR	*Security Assurance Requirements*

SCA	*Signature creation application*
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*

1.3 Associated references

Ref.	Document title
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017. CCMB-2017-04-001.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-002.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004.
[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 with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014.
[PP-SSCD2]	Protection profiles for secure signature creation device — Part 2: Device with key Generation, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, Version 2.0.1, 30 June 2016, CC Version - 3.1 Revision 3.
[PP-SSCD3]	Protection profiles for secure signature creation device – Part3: Device with key import, CEN/TC 224, BSI-CC-PP-0075-2012-MA-01, Version 1.0.2, 30 June 2016, CC Version - 3.1 Revision 3.
[PP-SSCD4]	Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, CEN/TC 224, BSI-CC-PP-0071-2012-MA-01, Version 1.0.1, 30 June 2016, CC Version - 3.1 Revision 4.
[PP-SSCD5]	Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, CEN/TC 224, BSI-CC-PP-0072-2012-MA-01, Version 1.0.1, 30 June 2016, CC Version - 3.1 Revision 4.
[PP-SSCD6]	Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application, CEN/TC 224, BSI-CC-PP-0076-2013-MA-01, Version 1.0.4, 30 June 2016, CC Version - 3.1 Revision 4.
[PP-JAVACARD]	Java Card Protection Profile – Open Configuration, Version 3.0, May, 2012. Certified by ANSSI under the reference ANSSI-CC-PP-2010/03-M01
[ST-IC]	Public Security Target, BSI-DSZ-CC-0945-V2-2018, Version 0.7, 06.11.2017, "Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13", Infineon Technologies AG (sanitised public document)
[CR-IC]	Certification Report - BSI-DSZ-CC-0945-V2-2018
[ST-PL]	FQR 110 8959 Ed 3.0 - ID One Cosmo V9 Essential Public ST Final

Ref.	Document title
[RNG-NIST]	The NIST SP 800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revise) March 2007
[REG]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[DIR]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.
[GP]	GlobalPlatform Card Specification 2.2.1, GPC_SPE_034, GlobalPlatform Inc., January 2011.
[JCRE]	"Java Card - RE" Runtime Environment Specification, Classic Edition Version 3.0.5, June 2015, Oracle Technology Network.
[JCVM]	"Java Card - VM" Virtual Machine Specification, Classic Edition Version 3.0.5, June 2015, Oracle Technology Network.
[JCAPI]	"Java Card - API" Application Programming Interfaces, Classic Edition Version 3.0.5, June 2015, Oracle Technology Network.
[JIL-1]	JIL-Certification-of-Open-Smart-Card-Products-v1.1-(for_trial_use), Version 1.1, 4 February 2013
[JIL-2]	Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[AGD_PRE]	FQR 220 1342 Ed 4 – AGD_PRE
[AGD_OPE]	FQR 220 1343 Ed 4 – AGD_OPE
[USR_GUIDE]	FQR 220 1401 Ed 5 - ID-One CNS V2 Java Applet - User Guide
AGD_PRE [JOP]	ID-One COSMO V9 Essential Pre-Perso Guide FQR 110 8797 Ed5 – 22/10/2018
AGD_OPE [JOP]	ID-One COSMO V9 Essential Reference Guide FQR 110 8823 Ed5 – 22/10/2018
[CNS_SPEC]	Carta Nazionale dei Servizi Functional Specification V1.1.6, DigitPa, 2 April 2011
[KEY_MGT]	Key Management Procedure for R&D Centers. Ref: I CRD13 2 CRD 510 02
[SEC_REC]	Applet Security Recommendations FQR 110 8794 Ed 4
[ADV_ARC]	FQR 220 1338 Ed 2 – ADV_ARC
[PGD]	203381 00 PGD AA - ID-One CNS V2
[SEC_ACCPT]	FQR 110 8921 – 24/09/2018 – Secure acceptance and delivery of sensitive elements
[LOAD_GUIDE]	ID-One COSMO V9 Essential Application Loading Protection Guidance FQR 110 8798 Ed1
[CEN-14890]	CEN-EN 14890-2:2008 Application Interface for smart cards used as Secure Signature Creation Devices – Part 2 : Additional Services
[RFC-6278]	IETF RFC 6278 – Use of Static Static Elliptic Curve Diffie-Hellman Key Agreement in Cryptographic Message Syntax
[PLT_API]	FQR 110 8827 Ed1- 23/04/2018 - Java Card API on ID-One Cosmo V9 platform

2 Security Target Introduction

This document is the Security Target for the CNS V2 Applet on ID-One COSMO V9 Essential Platform of IDEMIA.

The Carta Nazionale dei Servizi - CNS Applet is a configurable applet designed primarily for authentication and signature generation and as an eHealth secure data storage.

The TOE addressed by the current ST is a QSCD device (combination of SSCD Parts 1 to 6) that may:

1) SSCD Part 2: that performs the generation of signature keys in the device **[PP-SSCD2]**,
2) SSCD Part 3: that performs the import of the signature keys generated in a trusted manner outside the device **[PP-SSCD3]**,
3) SSCD Part 4: that specifies an extension for an SSCD with key generation (SSCD Part 2) that support establishing a trusted channel with a certificate generation application (CGA) **[PP-SSCD4],**
4) SSCD Part 5: that specifies an extension for an SSCD with key generation (SSCD Part 2) that additionally supports establishing a trusted channel with a signature creation application (SCA)) **[PP-SSCD5]** and
5) SSCD Part 6: that specifies an extension for an SSCD with key import (SSCD Part 3) that additionally supports establishing a trusted channel with a signature creation application (SCA) **[PP-SSCD6].**

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.

This document provides a list of security requirements for the the CNS Applet embedded in ID-One COSMO V9 Essential 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 TOE Summary specification (TSS).

2.1 ST Reference

Title	ID-One CNS V2 Public Security Target
ST Identification	FQR 550 0012 Ed 1
ST Version	V1.3
CC Version	3.1 Revision 5
Assurance Level	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
ITSEF	Brightsight
Certification Body	TÜV Rheinland Nederland B.V.
Compliant To Potection Profile	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]**

2.2 TOE Reference

TOE Commercial Name	ID-One™ CNS V2
Applet Code Version	203381
Internal Applet Version	00000109
Guidance Documents	**[AGD_PRE], [AGD_OPE], [USR_GUIDE], [SEC_REC], AGD_PRE [JOP], AGD_OPE [JOP], [PLT_API], [LOAD_GUIDE] and [SEC_ACCPT]**
Platform Name	ID-One COSMO V9 Essential Platform
Platform Certificate	CC-18-200833
IC Identifier	CC Identifier: IFX_CCI_000005, IFX_CCI_000008 and IFX_CCI_000014
IC Certificate	BSI-DSZ-CC-0945-V2-2018

2.3 TOE Overview

2.3.1 TOE usage and major Security Features

CNS is a Java Card application that provides a Qualified Signature Creation Device [QSCD].

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 the intended, legitimate user should be informed of the signatory's verification authentication data (VAD) required for use of the TOE in signing. If the VAD is a password or a PIN, 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. 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 security features:

- 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 QSCD 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 QSCD,
  - 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.

Even though Netlink Authentication is supported, it is out of the scope of evaluation and only usable for files out of the QSCD configuration as it does not provide any of the keys needed for this type of authentication.

2.3.2 TOE Type

The TOE is the Smart Card Integrated Circuit with Embedded Software serving as an QSCD (Qualified Signature Creation Device) in accordance to its functional specification. The Smart Card chip module can be embedded in a plastic card providing a physical interface between the terminal and the chip.

The product embedding CNS **[CNS-SPEC]** is an integrated circuit chip embedding an Operating system:

- based on :
  - Java Card technology **[JCRE], [JCVM], [JCAPI]** and
  - Global Platform technology **[GP]**

- With main responsibilities as :
  - To provide interface between the Integrated Circuit and the CNS applet
  - To provide to CNS applet, basic services to access to memories and all needed cryptographic operation
  - To ensure global management of the card (loading, installation and deletion of applets) and monitor the security of the card (data integrity and physical attacks counter-measures).

Since the TOE claims compliancy to CEN-EN 419 211-2 till CEN-EN 419 211-6 (Signature Protection Profiles **[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]** and **[PP-SSCD6]**), the TOE can be used as (depending on its configuration during personalization):

- Config#1 claiming compliancy to CEN/EN 419 211-2/3/4/5/6 (**[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]** and **[PP-SSCD6]**).
- Config#2 claiming compliancy to CEN/EN 419 211-2/3/4 (**[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**). This configuration does not support the trusted channel between the TOE and the SCA.
- Config#3 claiming compliancy to CEN/EN 419 211-2/3 (**[PP-SSCD2]**, **[PP-SSCD3]**). This configuration does not support the trusted channel between: (i) the TOE and the SCA; (ii) the TOE and the CGA.

The Applet is linked to a card reader/writer (card terminal) via the HW and physical interfaces of the smart card. The smart card has contact type and contactless type interfaces.

The TOE is designed and produced in a secure environment.

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

2.3.2.1 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 QSCD-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.

As shown in Figure 1 through Figure 5, the signing environment, the management environment and the preparation environment are secure and protect data exchanged with the TOE. The protection of data exchanged with the TOE is realized by a trusted communication.

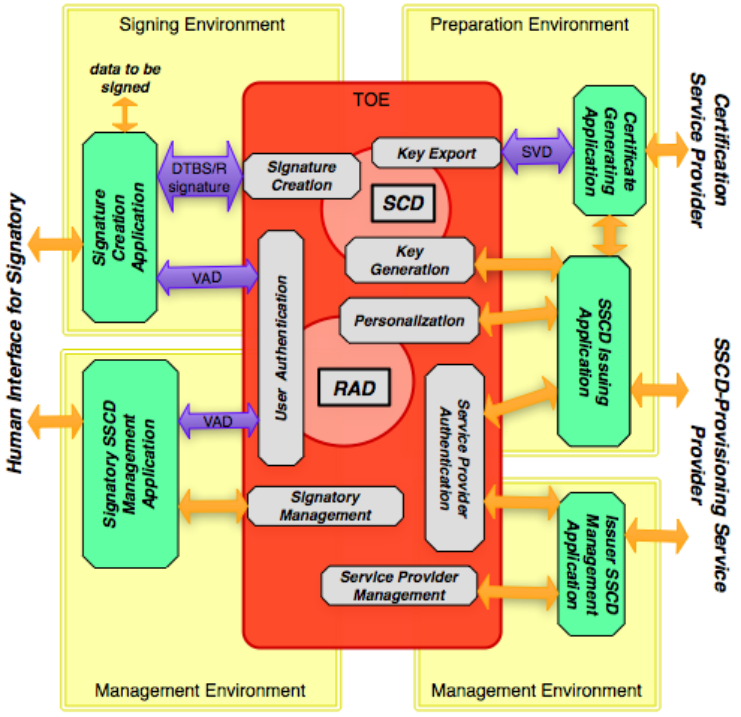

Figure 1: TOE and Operational environments with Key Generation

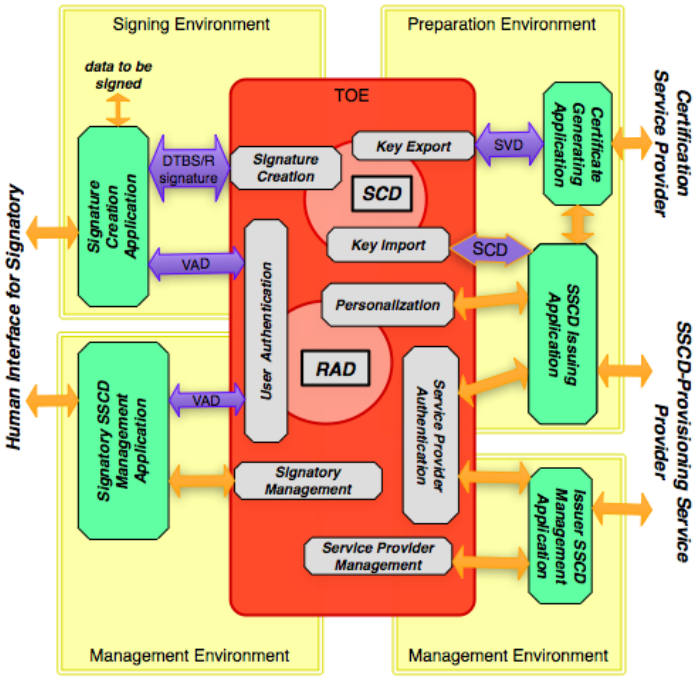

Figure 2: TOE and Operational environments with Key Import

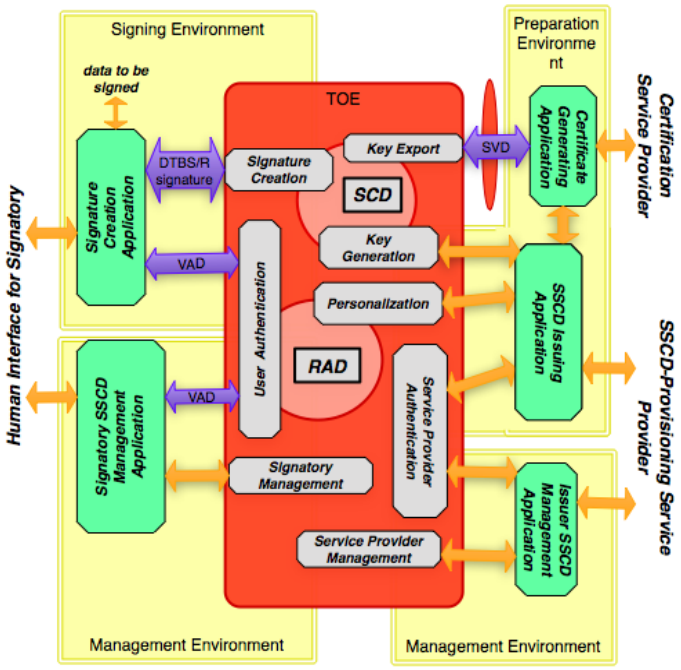

Figure 3: TOE and Operational environments with Key Generation and trusted channel to CGA

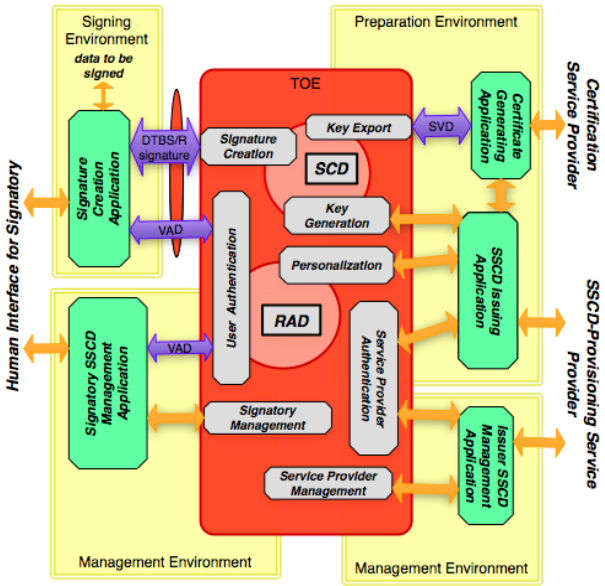

Figure 4: TOE and Operational environments with Key Generation and trusted channel to SCA

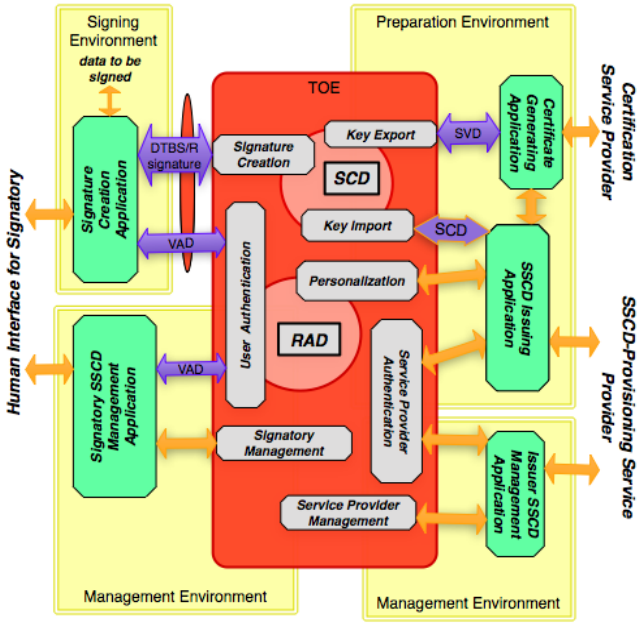

Figure 5: TOE and Operational environments with Key Import and trusted channel to SCA

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 QSCD. 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 Regulation [REG]. 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 or a PIN. 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 QSCD-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 QSCD 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 QSCD, 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.

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.

2.3.3 Required non-TOE hardware/software/firmware

The TOE is the CNS V2 Applet that is loaded on to a smart card. It is an independent product and does not need any additional hardware/software/firmware to ensure its security.
In order to be powered up and to be able to communicate, the TOE needs a card reader.

The TOE is capable of making use of an optional Server Applet. The server applet is only installed and used if the personalizing agent wants to use the File System Profile Information during the installation of the Applet. Information would include the File and Object IDs and Attributes to be created upon Applet installation. This information is encoded in the server applet.

This server applet is immediately deleted after installation of the CNS V2 Applet.
More details about this Server Applet are available in **[AGD_PRE]**.

2.4 TOE Description

The CNS application stores:

- the cardholder personal information
- the cardholder health information
- the cardholder authentication credentials (keypair and x509 certificate)
- the cardholder electronic signature credentials (keypair and x509 certificate)
- cardholder security codes (authentication and signature PIN PUK)
- issuer keys to allow post issuance configuration of free memory space

2.4.1 Physical Scope

The TOE is made of the following part:

- The IC reference is as below:

CC ID
IFX_CCI_000005 IFX_CCI_000008 IFX_CCI_000014

(For form factor of the IC, refer to the [ST-PL], Table 4.)

- The Platform is ID-One COSMO V9 Essential
- The CNS V2 Applet

The following guidance documents will be provided for the TOE:

Description	Audience	Form Factor of Delivery
[AGD_PRE]	Personalising Agent	Electronic Version
[USR_GUIDE]	Personalising Agent	
[AGD_OPE]	End user of the TOE	
AGD_PRE [JOP]	Prepersonalisation	
[PLT_API]	Application Developer	
AGD_OPE [JOP]	Application Developer	
[LOAD_GUIDE]	Issuer of the platform that aims to load applications	
[SEC_REC]	Developer of Sensitive Applications	
[SEC_ACCPT]	Chip Manufacturer Third party Production sites	

This ST Lite version of this Security Target also serves as a guidance document along with above mentioned documents.

All the above mentioned guidance documents will be delivered via mail in a .pgp encypted format.

Form factor and Delivery Preparation:

1. As per the Software Development Process of IDEMIA, upon completion of development activities, particular applet will be uploaded into CPS in CAP file format. Before uploading, the applet will be verified through Oracle verifier and IDEMIA verifier.
2. During Release for Sample as project milestone, status of the applet in CPS will be changed into "Pilot version" to be used further for manufacturing samples.
3. During Software Delivery Review as the final R&D project milestone, status of the applet in CPS will be changed into "Industrial release" to be used further for mass production.

Refer Life Cycle chapter of this ST for more details regarding TOE delivery as per different options.

2.4.2 Logical Scope

CNS V2 is based on Java Card Open Platform.

The CNS V2 applet fulfils the recommendations indicated in the guidance documentation of the Java Card Open Platform (**AGD_PRE [JOP], AGD_OPE [JOP] and [SEC_REC]**).
The logical scope of the TOE may be depicted as follows:

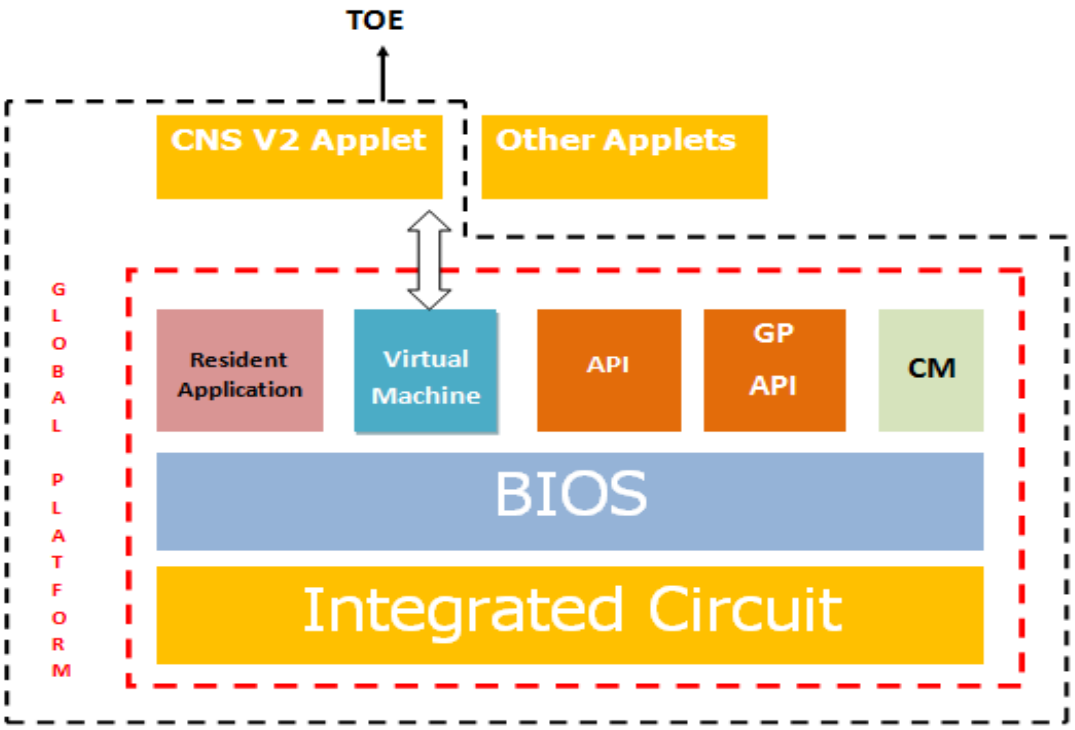

Figure 6 Logical Scope

2.4.2.1 TOE Scope

The TOE is made up of:

- The underlying Java Card Open Platform
- The CNS Applet
- The associated guidance documentation in **[AGD_PRE]**, **[AGD_OPE]** and **[USR_GUIDE]**
- The (pre)personalization agent key sets

Morover, as the platform is certified as a Java Card open platform and complies with the requirements of **[JIL-1]**, the TOE may contain any other applets that comply with **[JIL-1]** and the specific requirements of the TOE stated in the guidance documents. The TOE scope is shown in Figure 6. Once constructed, the TOE is a bare microchip with its external interfaces for communication. The physical medium on which the microchip is mounted does not alter or modify any security functions of the TOE.

3 Life cycle

With respect to the smartcard life-cycle, divided in 7 phases and according to the IC protection profile **[PP -IC]**, the TOE life cycle is divided in seven different phases.

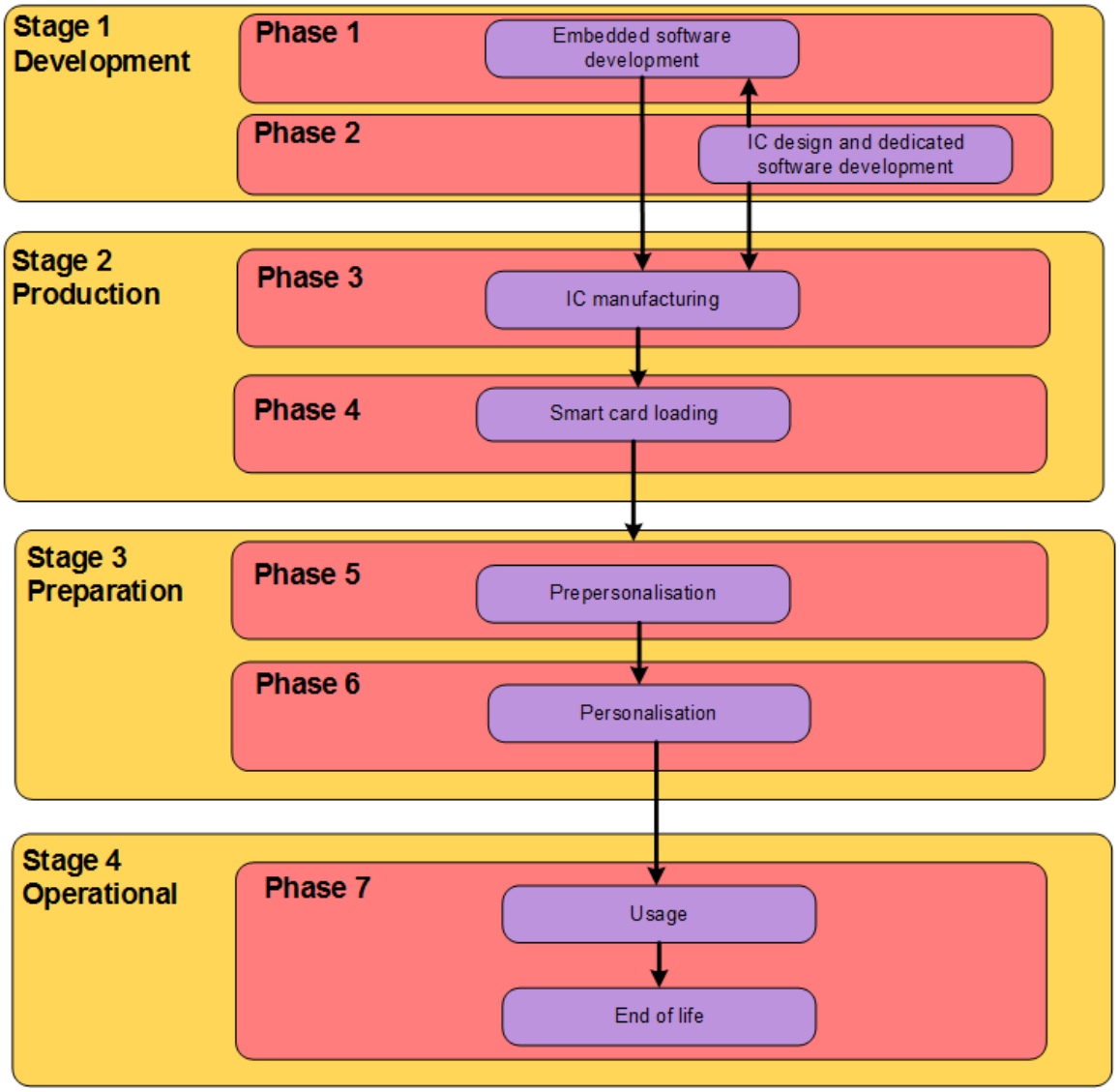

Figure 7 Life cycle Overview

The TOE is an applet embedded on a Java Card Open Platform. The underlying platform is conformant to the **[PP-IC]** smartcard life cycle, and the TOE is also conformant to the **[PP-IC]** smartcard lifecycle.

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

The development environment encompasses the environment in which the TOE is developed and tested:

- Java Card Open Platform components

- CNS V2 Applet

This Environment is composed of three phases:

Phase 1: Embedded Software Development
Phase 2: IC design and dedicated software development

3.1.1.1 Phase 1: **Embedded Software Development**

The IC Embedded Software Developer is in charge of:

- Specification, development and validation of the software (Java Card Operating System and CNS V2 Applet).

CNS V2 Applet and Java Card Open Platform (JOP) development environment is enforced by IDEMIA and its confidentiality and integrity are covered by the evaluation of the development premises of IDEMIA.

To ensure security, access to development tools and products elements (PC, card reader, documentation, source code...) is protected. The protection is based on measures for prevention and detection of unauthorized access.

Role	Actor	Covered by
Embedded Software Developer (CNS V2 Applet)	IDEMIA	**ALC**
Embedded Software Developer (Java Card Open Platform)	IDEMIA	**ALC**
Redaction and Review of Documentation	IDEMIA	**ALC**

At the end of phase 1, the Java Card platform code and CNS V2 Applet code are protected in integrity and confidentiality by the environment

3.1.1.2 Phase 2: **IC design and dedicated software development**

In this phase, the underlying integrated circuit is developed. This phase takes place at the manufacturing site of the IC provider.

The confidentiality and integrity of the Java Card packages and Java Card open platform is covered by the evaluation of the development premises of the IC manufacturer.

Roles, Actors, Sites and coverage for this phase of the product life-cycle are listed in the table below:

Role	Actor	Covered by
IC Developer	Infineon	**ALC [Infineon]**

3.1.2 Production Environment (Phases 3 & 4 of the IC life cycle)

In this environment, the following two phases take place:

- **Phase 3:** IC manufacturing
- **Phase 4:** Smart card loading

The IC manufacturer is responsible for producing the IC (manufacturing, testing, and initialisation). Depending on the intention:

- **(Option 1)** the developer sends the image (containing both the Java Card platform and the CNS applet) to be flashed in the IC to the IC manufacturer in the phase 3.

Or

- **(Option 2)** the platform developer sends the image (containing only the Java Card platform) to be flashed in the IC to the IC manufacturer in the phase 3. Once the Java Card platform has been loaded, the package of CNS is securely delivered from the applet developer to the smart card loader. The cap file of the applet is then loaded (using GP mechanism) in the Java Card platform by the smart card loader in phase 4 at IDEMIA audited site.

Or

- **(Option 3)** the developer sends the image (containing both the Java Card platform and the CNS applet) to be loaded in Flash (using the loader of the IC) to the smart card loader in phase 4.

Several life cycles are available, depending when the Flash Code is loaded. The following tables present roles, actors, sites and coverage for this for this environment of the product life-cycleand describe for each of them the TOE delivery point.

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	Image containing both platform and applet	Infineon	Infineon production plants Refer to Platform	ALC
Smart card loader	-	-	-	-
TOE Delivery Point				

Table 1 Image containing both platform and applet is loaded at IC manufacturer (Option 1)

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	Image containing only platform	Infineon	Infineon production plants Refer to Platform	ALC
Smart card loader	Cap file of the applet	IDEMIA	IDEMIA plant	ALC
TOE Delivery Point				

Table 2 Cap file of CNS applet is loaded through the loader of the IC manufacturer (Option 2)

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer send the components containing appropriate key for loading encrypted image	-	-	-	-
TOE Delivery Point				
Smart card loader	Image containing both platform and applet	IDEMIA or another agent	IDEMIA plants or others sites	AGD

Table 3 Image containing both platform and applet is loaded through the loader of the IC (Option 3)

3.1.3 Preparation Environment

In this environment, the following two phases take place:

- **Phase 5:** Prepersonalisation
- **Phase 6:** Personalisation

The preparation environment may not necessarily take place in a manufacturing site, but may be performed anywhere. All along these two phases, the TOE is self-protected as it requires the authentication of the prepersonalisation agent or personalisation agent prior to any operation.

The CNS applet is is prepersonalised and personalized according to **[AGD_PRE]**.

At the end of phase 6, the TOE is constructed. These two phases are covered by **[AGD_PRE]** tasks of the TOE and **AGD_OPE [JOP]** tasks of Platform.

3.1.4 Operational Environment

The TOE is under the control of the User (Signatory and/or Administrator).

This phase is covered by **[AGD_OPE]** of the TOE and **AGD_OPE [JOP]** of the underlying Platform.

4 Conformance Claims

4.1 CC Conformance

This Security Target claims conformance to [CC2], [CC3] and [CEM].

The conformance to the Common Criteria is claimed as follows:

CC	Conformance rationale
Part 2	Conformance to the extended part. ▪ FCS.RNG.1: "Quality metric for random numbers" ▪ FPT_EMS.1: "TOE Emanation" ▪ FIA_API.1: "Authentication proof of identity"
Part 3	Conformance to EAL 4, augmented with ▪ AVA_VAN.5: "Advanced methodical vulnerability analysis" ▪ ALC_DVS.2: "Sufficiency of security measures"

4.2 PP Claims

This security target claims strict conformance to 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]**.

The underlying integrated circuit is successfully evaluated and certified in accordance with the Security IC Platform Protection Profile **[PP -IC]**.

The underlying Java Card Open Platform of the TOE is evaluated and certified in accordance with the Java Card™ System Protection Profile Open Configuration **[PP-JAVACARD].**

4.3 Conformance Rationale

[PP-SSCD4] and **[PP-SSCD5]** are strictly conforming to the core **[PP-SSCD2]**. **[PP-SSCD6]** is strictly conforming to the core **[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.HID_VAD, OE.DTBS_Protect and OE.SSCD_Prov_Service. This ST adapts OE.HID_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-SSCD4]**.
   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) The security assurance requirements (SARs) are originally taken from SARs of **[CC3]** according to the package conformance EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5.

The document **[COMP]** shall be used in addition to the **[CC3]** and to the **[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	x	×	x	×
A.SCA	×	x	x	×	X	×
A.CSP		x			x	x
Threats						
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 4 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						
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						
OE.SVD_Auth	×	×	×	×	×	×
OE.CGA_QCert	×	×	×	×	×	×
OE.SSCD_Prov_Service	×	×		×	×	x
OE.SCD/SVD_Auth_Gen		×			×	×
OE.SCD_Unique		×			×	×
OE.SCD_SVD_Corresp		×			×	×
OE.SCD_Secrecy		x			x	×
OE.HID_VAD	×	×	×			x
OE.DTBS_Intend	×	×	×	×	x	×
OE.DTBS_Protect	×	×	×			x
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 5 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	×	×	×	×	×	×

TOE SFRs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
FMT_MSA.1/Signatory	×	×	×	×	×	×
FMT_MSA.2	×	×	×	×	×	×
FMT_MSA.3	×	×	×	×	×	×
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_RNG.1						×

Table 6 PP SFRs vs. ST

5 Security Problem Definition

5.1 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.

5.2 Users / Subjects

5.2.1 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.

5.2.2 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.

5.3 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.

5.4 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 [DIR]) 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 [DIR]), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the directive Annex I [DIR]). 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 [DIR]. 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.

5.5 Assumptions

5.5.1 All SSCD parts

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.

5.5.2 Parts 3 and 6 only

A.CSP

Secure SCD/SVD management by CSP

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

6 Security Objectives

6.1 Security Objectives for the TOE

6.1.1 All SSCD parts

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.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_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.Tamper_Resistance

Tamper resistance

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

6.1.2 SSCD parts 2, 4 and 5 only

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.

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.

6.1.3 SSCD parts 3 and 6 only

OT.SCD_Auth_Imp

Authorized SCD import

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

Application Note:

Authorized SCD import

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

6.1.4 SSCD part 4 only

OT.TOE_SSCD_Auth

Authentication proof as SSCD

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

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.

6.1.5 SSCD parts 5 and 6 only

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 core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.HID_VAD in the core PP 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. Therefore this ST re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

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/R received from the SCA. The TOE must not generate electronic signatures with the SCD for altered DTBS.

6.2 Security Objectives for the Operational Environment

6.2.1 All SSCD parts

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.

6.2.2 SSCD parts 2, 3 and 4 only

OE.HID_VAD

Protection of the VAD

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

OE.DTBS_Protect

SCA protects the data intended to be signed

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

6.2.3 SSCD parts 2, 3, 5 and 6 only

OE.SSCD_Prov_Service

Authentic SSCD provided by SSCD-provisioning service

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

6.2.4 SSCD parts 3 and 6 only

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 of the 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 in the operational 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 sent to the CGA and the SCD exported to the TOE of the signatory identified in the SVD certificate.

6.2.5 SSCD part 4 only

OE.Dev_Prov_Service

Authentic SSCD provided by SSCD Provisioning Service

The SSCD Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, 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.

Application 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_TC_SVD_Imp

CGA trusted channel for SVD import

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

OE.CGA_SSCD_Auth

Pre-initialisation 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.

6.2.6 SSCD parts 5 and 6 only

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 core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.HID_VAD in the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI) 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. Therefore this ST re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

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/R cannot be altered undetected in transit between the SCA and the TOE.

Application Note:

This security objective for the TOE is partly covering OE.DTBS_Protect from the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.DTBS_Protect in the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI) 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. Therefore this ST re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

6.3 Security Objectives Rationale

6.3.1 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 the directive [DIR], recital (18). This threat is countered by

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

Furthermore, generation and/or import of SCD known by an attacker is countered by OE.SCD/SVD_Auth_Gen, which ensures that only 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 counters this threat by implementing cryptographically secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographically secure electronic signatures. OE.SCD_Unique counters this threat by implementing cryptographically secure generation of the SCD/SVD pair.

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

OE.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD.

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. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure

destruction of the SCD, which may be initiated by the signatory. OT.Sigy_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE.

OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, OE.HID_VAD (Protection of the VAD) provides confidentiality and integrity of the VAD as needed by the authentication method employed. OE.Signatory ensures that the signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD. OE.Signatory ensures also that the signatory keeps their VAD confidential.

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 from the SCA to 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).

T.DTBS_Forgery addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of OE.DTBS_Protect, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R inside the TOE.

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.

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 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.

OE.SCD_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance.

6.3.2 Organisational Security Policies

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

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- OT.SCD_SVD_Corresp, which requires to ensure the correspondence between the SVD and the SCD during their generation,
- OE.SCD/SVD_Auth_Gen, which ensures that the SCD/SVD generation can be invoked by authorized users only,
- OT.SCD_Auth_Imp which ensures that authorised users only may invoke the import of the SCD,
- OE.SCD_SVD_Corresp, which requires the CSP to ensure the correspondence between the SVD and the SCD during their generation, and
- OE.CGA_QCert for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

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.

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 [DIR]. This is ensured as follows: < Parts 36 >

- OE.SCD_Unique meets the paragraph 1(a) of the directive [DIR], Annex III, by the requirements that the SCD used for signature creation can practically occur only once; < /Parts 36 > < Parts 245 >
- OT.SCD_Unique meets the paragraph 1(a) of Annex III [DIR], by the requirements that the SCD used for signature creation can practically occur only once; < /Parts 245 >
- < Parts 245 > OT.SCD_Unique, < /Parts 245 > OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(a) of Annex III [DIR] by the requirements to ensure secrecy of the SCD.
- OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of the SCD against specific attacks; < Parts 36 >

- OT.SCD_Auth_Imp, which limits SCD import to authorised users only;
- OE.SCD_Secrecy, which ensures the confidentiality of the SCD during generation and export to the TOE, and deletes the SCD after export to the TOE. The CSP does not use the SCD for signature creation; < /Parts 36 >
- OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III [DIR] by the requiements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE;

— OT.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only, and

- OT.Sigy_SigF meets the requirement in paragraph 1(c) of Annex III [DIR] 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 [DIR] as the TOE must not alter the DTBS/R.

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

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

- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialisation, personalisation and operational usage, < Parts 36 >
- OE.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only, < /Parts 36 > < Parts 245 >
- OT.Sigy_SigF, which requires the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.

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

< Part 4 > 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. < /Part 4 >

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, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures created with the TOE. OE.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, initialised and personalised as SSCD from the SSCD-provisioning service.

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

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

OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory ensures that the signatory keeps their VAD confidential. OE.DTBS_Intend, OE.DTBS_Protect and OT.DTBS_Integrity_TOE ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

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.

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 (SCA sends data intended to be signed), OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE), OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) and OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS.

6.3.3 Assumptions

6.3.3.1 All SSCD parts

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.

6.3.3.2 Parts 3 and 6 only

A.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 of the signature creation data), that SCD and SVD correspond to each other is addressed by OE.SCD_SVD_Corresp (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are deleted in the environment once exported to the TOE is addressed by OE.SCD_Secrecy (SCD Secrecy).

6.3.4 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, OE.SCD_SVD_Corresp, OT.TOE_TC_SVD_Exp, OE.CGA_TC_SVD_Imp	Section 6.3.1
T.SigF_Misuse	OT.Lifecycle_Security, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OE.Signatory, OE.DTBS_Intend, OT.TOE_TC_VAD_Imp, OT.TOE_TC_DTBS_Imp, OE.HID_TC_VAD_Exp, OE.SCA_TC_DTBS_Exp, OE.HID_VAD, OE.DTBS_Protect	Section 6.3.1
T.DTBS_Forgery	OT.DTBS_Integrity_TOE, OE.DTBS_Intend, OT.TOE_TC_DTBS_Imp, OE.SCA_TC_DTBS_Exp,	Section 6.3.1

	OE.DTBS_Protect	
T.Sig_Forgery	OT.SCD_Unique, OT.Sig_Secure, OE.CGA_QCert, OE.SCD_Unique	Section 6.3.1

Table 7 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.EMSEC_Design	T.Hack_Phys
OT.Tamper_ID	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_VAD_Imp	T.SigF_Misuse
OT.TOE_TC_DTBS_Imp	T.SigF_Misuse, T.DTBS_Forgery
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.HID_VAD	T.SigF_Misuse
OE.DTBS_Protect	T.SigF_Misuse, T.DTBS_Forgery
OE.SSCD_Prov_Service	
OE.SCD/SVD_Auth_Gen	T.SCD_Divulg
OE.SCD_Secrecy	T.SCD_Divulg
OE.SCD_Unique	T.SCD_Derive, T.Sig_Forgery
OE.SCD_SVD_Corresp	T.SVD_Forgery
OE.Dev_Prov_Service	
OE.CGA_TC_SVD_Imp	T.SVD_Forgery

OE.CGA_SSCD_Auth	
OE.HID_TC_VAD_Exp	T.SigF_Misuse
OE.SCA_TC_DTBS_Exp	T.SigF_Misuse, T.DTBS_Forgery

Table 8 Security Objectives and Threats - Coverage

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

Table 9 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.EMSEC_Design	P.Sigy_SSCD, P.Sig_Non-Repud
OT.Tamper_ID	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_VAD_Imp	P.Sig_Non-Repud
OT.TOE_TC_DTBS_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.HID_VAD	
OE.DTBS_Protect	P.Sig_Non-Repud
OE.SSCD_Prov_Service	P.Sigy_SSCD, P.Sig_Non-Repud
OE.SCD/SVD_Auth_Gen	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud
OE.SCD_Secrecy	P.Sigy_SSCD, P.Sig_Non-Repud
OE.SCD_Unique	P.Sigy_SSCD, P.Sig_Non-Repud
OE.SCD_SVD_Corresp	P.CSP_QCert, P.Sig_Non-Repud
OE.Dev_Prov_Service	P.Sigy_SSCD, P.Sig_Non-Repud
OE.CGA_TC_SVD_Imp	P.Sigy_SSCD, P.Sig_Non-Repud
OE.CGA_SSCD_Auth	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud
OE.HID_TC_VAD_Exp	P.Sig_Non-Repud
OE.SCA_TC_DTBS_Exp	P.Sig_Non-Repud

Table 10 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 11 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.HID_VAD	
OE.DTBS_Protect	
OE.SSCD_Prov_Service	
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_TC_SVD_Imp	
OE.CGA_SSCD_Auth	
OE.HID_TC_VAD_Exp	
OE.SCA_TC_DTBS_Exp	

Table 12 Security Objectives for the Operational Environment and Assumptions - Coverage

7 Extended Requirements

7.1 Extended Families

7.1.1 Extended Family FIA_API - Authentication Proof of Identity

7.1.1.1 Description

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.

Application note 10: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter 'Explicitly stated IT security requirements (APE_SRE)') from a TOE point of view.

7.1.1.2 Extended Components

Extended Component FIA_API.1

Description

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

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.

7.1.2 Extended Family FPT_EMS - TOE Emanation

7.1.2.1 Description

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.

7.1.2.2 Extended Components

Extended Component FPT_EMS.1

Description

This family defines requirements to mitigate intelligible emanations.

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.

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.

7.1.3 Extended Family FCS_RNG - Generation of random numbers

7.1.3.1 Description

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

7.1.3.2 Extended Components

Extended Component FCS_RNG.1

Description

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

Definition

FCS_RNG.1 Quality metric for random numbers

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic hybrid, deterministic] random number generator that implements [assignment: list of security capabilities].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: a defined quality metric].

Dependencies: No dependencies.

8 Security Requirements

8.1 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.

In some of the functional requirements below, the **[Editorially Refined]** tag has been used to signify a small change in the requirement, to adhere to proper English grammar, or to make it more understandable to the reader.

8.1.1 All SSCD parts

8.1.1.1 Protection of the TSF (FPT)

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **side channel emissions** in excess of **limits specified by the state-of-the-art attacks on smart card IC** 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 circuit 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**

- **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**
- **No other failure**.

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 **physical manipulation and physical probing** to the **TSF** by responding automatically such that the SFRs are always enforced.

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 **TSF**.

8.1.1.2 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,**
- **No other security management function**.

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 and SCD Import SFP** to restrict the ability to **modify** the security attributes **SCD/SVD management** to **R.Admin**.

FMT_MSA.1/Signatory Management of security attributes

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, SCD Import SFP and Signature Creation SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 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:

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

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**.

8.1.1.3 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,**
- **establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD,**
- **establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD,**
- **establishing a trusted channel between the CSP and the TOE by means of TSF required by FTP_ITC.1/SCD**

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_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer within 1 and 15** 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**.

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 the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD,**
- **establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD,**
- **establishing a trusted channel between the CSP and the TOE by means of TSF required by FTP_ITC.1/SCD**

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.

8.1.1.4 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_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**.

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**.

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

- **SCD**
- **SVD (if persistently stored by the TOE)**

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

FDP_ACC.1/Signature_Creation Subset access control

FDP_ACC.1.1/Signature_Creation The TSF shall enforce the **Signature Creation SFP** on

- **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"**.

8.1.1.5 Cryptographic support (FCS)

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **refer to the table below** in accordance with a specified cryptographic algorithm **refer to the table below** and cryptographic key sizes **refer to the table below** that meet the following: **refer to the table below:**

Cryptographic Operation / Protocol	Algorithm	Cryptographic Algorithms and Standards
Signature Computation with Off-Card Hashing	RSA and ECDSA	RSA-1024, 1536, 1792, and 2048 with PKCS#1 v1.5 RSA-1024, 1536, 1792, and 2048 with PKCS#1-PSS and SHA-1, 224, 256, 384 and 512 (FIPS PUB 180-3) EC-192, 224, 256, 320, 384, 512 and 521 following ANSI X9.62-1998
Encryption/Decryption	TDES, AES, and RSA	3DES CBC 2Key and 3DES CBC 3Key following FIPS PUB 46-3, ANSI X3.92, FIPS PUB 81, with ISO/IEC 9797 Mode 2 AES-128, AES-192, AES-256 following FIPS PUB 197 SP800-38B with ISO/IEC 9797 Mode 2 RSA-1024, 1536, 1792, and 2048 with No Padding following ANSI X9.31, ISO/IEC 9796-1, annex A, section A.4 and A.5, and annex C, PKCS#1 RSA-1024, 1536, 1792, and 2048 with PKCS#1-OAEP, using SHA-

		256 (FIPS 198)
Encryption Key Decipherment	**ECDH**	**EC-192, 224, 256, 320, 384, 512 and 521 following [CEN-14890] that uses RFC-6278 for ECDH**
Client/Server Authentication	**TDES, AES, and RSA**	**3DES MAC3 2Key and 3DES MAC3 3Key following FIPS PUB 46-3, ANSI X3.92, FIPS PUB 81 with ISO/IEC 9797 Mode 1 AES-128, AES-192, AES-256 CMAC following FIPS PUB 197 SP800-38B RSA-1024, 1536, 1792, and 2048 with PKCS#1 v1.5**
Generation of Key Pair Integrity Token	**ECDSA**	**EC-256 following ANSI X9.62-1998**

.

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 **see table below** that meets the following: **See table below**

Cryptographic Algorithm	**Key DestructionMethod**	**Standard**
DES, AES and RSA Keys	**Keys are deleted with platform's clearKey method**	**Java Card API Specification [JCAPI]**
ES Keys	**The private S component of the key is overwritten with random values**	**None**

.

8.1.2 SSCD parts 2, 4 and 5 only

8.1.2.1 Cryptographic support (FCS)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys 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:

key generation	**Use**	**key sizes**	**list of**

algorithm			**standards**
EC key pair generation	**SCD/SVD Generation**	**192,224,256, 320,384, 512 and 521 bits**	**ANS X9.62**
RSA CRT Key pair generation	**SCD/SVD Generation**	**1024, 1536, 1792, 2048 bits**	**RSA PKCS#1 v2.1**

.

8.1.2.2 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/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:

Note that here S.User can be either R.Sigy or R.Admin depending on the personalization done.

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 or 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**.

Application Note:

In FDP_ACF.1.1/SVD_Transfer S.User can either be R.Sigy or R.Admin

In FDP_ACF.1.2/SVD_Transfer The role R.Sigy or R.Admin that can export SVD depends on the personalisation done.

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**.

Application Note:

Note that here S.User can be either R.Sigy or R.Admin depending on the personalization done.

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.

Application Note:

Note that here S.User can be either R.Sigy or R.Admin depending on the personalization done.

8.1.3 SSCD parts 3 and 6 only

8.1.3.1 Trusted path/channels (FTP)

8.1.3.2 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_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_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: **The SCD shall be sent by an authorized trusted IT environment**.

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 user S.User is associated with the security attribute "SCD/SVD Management"**.

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

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**
- **Assignment: None**.

8.1.4 SSCD part 4 only

8.1.4.1 Trusted path/channels (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 The TSF shall permit **another trusted IT product** 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

- **data Authentication with Identity of Guarantor according to FIA_API.1 and FDP_DAU.2/SVD**
- **Assignment: None**.

8.1.4.2 User data protection (FDP)

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.

8.1.4.3 Identification and authentication (FIA)

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a **Mutual Authentication using Symmetric or Asymmetric Key Cryptograph** to prove the identity of the **SSCD**.

8.1.5 SSCD parts 5 and 6 only

8.1.5.1 User data protection (FDP)

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.

8.1.5.2 Trusted path/channels (FTP)

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 **the remote trusted IT product** 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

- **signature creation**
- **Assignment: 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**
- **Assignment: None**

8.1.6 Additional SFR

FCS_RNG.1 Quality metric for random numbers

FCS_RNG.1.1 The TSF shall provide a **deterministic** random number generator that implements **CTR_DRBG as defined in [RNG-NIST]**.

FCS_RNG.1.2 The TSF shall provide random numbers that meet **the average Shannon entropy per internal random bit exceeds 0.999**.

8.2 Security Assurance Requirements

The security assurance requirement level is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

8.2.1 ADV Development

8.2.1.1 ADV_ARC Security Architecture

ADV_ARC.1 Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.1.2 ADV_FSP Functional specification

ADV_FSP.4 Complete functional specification

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

8.2.1.3 ADV_IMP Implementation representation

ADV_IMP.1 Implementation representation of the TSF

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

8.2.1.4 ADV_TDS TOE design

ADV_TDS.3 Basic modular design

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

ADV_TDS.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

8.2.1.5 ADV_INT TSF internals

8.2.2 AGD Guidance documents

8.2.2.1 AGD_OPE Operational user guidance

AGD_OPE.1 Operational user guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.2.2 AGD_PRE Preparative procedures

AGD_PRE.1 Preparative procedures

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

8.2.3 ALC Life-cycle support

8.2.3.1 ALC_CMC CM capabilities

ALC_CMC.4 Production support, acceptance procedures and automation

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.3.2 ALC_CMS CM scope

ALC_CMS.4 Problem tracking CM coverage

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.3.3 ALC_DEL Delivery

ALC_DEL.1 Delivery procedures

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.3.4 ALC_DVS Development security

ALC_DVS.2 Sufficiency of security measures

ALC_DVS.2.1D The developer shall produce and provide development security documentation.

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_DVS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

8.2.3.5 ALC_LCD Life-cycle definition

ALC_LCD.1 Developer defined life-cycle model

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.3.6 ALC_TAT Tools and techniques

ALC_TAT.1 Well-defined development tools

ALC_TAT.1.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.4 ASE Security Target evaluation

8.2.4.1 ASE_CCL Conformance claims

ASE_CCL.1 Conformance claims

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.4.2 ASE_ECD Extended components definition

ASE_ECD.1 Extended components definition

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

8.2.4.3 ASE_INT ST introduction

ASE_INT.1 ST introduction

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

8.2.4.4 ASE_OBJ Security objectives

ASE_OBJ.2 Security objectives

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.4.5 ASE_REQ Security requirements

ASE_REQ.2 Derived security requirements

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.4.6 ASE_SPD Security problem definition

ASE_SPD.1 Security problem definition

ASE_APD.1.1D The developer shall provide a security problem definition.

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.4.7 ASE_TSS TOE summary specification

ASE_TSS.1 TOE summary specification

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

8.2.5 ATE Tests

8.2.5.1 ATE_COV Coverage

ATE_COV.2 Analysis of coverage

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.5.2 ATE_DPT Depth

ATE_DPT.1 Testing: basic design

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.5.3 ATE_FUN Functional tests

ATE_FUN.1 Functional testing

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.5.4 ATE_IND Independent testing

ATE_IND.2 Independent testing - sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

8.2.6 AVA Vulnerability assessment

8.2.6.1 AVA_VAN Vulnerability analysis

AVA_VAN.5 Advanced methodical vulnerability analysis

AVA_VAN.5.1D The developer shall provide the TOE for testing.

AVA_VAN.5.1C The TOE shall be suitable for testing.

AVA_VAN.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.5.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.5.3E The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.5.4E The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

8.3 Security Requirements Rationale

8.3.1 Objectives

8.3.1.1 Security Objectives for the TOE

All SSCD parts

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/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. 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.

OT.SCD_Secrecy is provided by the security functions specified by the following SFR. FCS_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_RIP.1 and

FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA). FDP_UCT.1/SCD and FTP_ITC.1/SCD ensures the confidentiality for SCD import.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 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 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 ensures that the DTBS/R is not altered by the TOE. The integrity functions specified by FDP_SDI.2/DTBS require that the DTBS/R has not been altered by the TOE.

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

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

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

SSCD parts 2, 4 and 5 only

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 FCS_RNG.1 provides random number for Authentication. 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 implements the requirement of practically unique SCD as laid down in Annex III [DIR], paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1 and FCS_RNG.1.

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.

SSCD parts 3 and 6 only

OT.SCD_Auth_Imp 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.

SSCD part 4 only

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 (additionally to the core PP Part2 SSCD KG) establishment of the trusted channel before (human) user is authenticated.

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

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

SSCD parts 5 and 6 only

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.

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.

8.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.Lifecycle_Security	FCS_CKM.1, FCS_CKM.4, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/Signature_Creation, FDP_ACC.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, FCS_COP.1, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FDP_ITC.1/SCD, FDP_UCT.1/SCD, FTP_ITC.1/SCD	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, FPT_TST.1, FCS_COP.1	Section 8.3.1
OT.Sigy_SigF	FDP_ACF.1/Signature_Creation, FDP_ACC.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.EMSEC_Design	FPT_EMS.1	Section 8.3.1
OT.Tamper_ID	FPT_PHP.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, FCS_RNG.1	Section 8.3.1
OT.SCD_Unique	FCS_CKM.1, FCS_RNG.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	FIA_UID.1, FIA_UAU.1, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import	Section 8.3.1
OT.TOE_SSCD_Auth	FIA_UAU.1, FIA_API.1	Section 8.3.1
OT.TOE_TC_SVD_Exp	FDP_ACF.1/SVD_Transfer, FDP_ACC.1/SVD_Transfer, FDP_DAU.2/SVD, FTP_ITC.1/SVD	Section 8.3.1
OT.TOE_TC_VAD_Imp	FTP_ITC.1/VAD	Section 8.3.1
OT.TOE_TC_DTBS_Imp	FDP_UIT.1/DTBS, FTP_ITC.1/DTBS	Section 8.3.1

Table 13 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
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
FMT_SMR.1	OT.Lifecycle_Security, OT.Sigy_SigF
FMT_SMF.1	OT.Lifecycle_Security, OT.Sigy_SigF, OT.SCD_SVD_Corresp
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.Sigy_SigF, OT.SCD/SVD_Auth_Gen
FMT_MSA.3	OT.Lifecycle_Security, OT.Sigy_SigF, OT.SCD/SVD_Auth_Gen

FMT_MSA.4	OT.Lifecycle_Security, OT.Sigy_SigF, OT.SCD/SVD_Auth_Gen, OT.SCD_SVD_Corresp
FMT_MTD.1/Admin	OT.Lifecycle_Security, OT.Sigy_SigF
FMT_MTD.1/Signatory	OT.Lifecycle_Security, OT.Sigy_SigF
FIA_UID.1	OT.Sigy_SigF, OT.SCD/SVD_Auth_Gen, OT.SCD_Auth_Imp
FIA_AFL.1	OT.Sigy_SigF
FIA_UAU.1	OT.Sigy_SigF, OT.SCD/SVD_Auth_Gen, OT.SCD_Auth_Imp, OT.TOE_SSCD_Auth
FDP_SDI.2/DTBS	OT.Sigy_SigF, OT.DTBS_Integrity_TOE
FDP_SDI.2/Persistent	OT.SCD_Secrecy, OT.Sig_Secure, OT.SCD_SVD_Corresp
FDP_RIP.1	OT.SCD_Secrecy, OT.Sigy_SigF
FDP_ACC.1/Signature_Creation	OT.Lifecycle_Security, OT.Sigy_SigF
FDP_ACF.1/Signature_Creation	OT.Lifecycle_Security, OT.Sigy_SigF
FCS_COP.1	OT.Lifecycle_Security, OT.Sig_Secure
FCS_CKM.4	OT.Lifecycle_Security, OT.SCD_Secrecy
FCS_CKM.1	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.SCD_Unique, OT.SCD_SVD_Corresp
FDP_ACC.1/SVD_Transfer	OT.Lifecycle_Security, OT.TOE_TC_SVD_Exp
FDP_ACF.1/SVD_Transfer	OT.Lifecycle_Security, OT.TOE_TC_SVD_Exp
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_UCT.1/SCD	OT.Lifecycle_Security, OT.SCD_Secrecy
FDP_ITC.1/SCD	OT.Lifecycle_Security
FDP_ACC.1/SCD_Import	OT.Lifecycle_Security, OT.SCD_Auth_Imp
FDP_ACF.1/SCD_Import	OT.Lifecycle_Security, OT.SCD_Auth_Imp
FTP_ITC.1/SCD	OT.Lifecycle_Security, OT.SCD_Secrecy
FTP_ITC.1/SVD	OT.TOE_TC_SVD_Exp
FDP_DAU.2/SVD	OT.TOE_TC_SVD_Exp
FIA_API.1	OT.TOE_SSCD_Auth
FDP_UIT.1/DTBS	OT.TOE_TC_DTBS_Imp
FTP_ITC.1/DTBS	OT.TOE_TC_DTBS_Imp

FTP_ITC.1/VAD	OT.TOE_TC_VAD_Imp
FCS_RNG.1	OT.SCD/SVD_Auth_Gen, OT.SCD_Unique

Table 14 SFRs and Security Objectives

8.3.3 Dependencies

8.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCS_RNG.1	No Dependencies	
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	
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)	FMT_SMR.1, FMT_SMF.1, FDP_ACC.1/Signature_Creation, FDP_ACC.1/SVD_Transfer, FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/SCD_Import
FMT_MSA.1/Signatory	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1, FDP_ACC.1/Signature_Creation
FMT_MSA.2	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD/SVD_Generation

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/Signature_Creation, FDP_ACC.1/SCD/SVD_Generation
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
FIA_UID.1	No Dependencies	
FIA_AFL.1	(FIA_UAU.1)	FIA_UAU.1
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FDP_SDI.2/DTBS	No Dependencies	
FDP_SDI.2/Persistent	No Dependencies	
FDP_RIP.1	No Dependencies	
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)	FMT_MSA.3, FDP_ACC.1/Signature_Creation
FCS_COP.1	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1, FDP_ITC.1/SCD
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1, FDP_ITC.1/SCD
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1, FCS_CKM.4
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)	FMT_MSA.3, FDP_ACC.1/SVD_Transfer
FDP_ACC.1/SCD/SVD_Generation	(FDP_ACF.1)	FDP_ACF.1/SCD/SVD_Generation
FDP_ACF.1/SCD/SVD_Generation	(FDP_ACC.1)	FMT_MSA.3,

	and (FMT_MSA.3)	FDP_ACC.1/SCD/SVD_Generation
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_ITC.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SCD_Import
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)	FMT_MSA.3, FDP_ACC.1/SCD_Import
FTP_ITC.1/SCD	No Dependencies	
FTP_ITC.1/SVD	No Dependencies	
FDP_DAU.2/SVD	(FIA_UID.1)	FIA_UID.1
FIA_API.1	No Dependencies	
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
FTP_ITC.1/DTBS	No Dependencies	
FTP_ITC.1/VAD	No Dependencies	

Table 15 SFRs Dependencies

8.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1

ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	(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.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, 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.4, 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.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Table 16 SARs Dependencies

8.3.4 Rationale for the Security Assurance Requirements

The assurance level for this Security Target is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. Augmentation results from the selection of:

- AVA_VAN.5 Advanced methodical vulnerability analysis
- ALC_DVS.2 Sufficiency of security measures

8.3.5 AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component. Independent

vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication.

All the dependencies of AVA_VAN.5, listed below are fulfilled:

- ADV_ARC.1
- ADV_FSP.4
- ADV_TDS.3
- ADV_IMP.1
- AGD_OPE.1
- AGD_PRE.1
- ATE_DPT.1

8.3.6 ALC_DVS.2 Sufficiency of security measures

In order to protect the TOE on development Phase, the component ALC_DVS.2 was added. This latter requires security documentation justifying that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_DVS.2 does not have any dependencies.

9 TOE Summary Specification

9.1 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.

9.1.1 Chip security functionalities

The full list of the IC Platform security functionalities can be checked in the IC Platform Security Target [ST-IC].

9.1.2 Platform security functionalities

The full list of the JC Platform security functionalities can be checked in the JC Platform Security Target [ST-PL].

9.1.3 Application security functionalities

SF.APP_CRYPTO

This SF performs high level cryptographic operations:

- Key generation:
  - SF.APP_CRYPTO performs RSA key generation of size 1024, 1536, 1792, 2048 bits in conformance with RSA PKCS#1 v2.1. Key generation is performed based on random numbers generated by a deterministic RNG according to **[RNG-NIST]**
  - SF.APP_CRYPTO performs EC key pair generation of size 192,224,256, 320,384, 512 and 521 bits in conformance with RSA ANS X9.62.
- Digital signature generation:
  - the signature generation function shall have an access condition based upon previous authentication of user.
- Key destruction
  - For DES, AES and RSA keys, the platform's KEY.clearKey method is used
  - for EC keys, the private s component is overwritten with random values
- SCD/SVD key pair consistency check: SF.APP_CRYPTO performs SCD/SVD consistency check before signature generation by signature generation followed by signature verification. If the signature verification does not match the signature generation, then the key pair is not consistent.
- Encryption/decryption: SF.APP_CRYPTO performs:
  - Encryption and Decryption using TDES 2 Key CBC and 3Key CBC in conformance with FIPS PUB 46-3, ANSI X3.92, FIPS PUB 81 and ISO/IEC 9797 Mode 2

- Encryption and Decryption using AES-128, AES-192, AES-256 following FIPS PUB 197 SP800-38B with ISO/IEC 9797 Mode 2.
- Encryption and Decryption using RSA-1024, 1536, 1792, and 2048 with No Padding
- RSA-1024, 1536, 1792, and 2048 with PKCS#1-OAEP, using SHA-256

o Integrity verification: SF.APP_CRYPTO performs ISO/IEC 9797-1 algorithm 3 padding 2 (3DES) or CMAC (AES) in order to achieve message authentication code in secure messaging.

o Authentication cryptogram creation/verification: SF.APP_CRYPTO performs the following authentication cryptogram calculation/verification:

- Mutual symmetric authentication based on TDES or AES
- Device symmetric authentication based on TDES or AES
- Device asymmetric authentication based on RSA
- Role symmetric authentication based on TDES or AES
- Role asymmetric authentication based on RSA

o Encryption Key Decipherment with ECDH - 192, 224, 256, 320, 384, 512 and 521 following CEN - EN 14890-2 using ECDH as defined in IETF RFC 6278

o Client/Server Authentication

- 3DES MAC3 2Key and 3DES MAC3 3Key following FIPS PUB 46-3, ANSI X3.92, FIPS PUB 81 with ISO/IEC 9797 Mode 1
- AES-128, AES-192, AES-256 CMAC following FIPS PUB 197 SP800-38B
- RSA-1024, 1536, 1792, and 2048 with PKCS#1 v1.5

o Random Number Generation according to FCS_RNG.1

It enables to perform e-Services such as

o Client/Server authentication

o Decryption key decipherment

All cryptographic functionalities are provided by the JC Platform and the IC (see [ST-PL], [ST-IC]).

SF.APP_INTEGRITY

The TOE performs self tests as described in FPT_TST.1 on the TSF data it stores to protect the TOE. This TSF also monitors the integrity of the access conditions of created data objects and also ensures that no residual information is available after a PIN update or clearance. This security functionality monitors the integrity of sensitive user data and the integrity of the DTBS/R(FDP_SDI.2/DTBS). The integrity of persistently stored data such as SCD, RAD and SVD is monitored using the JC Platform features (see [ST-PL])). In case of integrity error this TSF will:

o Prohibit the use of the altered data, and

o Inform the S.Signatory about integrity error.

SF.AUTHENTICATION

Only authenticated terminals can get access to the user data stored on the TOE. The applet offers several authentication schemes enabling to authenticate different roles as described in FMT_SMR.1, such as:

o The R.Sigy entitled to use the services offered by the card. It is called "User Authentication".

- The R.Admin of a service, to administrate some features. It is called "Role authentication".

and

- The device communicating with the card, to establish a trusted channel (secure messaging) and protect the communication. It is called "Device authentication".

The **User authentication** is based on the submission of a PIN (i.e., knowledge based).

- Knowledge based: The Authentication of the user relies on a shared secret (PIN), known by both the holder and the smartcard. The Card holder is authenticated by the means of the VERIFY command. For each SCD, separate signatory's RADs (PINs) are assigned. The verification process uses a velocity checking mechanism, thus a remaining tries counter and a maximum error counter are defined for each PIN. If the verification fails, the tries counter is decremented by one and an error status that contains the remaining attempts is returned by the application. When all available tries have failed, the PIN is blocked and can no longer be used. Note that a successful verification of the PIN resets its remaining tries counter to the maximum error counter.

The **Device authentication** aims at authenticating both entities willing to communicate and securing the communication between the card and a service provider (it might be a terminal, a server, etc). It enables the TOE to establish a trusted channel with remote IT entities such as the SCA, the CGA, and the HID. The device authentication may be either realized with symmetric or asymmetric scheme.

- Symmetric Authentication Scheme: The smart card implements a symmetric mutual authentication scheme. This one relies either on 3DES or AES Cipher block and used to:
  - Authenticate the terminal and the card.
  - Initialize the counter used at each checksum computation.
- Asymmetric Authentication Scheme based on RSA
- Device authentication with privacy protection:
  - Diffie-Hellman mutual authentication scheme
  - This asymmetric scheme relies on the Card Verifiable Certificate (CVC) PKI to authenticate the terminal and makes use of the RSA cryptography.

The **Role authentication** presents the procedure to authenticate an external entity to the card in order to associate to it a specific role (e.g., access rights). It enables the TOE to authenticate the Personalization Agent and the Administrator. Two schemes may be used:

- A symmetric role authentication relying either on 3DES or AES Cipher block
- An asymmetric role authentication based on RSA

This SF performs Client/Server authentication (e-Services):

- this feature enables to authenticate the TOE on behalf of the cardholder’s PC to a remote web server.

In the applet, the Access conditions "Secure Messaging" mandates both a successful terminal authentication and an active secure messaging session. The established secure messaging session along with terminal authentication helps identify the SSCD itself as required by FIA_API.1.

This security function manages authentication failure: when the "highest value in the configurable range of positive numbers fixed by the Adminstrator" unsuccessful authentication attempts has been met, the TSF shall block the PIN (RAD) and PUK. It also doesnt allow any new authentication attempts as defined by FIA_AFL.1.

This security functionality allows the following operations to be performed before the user is identified or authenticated to meet FAU_UID.1 and FAU_UAU.1:

- Identification of the user(if not already identified),
- Self test according to FPT_TST.1
- Establishing a trusted path between the HID and the TOE,
- Establishing a trusted channel between the SCA and the TOE,
- Establishing a trusted channel between the CGA and the TOE.

SF.MANAGEMENT

This SF manages the access to objects (files, directories, data and secrets) stored in the file system. It also controls write access of initialization, pre-personalization and personalization data based on the roles described in FMT_SMR.1.

This SF ensures secure management of secrets such as cryptographic keys. It also covers access to keys as well as secure key deletion.

This SF controls all the operations relative to the RAD/VAD management, to ensure FMT_SMF.1 is enforced, including the Cardholder (signatory) authentication:

- RAD creation: the RAD is stored and is associated to a maximum successful presentation number (usage counter) and to a maximum error number.
- VAD verification: the RAD can be accessed only if its format and integrity are correct and if the usage counter has not reached 0. If the RAD is blocked, then it cannot be used anymore.
- RAD ratification counter: The number of authentication attempts is limited by a counter associated to the RAD. The counter is decremented each time the VAD verification fails. The RAD cannot be used any longer if the counter reaches zero.
- RAD usage counter: the usage counter is decremented each time the RAD is verified successfully. When this counter reaches 0, the RAD cannot be verified anymore.
- RAD modification: the RAD can be changed by the cardholder (loading a new value). The RAD is managed and stored by the application. The operations on RAD and VAD are performed thanks to services offered by the JC Platform using by the javacard.framework.OwnerPin class

This SF manages the following functions related to security attributes:

- Controls access for and manages:
  - Modification of SCD/SVD Management(S.Admin)
  - Modification of SCD Operational(S.Sigy)
- Change the default value the attribute of SCD Identifer
- Management of SCD Operational attribute in case of SCD/SVD pair generation or SCD import without S.Sigy authentication as described in FMT_MSA.4.
- Ensures secure values are accepted for the above security attributes to enforce FMT_MSA.2 and provides restrictive default values for them FMT_MSA.3.

This SF manages the security environment of the application and:

- Maintains the roles of Signatory and Administrator as defined in FMT_SMR.1.
- Controls if the authentication required for a specific operation has been performed with success.
- Ensures that only secure values are accepted for security attributes. This security functionality restricts the ability to perform the function Signature creation to

Signatory to enforce FMT_MOF.1. This security functionality ensures that only Administrator is authorized to

- Modify Initialization SFP and Signature creation SFP attributes
- Specify alternative default values

This SF provides the electronic signature application with access control and ensures that the following operations are executed by authorized roles:

- o Export of SVD to CGA by R.Sigy or R.Admin depending on the personalization
- o Generation of SCD/SVD pair by the either R.Sigy or R.Admin depending on the personalization
- o Creation of RAD by the Administrator
- o Signing of DTBS/R by S.Signatory
- o Import of SCD

This SF manages:

- o Enabling of the signature creation function for FMT_SMF.1
- o Session key generation
  - Session keys are protected in integrity and confidentiality during generation. This SF enforces secure storage of the session keys during generation
- o The creation of any kind of keys and the DH parameters
- o The update of the keys (symmetric key used for authentication of external entity, SCD/SVD, e-Services keys, asymmetric keys for TOE's authentication) and the DH Domain parameters

This SF manages key destruction according to FCS_CKM.4 when:

- o A key value is updated (by import or generation), the former key value is destroyed
- o This SF calls the security function from the JC Platform to erase keys The respective key destruction methods for different keys are defined in SF.APP_CRYPTO

This SF manages Secret loading:

- o Loading of a secret is always done by an authorized user through a secure command. This command is accepted only after authentication of the authorized user.

This SF manages the secure transfer of every secret to the cryptoprocessor when used for cryptographic operation.

Access control is enforced by the APDU methods as specified in the interfaces defined in the functional specification.

SF.PHYSICAL_PROTECTION

This security function uses platform functionality to protect the TOE against physical attacks(FPT_PHP.1, FPT_PHP.3). It ensures their detection and provides counteractions. It also ensures that the TOE emanations don't exceed the specified limits as described in FPT_EMS.1.

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. The counter is

reinitialised when the authentication is successful. If the counter reaches its maximum value, then the related secret is blocked and cannot be used anymore.

SF.SAFE_STATE_MANAGEMENT

This security function utilizes platform and ic functions to ensure that the TOE gets back to a secure state when any of the conditions described in FPT_FLS.1 occur.

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. This security function requires the TOE and the entity between which a trusted channel shall be established to be authenticated with SF.AUTHENTICATION.

This SF helps ensure by means of these secure communication channels that FTP_ITC.1/SCD, FTP_ITC.1/SVD, FTP_ITC.1/DTBS, FTP_ITC.1/VAD is enforced.

The applet performs the following secure messaging tasks with external applications (SCA, HID or CGA) for protection of the communication data as the DTBS, authentication data as the VAD or for ensuring the integrity of the SVD:

- Encryption and decryption of the transmitted message.
- MAC generation and verification for secure messaging.
- Random number generation.

This SF manages four modes of secure channel during the personalization phase:

- No secure messaging
- Integrity mode
- Confidentiality mode
- Integrity and confidentiality mode

When the secure messaging session is closed or when an error is detected by the TOE, the session keys are erased.

9.2 SFRs and TSS

9.2.1 SFRs and TSS - Rationale

All SSCD parts

Protection of the TSF (FPT)

FPT_EMS.1 is enforced by the SF.PHYSICAL_PROTECTION functionality. SF.PHYSICAL_PROTECTION is responsible for maintaining physical security and ensuring there are no emanations during secret operations in the TOE.

FPT_FLS.1 is met by SF.SAFE_STATE_MANAGEMENT

FPT_PHP.1 is met by SF.PHYSICAL_PROTECTION, the JC Platform and the IC that ensure that physical tampering of the TOE is detected and that the proper actions (reset, card termination) are taken, so that is can be determined if a physical tampering has occurred.

FPT_PHP.3 is met by the JC Platform and the IC that ensures that physical tampering of the TOE is detected and that the proper actions (reset, card termination) in order to protect the TOE.It is also met by SF.PHYSICAL_PROTECTION that monitors the integrity of sensitive data.

FPT_TST.1 is met by JC Platform and the IC that performs a set of self-tests at start-up, thus checking the correct operation of the TSF, and that verifies the integrity of the stored executable code before or during its execution and by SF.APP_INTEGRITY that provides means to verify the integrity of the data stored on the TOE.

Security management (FMT)

FMT_SMR.1 is met by SF.AUTHENTICATION that provides user authentication as administrator or as signatory and by SF.MANAGEMENT that grants to the administrator and to the signatory specific access rights, thus defining roles for the TOE.

FMT_SMF.1 requires that the TSF shall be capable of performing the following management functions: (1) Creation and modification of the reference authentication data (RAD), (2) Enabling the signature-creation function, (3) Modification of the security attribute SCD/SVD management, SCD operational, (4) Change the default value of the security attribute SCD Identifier. This is realized by SF.MANAGEMENT.

FMT_MOF.1 is met by SF.MANAGEMENT and SF.AUTHENTICATION that ensures that only authenticated signatory can perform DTBS signature.

FMT_MSA.1/Admin is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE.

FMT_MSA.1/Signatory is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE.

FMT_MSA.2 is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE and in particular manages the security attributes.

FMT_MSA.3 is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE and in particular manage the security attributes, their initialisation and their access rights.

FMT_MSA.4 requires that the TSF shall use the following rules to set the value of security attributes: (1) if S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute 'SCD operational of the SCD' shall be set to 'no' as a single operation; (2) if S.Sigy successfully generates an SCD/SVD pair the security attribute 'SCD operational of the SCD' shall be set to 'yes' as a single operation. This is realized by SF.MANAGEMENT and SF.AUTHENTICATION.

FMT_MTD.1/Admin

- is met by SF.MANAGEMENT that manages the authentication function and ensure that only authenticated administrator can create the RAD.
- is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/Signatory

- is met by SF.MANAGEMENT that manages the authentication function and ensure that only authenticated signatory can modify the RAD.
- is met by SF.AUTHENTICATION that provides the authentication protocol.

Identification and authentication (FIA)

FIA_UID.1

- is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to autorized functions.

FIA_AFL.1

- This SFR is met by SF.AUTHENTICATION and SF.MANAGEMENT.
- This SFR is also met by SF.RATIF that ensures that the RAD is blocked after a defined number of failed successive signatory authentication attempts.

FIA_UAU.1

- is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to autorized functions.
- is met by SF.TRUSTED_CHANNEL that provides a trusted secure messaging with CGA and SCA.

User data protection (FDP)

FDP_SDI.2/DTBS is met by SF.APP_INTEGRITY, that ensures the integrity of data stored in the TOE, by the JC Platform and the IC that ensure that the proper reaction is taken

(reset or card termination) if an integrity error is detected, so that the user knows an error had occurred and that no altered data can be used.

FDP_SDI.2/Persistent is met by SF.APP_INTEGRITY, that ensures the integrity of data stored in the TOE, by the JC Platform and the IC that ensure that the proper reaction is taken (reset or card termination) if an integrity error is detected, so that the user knows an error had occurred and that no altered data can be used.

FDP_RIP.1 is met by SF.MANAGEMENT that ensures erasure of data in FLASH and in RAM (e.g. after the signature creation process), and in particular of SCD, VAD and RAD.

FDP_ACC.1/Signature_Creation is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that all the access conditions are met before a dedicated operation can be performed, and in particular that only a user authenticated as signatory can perform signature of DTBS loading from an authorized SCA with a RSA key pair whose consistency has been verified, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/Signature_Creation is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that all the access conditions are met before a dedicated operation can be performed, and in particular that only a user authenticated as signatory can perform signature of DTBS loading from an authorized SCA with a RSA key pair whose consistency has been verified, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

Cryptographic support (FCS)

FCS_COP.1

- is met by SF.APP_CRYPTO that provides support for the Cryptographic algorithms using platform functionalities

FCS_CKM.4 is met by SF.MANAGEMENT and SF.APP_CRYPTO, as SF.MANAGEMENT manages the secure destruction of secret using the methods described in SF.APP_CRYPTO, and in particular of the SCD.

SSCD parts 2, 4 and 5 only

Cryptographic support (FCS)

FCS_CKM.1

- is met by SF.APP_CRYPTO that ensures that the TOE generates SCD/SVD cryptographic key pairs.
- is also met by SF.APP_CRYPTO, which provides RSA calculation.
- is also met by SF.MANAGEMENT, which ensures the protection of the keys during generation.

User data protection (FDP)

FDP_ACC.1/SVD_Transfer is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SVD export, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/SVD_Transfer is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SVD export, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACC.1/SCD/SVD_Generation is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD/SVD generation, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/SCD/SVD_Generation is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD/SVD generation, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

SSCD parts 3 and 6 only

User data protection (FDP)

FDP_UCT.1/SCD is met by SF.AUTHENTICATION and SF.MANAGEMENT that ensure that all the conditions are met before allowing a SCD import and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to protect the SCD from disclosure during its import.

FDP_ITC.1/SCD is met by SF.AUTHENTICATION and SF.MANAGEMENT that ensure that all the required conditions are met before allowing a SCD import operation.

FDP_ACC.1/SCD_Import is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD import, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/SCD_Import is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD import, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FTP_ITC.1/SCD is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for SCD Import and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a CSP to protect the exchanged data (SCD) from modification and disclosure.

SSCD part 4 only

Trusted path/channels (FTP)

FTP_ITC.1/SVD is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for SVD Transfer and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a CGA to protect the exchanged data (SVD) from modification and disclosure.

User data protection (FDP)

FDP_DAU.2/SVD is met by SF.AUTHENTICATION and SF.TRUSTED_CHANNEL to ensure that exported SVD to the CGA is authenticated and unmodified.

Identification and authentication (FIA)

FIA_API.1 is met by SF.AUTHENTICATION that provides mutual authentication via a succesful Terminal Authentication and an established Secure Messaging Session.

SSCD parts 5 and 6 only

User data protection (FDP)

FDP_UIT.1/DTBS requires that integrity of the DTBS/R to be signed is to be verified, as well as the DTBS/R is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms (SF.TRUSTED_CHANNEL, SF.APP_CRYPTO).

Trusted path/channels (FTP)

FTP_ITC.1/DTBS is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for DTBS Import and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a SCA to protect the exchanged data (DTBS) from modification and disclosure.

FTP_ITC.1/VAD is met by SF.AUTHENTICATION, SF.MANAGEMENT that enforce the access right policy for VAD transfer and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a HID to protect the exchanged data (VAD) from modification and disclosure.

Additional SFR

FCS_RNG.1 The FCS_RNG.1 SFR is enforced by the SF.APP_CRYPTO functionality. SF.APP_CRYPTO ensures that a random number compliant with the requirement is generated when needed.

9.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FPT_EMS.1	SF.PHYSICAL_PROTECTION
FPT_FLS.1	SF.SAFE_STATE_MANAGEMENT
FPT_PHP.1	SF.PHYSICAL_PROTECTION
FPT_PHP.3	SF.PHYSICAL_PROTECTION
FPT_TST.1	SF.APP_INTEGRITY
FMT_SMR.1	SF.AUTHENTICATION, SF.MANAGEMENT
FMT_SMF.1	SF.MANAGEMENT
FMT_MOF.1	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MSA.1/Admin	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MSA.1/Signatory	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MSA.2	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MSA.3	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MSA.4	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MTD.1/Admin	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MTD.1/Signatory	SF.MANAGEMENT, SF.AUTHENTICATION
FIA_UID.1	SF.AUTHENTICATION, SF.MANAGEMENT
FIA_AFL.1	SF.MANAGEMENT, SF.AUTHENTICATION, SF.RATIF
FIA_UAU.1	SF.AUTHENTICATION, SF.MANAGEMENT, SF.TRUSTED_CHANNEL
FDP_SDI.2/DTBS	SF.APP_INTEGRITY
FDP_SDI.2/Persistent	SF.APP_INTEGRITY
FDP_RIP.1	SF.MANAGEMENT
FDP_ACC.1/Signature_Creation	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACF.1/Signature_Creation	SF.MANAGEMENT, SF.AUTHENTICATION
FCS_COP.1	SF.APP_CRYPTO, SF.AUTHENTICATION, SF.TRUSTED_CHANNEL
FCS_CKM.4	SF.MANAGEMENT, SF.APP_CRYPTO
FCS_CKM.1	SF.APP_CRYPTO, SF.MANAGEMENT
FDP_ACC.1/SVD_Transfer	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACF.1/SVD_Transfer	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACC.1/SCD/SVD_Generation	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACF.1/SCD/SVD_Generation	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_UCT.1/SCD	SF.TRUSTED_CHANNEL, SF.APP_CRYPTO, SF.AUTHENTICATION, SF.MANAGEMENT

FDP_ITC.1/SCD	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACC.1/SCD_Import	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACF.1/SCD_Import	SF.MANAGEMENT, SF.AUTHENTICATION
FTP_ITC.1/SCD	SF.MANAGEMENT, SF.APP_CRYPTO, SF.TRUSTED_CHANNEL, SF.AUTHENTICATION
FTP_ITC.1/SVD	SF.MANAGEMENT, SF.TRUSTED_CHANNEL, SF.APP_CRYPTO, SF.AUTHENTICATION
FDP_DAU.2/SVD	SF.AUTHENTICATION, SF.TRUSTED_CHANNEL
FIA_API.1	SF.AUTHENTICATION
FDP_UIT.1/DTBS	SF.TRUSTED_CHANNEL, SF.APP_CRYPTO
FTP_ITC.1/DTBS	SF.TRUSTED_CHANNEL, SF.APP_CRYPTO, SF.MANAGEMENT, SF.AUTHENTICATION
FTP_ITC.1/VAD	SF.TRUSTED_CHANNEL, SF.APP_CRYPTO, SF.AUTHENTICATION, SF.MANAGEMENT
FCS_RNG.1	SF.APP_CRYPTO

Table 17 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
SF.APP_CRYPTO	FCS_RNG.1, FCS_COP.1, FCS_CKM.4, FCS_CKM.1, FDP_UCT.1/SCD, FTP_ITC.1/SCD, FTP_ITC.1/SVD, FDP_UIT.1/DTBS, FTP_ITC.1/DTBS, FTP_ITC.1/VAD
SF.APP_INTEGRITY	FPT_TST.1, FDP_SDI.2/DTBS, FDP_SDI.2/Persistent
SF.AUTHENTICATION	FMT_SMR.1, 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, FIA_UID.1, FIA_AFL.1, FIA_UAU.1, FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, FCS_COP.1, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FDP_UCT.1/SCD, FDP_ITC.1/SCD, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FTP_ITC.1/SCD, FTP_ITC.1/SVD, FDP_DAU.2/SVD, FIA_API.1, FTP_ITC.1/DTBS, FTP_ITC.1/VAD
SF.MANAGEMENT	FMT_SMR.1, FMT_SMF.1, 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, FIA_UID.1, FIA_AFL.1, FIA_UAU.1, FDP_RIP.1, FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, FCS_CKM.4, FCS_CKM.1, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer,

	FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FDP_UCT.1/SCD, FDP_ITC.1/SCD, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FTP_ITC.1/SCD, FTP_ITC.1/SVD, FTP_ITC.1/DTBS, FTP_ITC.1/VAD
SF.PHYSICAL_PROTECTION	FPT_EMS.1, FPT_PHP.1, FPT_PHP.3
SF.RATIF	FIA_AFL.1
SF.SAFE_STATE_MANAGEMENT	FPT_FLS.1
SF.TRUSTED_CHANNEL	FIA_UAU.1, FCS_COP.1, FDP_UCT.1/SCD, FTP_ITC.1/SCD, FTP_ITC.1/SVD, FDP_DAU.2/SVD, FDP_UIT.1/DTBS, FTP_ITC.1/DTBS, FTP_ITC.1/VAD

Table 18 TSS and SFRs - Coverage