SECURITY TARGET LITE
IDEAL CITIZ V2.16-I EMBEDDING VITALE APPLICATION

Reference: 2018_2000035874

Table of contents

1 INTRODUCTION 7

1.1 ST IDENTIFICATION 9
1.2 TOE REFERENCE 9
1.3 REVISIONS AND COMMENTS 9
1.4 TOE DOCUMENTATION 10

2 TECHNICAL TERMS, ABBREVIATION AND ASSOCIATED REFERENCES 11

2.1 TECHNICAL TERMS 11
2.2 ABBREVIATION 14
2.3 ASSOCIATED REFERENCES 16

3 TOE OVERVIEW 18

3.1 TOE PRESENTAION 18
3.2 TOE TYPE 18
3.3 TOE DESCRIPTION 19
3.3.1 Integrated Circuit M7892 B11 19
3.3.2 Java Card Platform IDeal Citiz v2.16-i 20
3.3.3 Application Layer 20
3.3.4 Application Data 21
3.3.5 Required non-TOE hardware/software/firmware 22
3.4 TOE FUNCTIONS 23
3.5 OPERATIONS OF THE TOE 24
3.6 MAJOR SECURITY FEATURES OF THE TOE 28
3.6.1 Authentication mechanisms 28
3.6.2 Cryptographic 29
3.6.3 Key Management 29
3.6.4 PIN Management 29
3.6.5 Trusted Channels 29
3.6.6 Access Control 30
3.6.7 Data Storage 30
3.6.8 Integrity 30
3.6.9 Confidentiality 30
3.6.10 Features from the Platform 30

4 LIFE CYCLE 31

4.1 SSCD PRODUCT LIFE CYCLE 31
4.1.1 SSCD Preparation phase 31
4.1.2 SSCD Operational Use phase 32
4.2 TOE LIFE CYCLE 33
4.2.1 Development phase (Stages 1 & 2 of the IC life cycle [PP-IC]) 34
4.2.2 Production phase (Stages 3 & 4 of the IC life cycle [PP-IC]) 34
4.2.3 Preparation phase (Stages 5 & 6 of the IC life cycle [PP-IC]) 35
4.2.4 Operational phase (Stage 7 of the IC life cycle [PP-IC]) 36

5 CONFORMANCE CLAIMS 38

5.1 CC CONFORMANCE 38
5.2 PP CLAIMS 38
5.3 CONFORMANCE RATIONALE 39

6 SECURITY PROBLEM DEFINITION 46

6.1 ASSETS 46
6.1.1 From PPs 46

6.1.2 Additional Assets 46
6.2 USERS / SUBJECTS 47
6.2.1 Threat agents 47
6.2.2 Miscellaneous 47
6.3 THREATS 47
6.4 ORGANISATIONAL SECURITY POLICIES 48
6.5 ASSUMPTIONS 49
6.5.1 All SSCD parts 49
6.5.2 Parts 3 and 6 only 49
6.5.3 Additional Assumption 49
7 SECURITY OBJECTIVES 51
7.1 SECURITY OBJECTIVES FOR THE TOE 51
7.1.1 All SSCD parts 51
7.1.2 SSCD parts 2, 4 and 5 only 52
7.1.3 SSCD parts 3 and 6 only 52
7.1.4 SSCD part 4 only 53
7.1.5 SSCD parts 5 and 6 only 53
7.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 53
7.2.1 All SSCD parts 53
7.2.2 SSCD parts 3 and 6 only 54
7.2.3 SSCD part 4 only 55
7.2.4 SSCD parts 5 and 6 only 55
7.2.5 Additional OE 56
7.3 SECURITY OBJECTIVES RATIONALE 57
7.3.1 Threats 57
7.3.2 Organisational Security Policies 59
7.3.3 Assumptions 62
7.3.4 SPD and Security Objectives 62
8 EXTENDED REQUIREMENTS 67
8.1 EXTENDED FAMILIES 67
8.1.1 Extended Family FPT_EMS - TOE Emanation 67
8.1.2 Extended Family FIA_API - Authentication Proof of Identity 68
9 SECURITY REQUIREMENTS 69
9.1 SECURITY FUNCTIONAL REQUIREMENTS 69
9.1.1 All SSCD parts 69
9.1.2 SSCD parts 2, 4 and 5 only 78
9.1.3 SSCD parts 3 and 6 only 80
9.1.4 SSCD part 4 only 82
9.1.5 SSCD parts 5 and 6 only 83
9.2 SECURITY ASSURANCE REQUIREMENTS 84
9.3 SECURITY REQUIREMENTS RATIONALE 84
9.3.1 Objectives 84
9.3.2 Rationale tables of Security Objectives and SFRs 87
9.3.3 Dependencies 90
9.3.4 Rationale for the Security Assurance Requirements 93
10 TOE SUMMARY SPECIFICATION 95
10.1 TOE SUMMARY SPECIFICATION 95
10.1.1 Chip security functionalities 95
10.1.2 Platform security functionalities 95
10.1.3 Application security functionalities 95

10.2 SFRs AND TSS.....101
10.2.1 SFRs and TSS - Rationale 101
10.2.2 Association tables of SFRs and TSS 107

Table of figures

Figure 1: VITALE Architecture 7
Figure 2: TOE physical scope 19
Figure 3: TOE and Operational environments with Key Generation 24
Figure 4: TOE and Operational environments with Key Import 25
Figure 5: TOE and Operational environments with Key Generation and trusted channel to CGA 25
Figure 6: TOE and Operational environments with Key Generation and trusted channel to SCA 26
Figure 7: TOE and Operational environments with Key Import and trusted channel to SCA 26
Figure 8: SSCD Product Life Cycle 31
Figure 9: TOE Life Cycle 33

Table of tables

Table 1 PP SPDs vs. ST 41
Table 2 PP Security Objectives vs. ST 43
Table 3 PP SFRs vs. ST 45
Table 4 Threats and Security Objectives - Coverage 63
Table 5 Security Objectives and Threats - Coverage 64
Table 6 OSPs and Security Objectives - Coverage 64
Table 7 Security Objectives and OSPs - Coverage 65
Table 8 Assumptions and Security Objectives for the Operational Environment - Coverage 66
Table 9 Security Objectives for the Operational Environment and Assumptions - Coverage 66
Table 10 Security Objectives and SFRs - Coverage 88
Table 11 SFRs and Security Objectives 90
Table 12 SFRs Dependencies 92
Table 13 SARs Dependencies 93
Table 14 SFRs and TSS - Coverage 108

1 Introduction

This document is the Security Target Lite for the VITALE product on IDeal Citiz™ v2.16-i Platform which is an IDEMIA specific Java Card implementation [JC] of the SESAM VITALE specification [FSP] and the GIXEL IAS Premium v1.01 specification [IAS-PRE].

VITALE is the support of health services as defined in the SESAM VITALE context to offer government e-services.

VITALE is a multi-applicative software intended to host four types of applications: VITALE2, VITALE1, ADELE and AIP. During the pre-personalization and personalization phases, the product can be configured to serve different use cases.

VITALE2 Application must replace progressively VITALE1 that is currently in operation and maintained in parallel with VITALE2. The VITALE card is still supporting VITALE1.

VITALE architecture can be viewed as shown in the following figure:

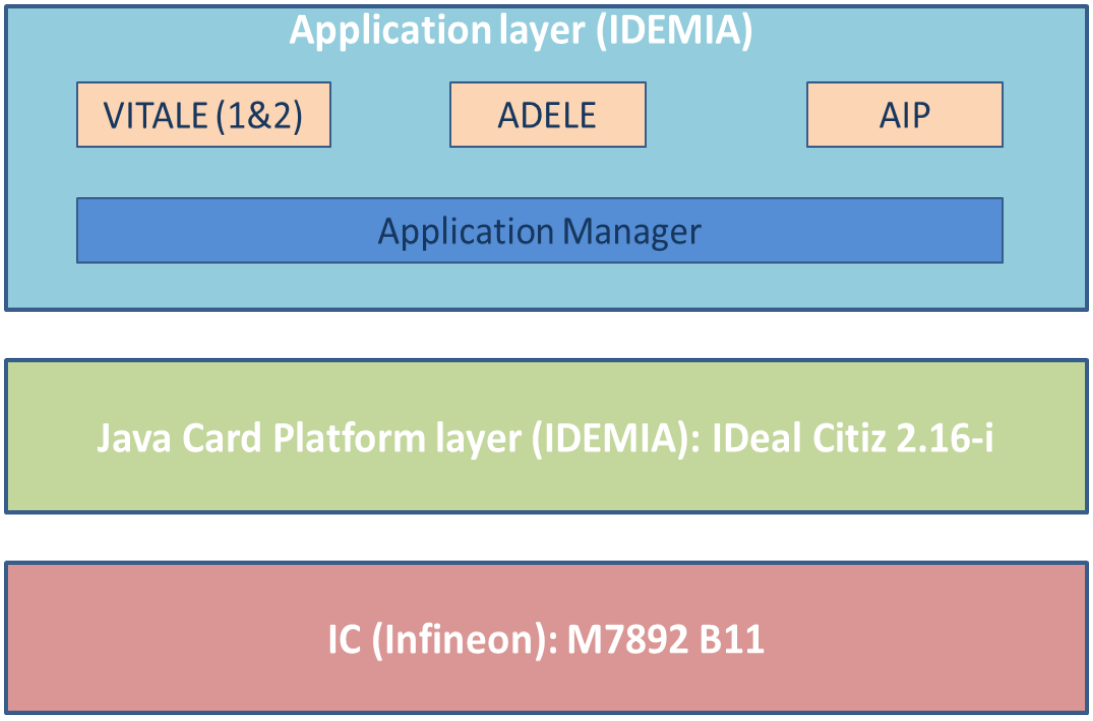

Figure 1: VITALE Architecture

The scope of the TOE in this security target encompasses only VITALE2, VITALE1, and ADELE.

In this document, the term 'VITALE' referes to the TOE which encompasses VITALE2, VITALE1, as well as ADELE.

VITALE is configured during the personalization phase, using the AIP Application. The AIP is out of the TOE as it is desactivated in the operational phase.

The TOE addressed by the current ST is a SSCD device (combination of SSCD Parts 2 to 6) according to [DIR] 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].

VITALE is a set of Java Card services intended to be used exclusively on the IDeal Citiz™ v2.16-i Java Card Platform, which is certified according to CC EAL 5+ [ST-PL]. This Platform is based on the Infineon M7892 B11 IC security controller, which is itself certified according to CC EAL 6+ [ST-IC], [CR-IC].

This ST has been conceived to prepare a Common Criteria evaluation following the "compositional approach" described in [COMP]. This approach consists in starting from a Platform that has been independently certified, and performing an evaluation of the product resulting from embedding an Application into it, which makes use of some of the results issued from the evaluation of the IDeal Citiz™ v2.16-i Java Card Platform.

This document provides a list of security requirements for a VITALE embedded on IDeal Citiz™ v2.16-i Java Card Platform.

This Security Target describes:

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

The assurance level for the TOE is CC EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

1.1 ST Identification

Title	Security Target Lite IDeal Citiz v2.16-i embedding VITALE application
Reference	2018_2000035874
Version	1.2
Date of Issue	24/09/2018
ITSEF	CEA-LETI
Certification Body	ANSSI
Author	IDEMIA
CC Version	3.1 Revision 5
Assurance Level	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
Protection Profiles	PP SSCD-Part 2 Key Generation [PP-SSCD2], PP SSCD-Part 3 Key Import [PP-SSCD3], PP SSCD-Part 4 Key Generation and Trusted Channel with CGA [PP-SSCD4], PP SSCD-Part 5 Key Generation and Trusted Channel with SCA [PP-SSCD5], PP SSCD-Part 6 Key Import and Trusted Channel with SCA [PP-SSCD6]

1.2 TOE Reference

Developer	IDEMIA
TOE commercial name	IDeal Citiz v2.16-i embedding VITALE applicationn
TOE version number	1.2
Name of JC Platform	IDeal Citiz v2.16i on M7892 B11 Java Card Open Platform [ST-PL]
Version of JC Platform	2.1.2
JC Ref. Certificate	ANSSI-CC-2017/74 [CR-PL]
IC Identifiers	Infineon M7892 B11 [ST-IC]
IC Ref. Certificate	BSI-DSZ-CC-0782-V3-2017 [CR-IC]

1.3 Revisions and Comments

Version	Issue Date	Author	Comments
1.0	16-05-2018	IDEMIA	Initial Version
1.1	08-06-2018	IDEMIA	Update TOE reference
1.2	24-09-2018	IDEMIA	Update AGD versions

1.4 TOE Documentation

The TOE documentation is listed in the table below:

[AGD_OPE]	2018_2000033538 - Guide d'utilisation Manuel utilisateur, v1.4
[AGD_PRE]	2018_2000033539 - Guide d'utilisation Manuel de Pré-Personnalisation – Personnalisation, v1.6
[FSP_VITALE]	2017_2000024578 - Spécifications techniques - Spécification fonctionnelle VITALE
[FSP_ADELE]	2017_2000024577 - Spécifications techniques - Spécification fonctionnelle ADELE
[FSP_AIP]	2017_2000024579 - Spécifications techniques - Spécification fonctionnelle AIP

2 Technical terms, Abbreviation and Associated references

2.1 Technical terms

Term	Definition
Application note	*Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.*
Administrator	*user who performs TOE initialization, TOE personalization, or other TOE administrative functions*
Advanced electronic signature	*An electronic signature which meets the following requirements [DIR]:* *(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 information	*information associated with an SCD/SVD pair that may be stored in a secure signature creation device* *NOTE 1: Certificate info is either* - *a signer's public key certificate or,* - *one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values.* *NOTE 2: Certificate info may contain information to allow the user to distinguish between several certificates.*
Certificate-generation application (CGA)	*collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate*

Term	Definition
Certification service provider (CSP)	*entity that issues certificates or provides other services related to electronic signatures*
Data to be signed (DTBS)	*all of the electronic data to be signed including a user message and signature attributes*
Data to be signed or its unique representation (DTBS/R)	*data received by a secure signature creation device as input in a single signature creation operation* *NOTE: Examples of DTBS/R are* - *a hash value of the data to be signed (DTBS), or* - *an intermediate hash value of a first part of the DTBS complemented with a remaining part of the DTBS, or* - *the DTBS.*
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.*
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).*

Term	Definition
Public Key	*Publicly known key in an asymmetric cipher which is used for encryption and verification of digital signatures.*
Public key infrastructure (PKI)	*Combination of hardware and software components, policies, and different procedures used to manage digital certificates.*
Qualified certificate	*public key certificate that meets the requirements laid down in Annex I and that is provided by a CSP that fulfils the requirements laid down in Annex II (the directive: 2.10) [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).*
Random numbers	*Many cryptographic algorithms or protocols require a random element, mostly in form of a random number, which is newly generated in each case. In these cases, the security of the procedure depends in part on the suitability of these random numbers. As the generation of real random numbers within computers still imposes a problem (a source for real random events can in fact only be gained by exact observation of physical events, which is not easy to realize for software), so called pseudo random numbers are used instead.*
Reference authentication data (RAD)	*Data persistently stored by the TOE for authentication of a user as authorised for a particular role.*
Secure messaging	*Secure messaging using encryption and message authentication code ac-cording to ISO/IEC 7816-4.*
Secure signature creation device (SSCD)	*Personalized device that meets the requirements laid down in [DIR], Annex III by being evaluated according to a security target conforming to this PP ([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.*
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*

Term	Definition
Signature verification data (SVD)	*public cryptographic key that can be used to verify an electronic signature*
Signed data object	*The electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.*
Smart card	*A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (ROM, 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*

2.2 Abbreviation

Acronym	Definition
ADF	*Application Dedicated File*
AES	*Advanced Encryption Standard*
AID	*Application Identifier*
APDU	*Application Protocol Data Unit*
CA	*Certification authority*
CAD	*card acceptance device*
CC	*Common Criteria*
CGA	*Certification generation application*
CPU	*Central Processing Unit*
CSP	*certification service provider*
CHA	*Certificate Holder Authority*
CHR	*Certificate Holder Reference*
CIA	*Cryptographic Information Application*
CPI	*Card Profile Identifier*
CRT	*Control Reference Template*

CVC	*Card Verifiable Certificate*
DPA	*differential power analysis*
DTBS	*Data to be signed*
DTBS/R	*Data to be signed or its unique representation*
DF	*Directory File*
DO	*Data Object*
DOCP	*Data Object Control Parameters*
DOUP	*Data Object Usage Parameters*
EAL	*Evaluation assurance level*
EF	*Elementary File*
FCP	*File Control Parameter*
FLASH	*electrically erasable and programmable read only memory*
IAS	*Identification Authentification Signature*
GP	*GlobalPlatform*
HID	*human interface device*
IT	*Information technology*
JCVM	*Java Card virtual machine*
MAC	*Message Authentication Code*
MPU	*Memory Protection Unit*
MF	*Master File*
MSE	*Manage Security Environment*
NVM	*Non Volatile Memory*
OS	*Operating System*
OSP	*Organizational security policy*
OAEP	*Optimal Asymmetric Encryption Padding*
OS	*Operating System*
PIN	*Personal Identification Number*
PP	*Protection profile*
PUK	*PIN Unblocked Key*
PKI	*Public Key Infrastructure*
RAD	*Reference authentication data*
RAM	*random access memory*
RF	*Radio Frequency*
RNG	*random number generation*
ROM	*read only memory*
SAR	*Security Assurance Requirements*

SCA	*Signature creation application*
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*
SGF	*Système de gestion de fichiers*
SM	*Secure Messaging*
TOE	*Target of evaluation*
TSF	*TOE security functionality*
VAD	*Verification authentication data*

2.3 Associated references

Reference	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]	Composite product evaluation for smart cards and similar devices, Version 1.5, October 2017.
[PP-SSCD2]	Protection profiles for secure signature creation device — Part 2: Device with key Generation, BSI-CC-PP-0059-2009-MA-01, Version 2.0.1, 23/01/2012.
[PP-SSCD3]	Protection profiles for secure signature creation device — Part 3: Device with key Import, BSI-CC-PP-0075-2012, Version 1.0.2, 27/09/2012.
[PP-SSCD4]	Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, BSI-CC-PP-0071-2012, Version 1.0.1, 12/12/2012.

[PP-SSCD5]	Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, BSI-CC-PP-0072-2012, Version 1.0.1, 12/12/2012.
[PP-SSCD6]	Protection profiles for secure signature creation device — Part 3: Extention for Device with key Import and trusted communication with signature creation application, BSI-CC-PP-0076-2013, Version 1.04, 16/04/2013.
[PP-PL]	Java Card™ System Protection Profile "Open Configuration" Version 3.0, May 2012
[ST-PL]	Security Target Lite of IDealCitiz v2.16I on Infineon M7892 B11 – Java Card Open Platform, réf. 2017_2000030456, v1.2, 6 octobre 2017, IDEMIA.
[CR-PL]	Rapport de certification ANSSI-CC-2017/74 - IDeal Citiz v2.16-i on M7892 B11 - Java Card Open Platform. 08-01-2018. ANSSI
[PP-IC]	Security IC platform protection profile, version 1.0, 15th June 2007. Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035.
[ST-IC]	Infineon, Security Target Lite, M7892 B11, Recertification, Including optional Software Libraries RSA - EC - SHA- 2 - Toolbox, Common Criteria CC v3.1 EAL6 augmented (EAL6+), version 2.6, 2017-08-02.
[CR-IC]	Certification Report BSI-DSZ-CC-0782-V3-2017 for Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware), 5 septembre 2017, BSI.
[IAS-PRE]	Identification Authentication Signature (IAS) Premium Technical Specifications Revision: 1.0.1, October 2006
[FSP]	Specification de l'application VITALE: 2017_2000024577 - Spécifications techniques - Spécification fonctionnelle ADELE 2017_2000024578 - Spécifications techniques - Spécification fonctionnelle VITALE 2017_2000024579 - Spécifications techniques - Spécification fonctionnelle AIP 2017_2000024580 - Spécifications techniques - Spécification fonctionnelle GA 2017_2000024581 - Spécifications techniques - Spécification fonctionnelle Card Manager 2017_2000024780 - Spécifications techniques - Spécification produit carte VITALE2 Infineon
[DIR]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.
[JC]	Java Card Platform, versions 3.0.1, Classic Edition, including Specification Errata, October 2010, Updated February 2011. Published by Oracle: - Virtual Machine Specification - Application Programming Interface - Runtime Environment Specification
[AIS31]	BSI - Functionality classes and evaluation methodology for physical random number generators AIS31, Version 3, 2013-05-15

3 TOE Overview

3.1 TOE Presentaion

The TOE is an integrated circuit chip embedding

- An Operating system providing:
  - Java Card interfaces, as specified in [JC]
  - Extended interfaces for targeted applications needs
- VITALE application compliant with [FSP]

3.2 TOE Type

The TOE is a SSCD Application based on Java Card. It is designed to be fully compliant with the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a community framework for electronic signature [DIR]. It provides SSCD services containing data needed for generating electronic signatures on behalf of the Card Holder as well as for user authentication; this application is intended to be used in the context of official and commercial services, where an electronic signature of the Card Holder is required: to be certified according to [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6].

The TOE comprises of:

- The Infineon M7892 B11 integrated circuit [ST-IC],
- The IDeal Citiz™ v2.16-i Java Card platform,
- VITALE2, VITALE1 and ADELE containing the SSCD functionality and,
- The associated guidance documentation [AGD_OPE], [AGD_PRE].

The following Figure describes the architecture of the card and highlights the components of the card that are part of the TOE.

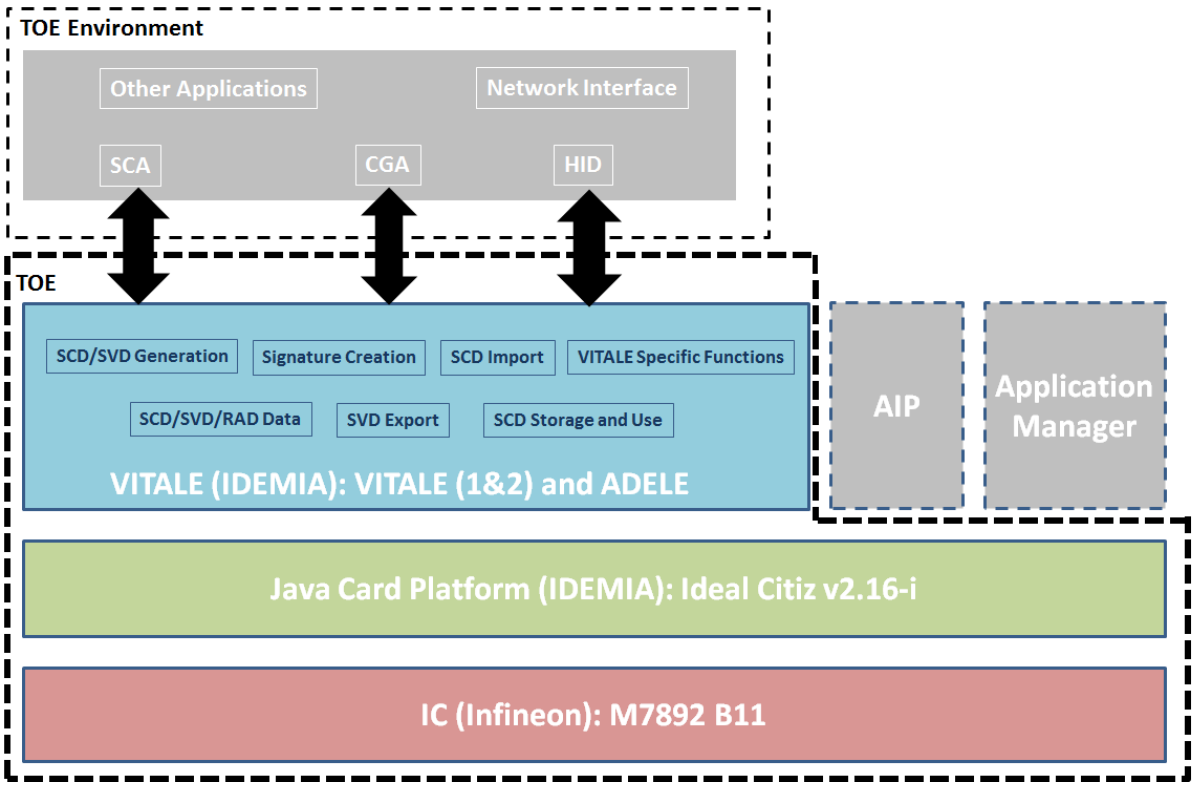

Figure 2: TOE physical scope

3.3 TOE Description

This section provides a quick overview of the components of the card. Note that the AIP component, Application Manager component, the whole Java Card Platform Layer and the IC provide functionalities to all the applicative VITALE components (VITALE2, VITALE1 and ADELE).

3.3.1 Integrated Circuit M7892 B11

More information on the chip is given in the related certification report [CR-IC] and related Security Target [ST-IC].

The IC implements security features able to ensure:

- The confidentiality and the integrity of information processed and flowing through the Card and the terminal,
- The resistance of the secure IC to externals attacks such as physical tampering, environmental stress or any other attacks that could compromise the sensitive assets stored or flowing through it.
- Secure low-level cryptographic processing
- Access to low-level functionality is done only via APIs (incl. integrity/confidentiality of private data/code)
- TOE protection: does not allow any native code or application to be bypassed or altered
- Secure operation: supports the needs for any modification to a single persistent object or class field to be atomic and provides low level transaction concurrency control.

- Memory management provides:
  - storage in persistent or volatile memory, depending on the needs.
  - low-level control accesses (segmentation fault detection)
  - a mean to perform memory operations atomically.

3.3.2 Java Card Platform IDeal Citiz v2.16-i

More information on the Java Card Platform is given in the related certification report [CR-PL] and related Security Target [ST-PL].

The JC Platform layer is responsible for:

- Providing an interface to all Applications that ensures that the Runtime Environment security mechanisms cannot be bypassed, desactivated, corrupted or otherwise circumvented;
- Performing secure memory management to ensure that:
  - Each Application's code and data (including transient session data) as well as the Runtime Environment itself and its data (including transient session data) is protected from unauthorized access from within the card. The Runtime Environment provides isolation between Security Domains via an Application Firewall.
  - When more than one logical channel is supported, each concurrently selected Application's code and data (including transient session data) as well as the Runtime Environment itself and its data (including transient session data) is protected from unauthorized access from within the card; The previous contents of the memory is not accessible when that memory is reused;
  - The memory recovery process is secure and consistent in case of a loss of power or withdrawal of the card from the card reader while an operation is in progress;
- Providing communication services with off-card entities that ensures the proper transmission (according to the specific communication protocol rules) of unaltered command and response messages
- Providing applications with cryptographic means to protect their communications.

3.3.3 Application Layer

3.3.3.1 ADELE

ADELE application is a part of VITALE. It is a complete set of commands used for SSCD that are conforms to [FSP_ADELE]. This application is evaluated like VITALE2 as they provide the same list of security functions. See section 3.6 for details about the services provided by this Application.

3.3.3.2 VITALE1

VITALE card supports the VITALE1 commands ([FSP_VITALE]) for an ascendant compatibility. VITALE1 data are stored in a binary file. These commands are maintained essentially so that VITALE2 could generate VITALE1 certificate. VITALE1 performs the following functionality:

- Read
  - This command is used to access to data in VITALE1 file.
- Read Result

- This function is used in order to
  - obtain the size of the binairy file VITALE1
  - obtain the algorithm used by the CERTIFICATION function of the signature service (based on TDES)
  - retrieve other application parameters.

- Seal Calculation (**MAC Retail** TDES)
  - This function manages the sealing of data and computes the symmetric signature VITALE1 (**MAC Retail**). These data are needed for the authentication done by the terminal. The proof is represented by a certificate, calculated from a TDES key.

3.3.3.3 VITALE2

The VITALE2 application is a complete set of commands used for SSCD that are conforms to [FSP_VITALE]. This includes the management of the RAD and the signature keys, the signing operation and the user authentication. The access to the services depends on the user role, VITALE 2 card status and application status that perform the service. See section 3.6 for more details about the services provided by this Application.

The VITALE2 application includes the following specific functions:

Block card
This function enables to block the card.

Protection mode modification
Three protection modes are defined. These modes define the access rules to the VITALE files. This function enables to select a mode protection for VITALE 2 data.

Seal calculation
This function enables the data sealing with two keys, base on the algorithm TDES and AES.

Data ciphering
This function enables the data confidentiality, using TDES and AES keys.

Symmetric internal authentication
This function enables the calculation of an authentication cryptogram from a TDES and AES key.

3.3.4 Application Data

3.3.4.1 Specific Data for VITALE

All data objects SGF (EF, DF and ADF) and SDO are described in chapters 4 & 5 from [FSP_ADELE] and [FSP_VITALE].

Data for VITALE are the following:

- The set of data defined in the framework of the VITALE1, VITALE2 and ADELE

- Directories and Files
- Objects

- The set of data represented by cryptographic keys, PIN/PUK codes and security environments SE associated to VITALE1, VITALE2 and ADELE services such as electronic signature, certificate calculation/verification, authentication mechanisms, etc. (see chapter 3.6 for more information).
- The set of data defined in the framework of the VITALE 1 card operation and linked to the insurer (the embedder) and entitled persons related to him ("ayants droits" in French, e.g. children of the card holder).
- The set of data defined in the framework of VITALE 2 card, and linked to the set of VITALE 2 data.
- The set of data specific to the electronic signature services within the context of VITALE.
- The set of data represented by cryptographic keys associated to VITALE 1 and 2 services and electronic signature, and the PIN code associated to these services to authenticate the bearer.

3.3.4.2 Shared Data between VITALE2 and ADELE

Data shared by VITALE2 and ADELE applications are the following:

- The set of data related to the identification of the holder
- "Card" certificates
- PIN code and associated PUK code that are defined for these two appli-cations
- Private authentication key and associated DH parameters
- Data linked to card physical support, such as serial number

3.3.5 Required non-TOE hardware/software/firmware

As shown in Figure 2, the AIP component is outside the scope of evaluation. The AIP is a complete set of commands described in [FSP_AIP] and used to personalize VITALE applications. This application is desactivated in "user" phase. It provides:

- Applications instances creation of VITALE2, VITALE1 and ADELE
- Personalization of those applications
- Loading of personalization data

Figure 2 shows also that other elements such as Signature Creation Application (SCA), Certificate Generation Application (CGA), Human Interface Device (HID) are considered as part of the environment of the TOE and are outside the scope of evaluation. Futrther details are given in Section 3.5 that presents a functional overview of the TOE in its distinct operational environments (the signing environment, the management environment and the preparation environment).

3.4 TOE Functions

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

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

The TOE provides the following functions:

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

The TOE is prepared for the signatory's use by

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

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

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

If 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 information, if any exists.

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

As shown in Figure 3 through Figure 7, the signing environment, the management environment and the preparation environment are secured and protect data exchanged with the TOE. The protection of data exchanged with the TOE is realized by a trusted communication.

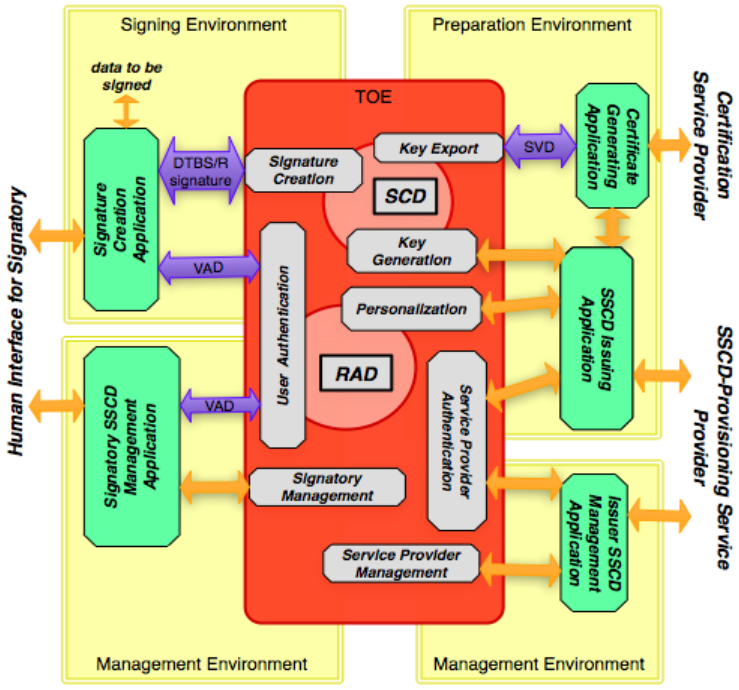

Figure 3: TOE and Operational environments with Key Generation

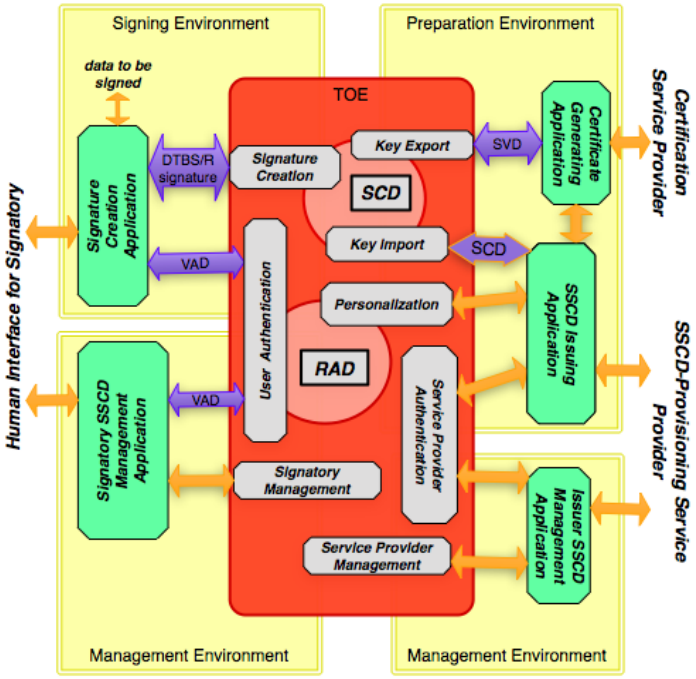

Figure 4: TOE and Operational environments with Key Import

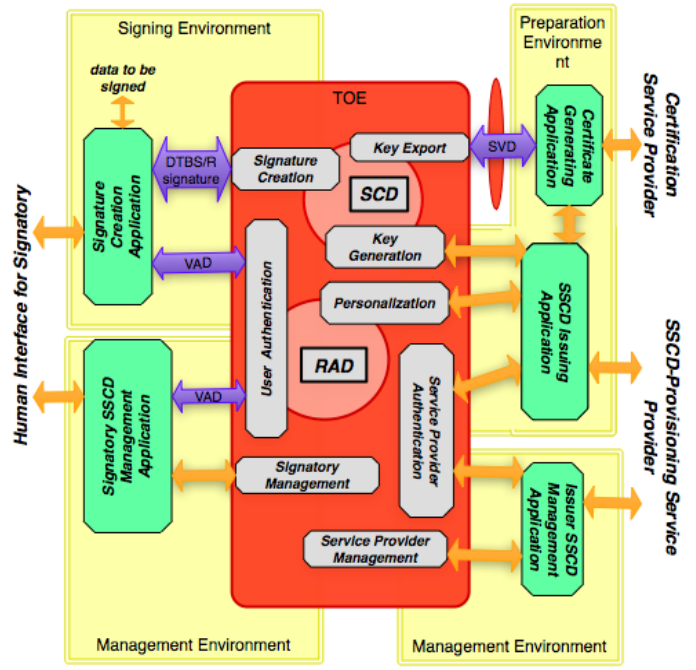

Figure 5: TOE and Operational environments with Key Generation and trusted channel to CGA

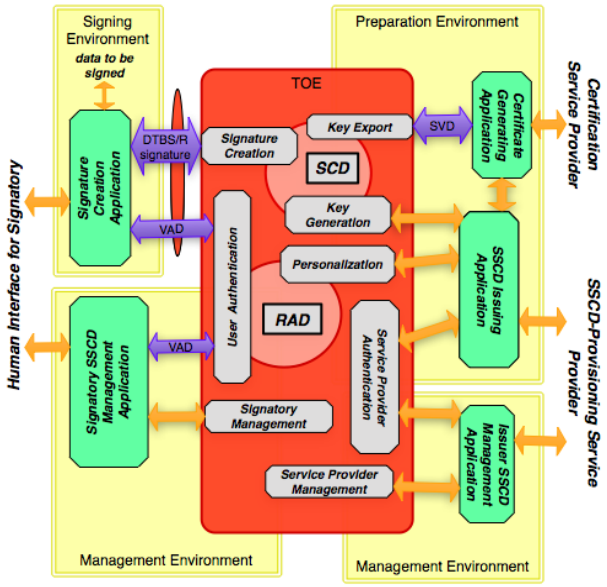

Figure 6: TOE and Operational environments with Key Generation and trusted channel to SCA

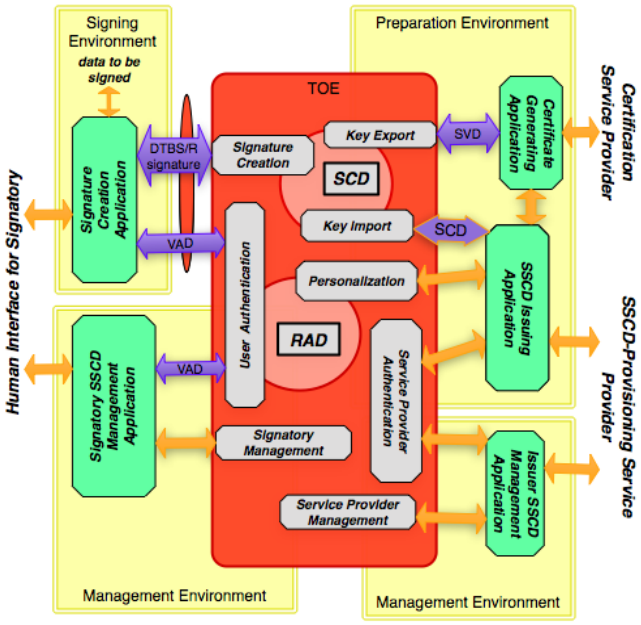

Figure 7: TOE and Operational environments with Key Import and trusted channel to SCA

The TOE stores signature creation data (SCD) and reference authentication data (RAD). The TOE may store multiple instances of SCD. In this case the TOE shall provide a function to identify each SCD and the SCA can provide an interface to the signer to select an SCD for use in the signature creation function of the SSCD. The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. The digital signature created by the TOE is a qualified electronic signature as defined in Article 5.1 of

the directive [DIR]. Determining the state of the certificate as qualified is beyond the scope of this standard.

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

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

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

The TOE is a SSCD 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 PIN initiates the digital signature creation function of the smart card through the terminal.

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

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

I. by the TOE itself or
II. by a trusted human interface device connected via a trusted channel with the TOE.

The HI is considered as part of the environment of the TOE. This device is used for the input of VAD for authentication by knowledge. The TOE holds RAD to check the provided VAD.

3.6 Major security features of the TOE

The TOE provides the following TOE security features:

3.6.1 Authentication mechanisms

This feature provides functions to authenticate different roles:

- Authenticate the cardholder based on a RAD verification (by PIN) or PUK code. It is called 'User Authentication'. See [IAS-PRE] section 8.1.
- Authenticate the device communicating with the card, to establish a trusted channel (secure messaging) and protect the communication. It is called 'Mutual Device authentication'. It may use symmetric or asymmetric scheme. See [IAS-PRE] section 8.2. It includes:
    - « Symmetric Authentication scheme » (see [ESIGN K 1] section 8.7 and [IAS-PRE] section 8.2.2)
    - « Device authentication with privacy protection » (see [ESIGN K 1] section 8.5 and [IAS-PRE] section 8.2.3)
- Authenticate the Administrator of the TOE that may have some administration rights (on the TOE, personalization rights, on the SCD management…) using either symmetric (see [IAS-PRE] section 8.3.1) and/or asymmetric (see [IAS-PRE] section 8.3.2) mechanisms or PIN verification. It is called 'Role authentication'. The Administrator is entitled to identify the TOE.
- Perform mutual authentication of external remote entities such as the SCA and CGA and initiate a trusted channel with them using either symmetric (see [IAS-PRE] section 8.3.1) and/or asymmetric (see [IAS-PRE] section 8.3.2) mechanisms.
- Perform internal Client/Server authentication (e-Services), encryption key decipherment and certificate verification. See [IAS-PRE] section 8.4.
    - Client/Server authentication: this feature enables to authenticate the TOE on behalf of the cardholder's PC to a remote web server.
    - Encryption key decipherment: this feature enables the cardholder to store secret data on an electronic vault. The key needed to decipher the key encrypting these data is securely stored in the TOE. The cardholder's PC sends the encrypted encryption key to the TOE to get the plain encryption key.
    - Certificate verification: this feature enables the TOE to verify a certificate issued by a certification authority the TOE trusts. The trust is established by the transfer to the TOE of a public RSA key of an authority certified by an authority whose public key is present in the TOE (either permanently stored, either imported through a certificate). This feature is used when the authentication key of a remote entity is certified by a Root certification Authority (RCA).
- Internal Asymmetric Authentication of the card (See [IAS-PRE] section 8.5).
- Ensure that only authenticated terminals can get access to the user data stored on the TOE.

3.6.2 Cryptographic

This feature performs the following cryptographic operations (see FCS_COP.1 for more setails about crypto algos, key sizes and standards):

- SCD/SVD key generation based on RSA
- Session keys generation for secure messaging based on TDES or AES
- Key Destruction by overwriting with zero
- Asymmetric authentication (Role, Device, C/S and DAPP) based on RSA
- Symmetric authentication (Role and Device) based on TDES or AES
- Signature Creation based on RSA
- Random Number Generation that meets Class PTG.2 according to [AIS31]
- Encryption and decryption of the transmitted message based on TDES or AES
- MAC generation and verification for secure messaging.
- DH key agreement.
- Secure hash computation
- Certificate calculation and verification
- Ciphering Key Decryption
- Data Ciphering/Deciphering

The implementation of these cryptographic operations is mainly based on the Security Functionalities provided by the Platform.

3.6.3 Key Management

This feature provides functions to:

- Import and Install an SCD, generated outside the TOE in a trusted environment and communicated through a secure channel link
- Generate an SCD
- Disabling an SCD it holds
- Create, extend or modify certificate info stored in the TOE
- Create SVD for an SCD stored and export it for certification by a certificate generating application protected by trusted channel
- Manage the authentication keys stored in the TOE
- Handle cryptographic data objects dedicated to store the keys, DH parameters and the security environments, as well as their attributes.

3.6.4 PIN Management

Management of the PIN. The TOE enables to create, set, change, and reset the PIN through APDU commands as well as retrieve the remaining tries counter.

3.6.5 Trusted Channels

This feature realizes a secure communication channel to verify authenticity and integrity as well as securing confidentiality of user data between the TOE and other devices connected. The TOE provides a trusted, cryptographically protected communication with external applications as CGA and SCA, Device and external roles.

This feature si based on TDES or AES to generate session keys for secure messaging

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

The feature includes functions for management of the cryptographic keys, parameters and configuration used to establish the trusted communication. See section 9.1 from [IAS-PRE] for more details.

3.6.6 Access Control

This feature manages the access to objects (files, directories, data, secrets, PIN, Keys , SDOs, …) stored in VITALE file system. It ensures secure management of secrets such as cryptographic keys. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification. This function ensures that it is not possible to bypass the access controls. The access condition is granted if the security conditions are fulfilled. Any access condition to fulfill is a combination of security conditions based on identified Keys/PIN/Secrets:

- User Authentication by PIN (RAD). It may be used to authenticate the end user or an administrator
- Authentication of a remote administrator by symmetric or asymmetric mechanisms
- Mutual authentication with a remote IT device (SCA or CGA)
- Communication protected in integrity and confidentiality

3.6.7 Data Storage

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

3.6.8 Integrity

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

3.6.9 Confidentiality

This feature ensures the confidentiality of sensitive user data and secrets by providing secret asymmetric deciphering and symmetric data ciphering services.

3.6.10 Features from the Platform

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

- Protection against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.
- Protection against tampering and the stored assets can not be retrieved or altered by physical manipulation
- Protection against physical attack and perform self tests as described in [ST-PL].
- Security domains are supported by the Java Card platform.
- Cryptographic operations (see section 3.6.2): Signature Key Generation, Random Number Generation, signature creation, secure messaging, Symmetric and Asymmetric Encryption/Decryption, Hash calculation, MAC and key exchange, etc.

4 Life Cycle

4.1 SSCD Product Life Cycle

The TOE life cycle in Figure 7 distinguishes stages for development, production, preparation and operational use. The development and production of the TOE (cf. CC part 1 [CC1], para.139) together constitute the development phase of the TOE.

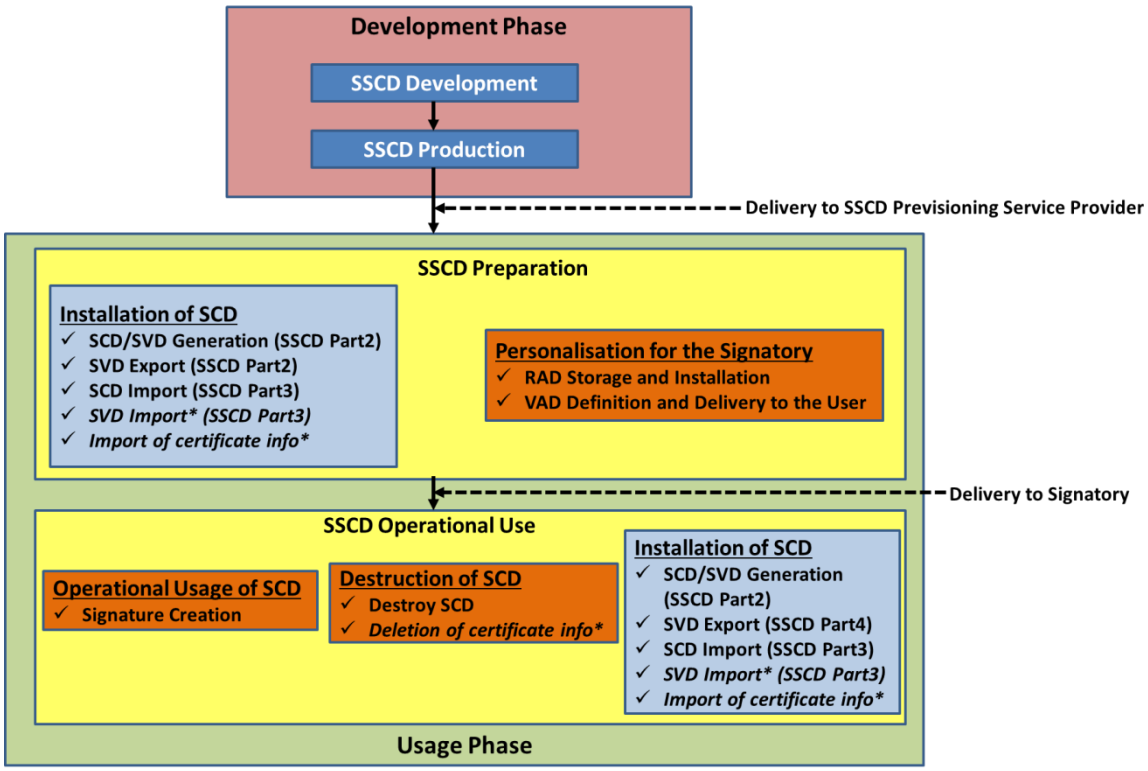

Figure 8: SSCD Product Life Cycle

The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class. The development phase ends with the delivery of the TOE to an SSCD-provisioning service provider. The functional integrity of the TOE shall be protected in delivering it to an SSCD-provisioning service provider.

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

4.1.1 SSCD Preparation phase

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

During preparation of the TOE, as specified above, an SSCD-provisioning service provider performs the following tasks:

1) Obtains information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user of the TOE.
2) Generates a PIN of the legitimate user, stores this data as RAD in the TOE and prepares information about the VAD for delivery to the legitimate user.
3) *SSCD Part 3 only:* The initialization of the TOE, i.e. the CSP generates the SCD/SVD pair by means of a SCD/SVD generation device, loads the SCD to the TOE, and sends the SVD to the CGA. The TOE may import and store the SCD/SVD pair.
4) *SSCD Part 2 only:* The generation of an SCD/SVD pair by the TOE
5) Generates a (qualified) certificate for the SVD
6) Optionally, presents certificate info to the SSCD.
7) Delivers the TOE and the accompanying VAD info to the legitimate user.

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

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

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

4.1.2 SSCD Operational Use phase

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

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

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

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

The lifecycle may allow import of SCDs (*SSCD Part 3*) or generation of SCD/SVD key pairs (*SSCD Part 2*) after delivery to the signatory as well.

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

4.2 TOE Life Cycle

The TOE life cycle is shown in Figure 8. It is described in terms of the following four life cycle phases and seven stages.

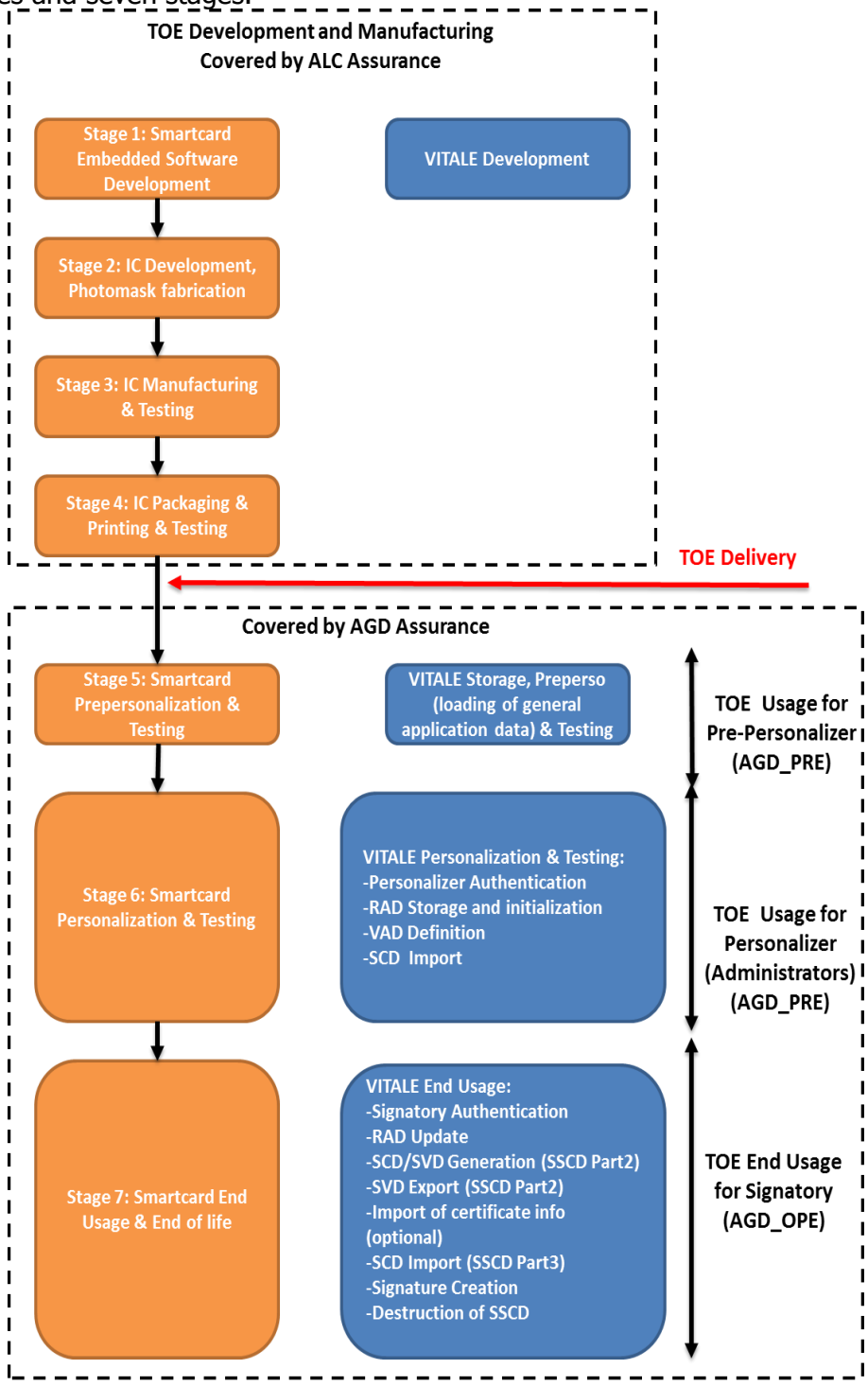

Figure 9: TOE Life Cycle

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

The development environment encompasses the environment in which the TOE is developed, i.e.

- IDeal Citiz v2.16-i Java Card Platform components
- VITALE: VITALE2, VITALE1, ADELE Applications and interfaces

This phase is composed of two stages:

- Stage 1: Embedded software development
- Stage 2: IC development

The IC Developer (Infineon):

- Designs the IC, develops the IC dedicated software and provides information, software or tools to the Embedded software developer (IDEMIA).
- Receives the Embedded software from the developer, through trusted delivery and verification procedures.
- Builds the database of the IC required to construct the photomask.

The Embedded Software Developer (IDEMIA) is in charge of:

- Specification, development and validation of the software (IDeal Citiz™ v2.16-i Java Card Platform & VITALE and development of the guidance documentation associated with these TOE components.
- Use of the guidance documentation for the IC.

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

The confidentiality and integrity of the cap files and of the IDeal Citiz™ v2.16-i Platform is covered by the ALC evaluation of the development premises of IDEMIA.

At the end of Stage 1, VITALE and IDeal Citiz™ v2.16-i Platform are transferred to the chip manufacturer in order to be loaded into the Flash.

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

Stage	Role	Actor	Site	Covered by
1	Embedded Software Developer	IDEMIA R&D	Osny and Meyreuil - France	ALC
2	IC Developer	Infineon	Infineon development site(s) mentioned in [CR-IC]	ALC

4.2.2 Production phase (Stages 3 & 4 of the IC life cycle [PP-IC])

In this phase, the embedded software (IDeal Citiz™ and VITALE) is loaded into the flash memory.

This phase is composed of two stages:

- Stage 3: IC manufacturing and testing

- Stage 4: IC Packaging

The IC Manufacturer is responsible for producing the IC through five main steps:
- IC manufacturing,
- Load of VITALE in the non-volatile programmable memories (for instance FLASH),
- IC testing,
- Add initialization data in FLASH and keys,
- Write the IC Identification Data onto the chip to control the IC as SSCD during the IC manufacturing and the delivery process to the Pre-personalizer.

The IC Packaging Manufacturer is responsible for:
- Combine the IC with hardware for the contact based / contactless interface,
- IC packaging and testing.

The TOE is protected during transfer between various parties.

The point of delivery is the end of Stage 4.

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

Stage	Role	Actor	Site	Covered by
3	IC Manufacturer	Infineon	Infineon production site(s) mentioned in [CR-IC]	ALC
4	IC Packaging Manufacturer	Infineon	Infineon production site(s) mentioned in [CR-IC]	ALC
TOE Delivery Point				

4.2.3 Preparation phase (Stages 5 & 6 of the IC life cycle [PP-IC])

This phase is composed of two stages:
- Stage 5: Smartcard Pre-personalization & Testing
- Stage 6: Smartcard Personalization & Testing

The Pre-personalizer is responsible for:
- Initializing of the VITALE File System
- Equipping VITALE with pre-personalization Data and the personalization key set via AIP

The pre-personalized Card is securely delivered from the Pre-personalizer to the Personalizer.

This phase consists of:
a) Finishing process of the product (Composite product integration)
b) Personalization: RAD storage and VAD delivery processes
   - The Personalizer authenticates himself to the TOE
   - The Personalizer imports the RAD to the TOE
   - The VAD is securely delivered to the Signatory
c) SCD initialization by SCD Import

- The Personalizer authenticates himself to the TOE
- The Personalizer requests the generation of a SCD/SVD key pair on the CSP
- The SCD is imported to the TOE
- The SVD is exported to the CGA by the CSP
- The CGA generates the certificate
- Optionally, the certificate is imported into the TOE

d) Create the security policies to be applied to files and objects

During this phase, the Application is pre-personalized and personalized according to AGD_PRE.

At the end of Stage 6, the TOE is constructed.

In this phase, the AIP application is activated by default (ADF automatic creation) and automatically desactivated at the end of Stage 6 (during the transition to the User phase Stage 7).

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

Stage	Role	Actor	Site	Covered by
5	Pre-Personalizer	Pre-Personalization Agent offcard	The agent who pre-personalizes the SSCD for the holder	AGD_PRE
6	Personalizer (Administrator)	Personalization Agent offcard	The agent who personalizes the SSCD for the holder	AGD_PRE

4.2.4 Operational phase (Stage 7 of the IC life cycle [PP-IC])

In this phase, the TOE is operational and used as a signing document by the end user to sign transactions.

The TOE is under the control of the Signatory and/or the Administrator

This phase is composed of one stage:

- Stage 7: Smartcard End Usage

This phase consists of:

a) Update RAD and the delivery of the VAD to the Signatory
b) SCD/SVD key pair generation
   - The Signatory use his PIN (VAD) code to authenticate himself to the TOE
   - The Signatory requests the generation of a SCD/SVD key pair on the TOE
   - The SVD is exported to the CGA
   - The CGA generates the certificate
   - Optionally, the certificate is imported into the TOE
c) SCD Import
   - The Signatory use his PIN (VAD) code to authenticate himself to the TOE
   - The Signatory requests the generation of a SCD/SVD key pair on the CSP

- The SCD is imported to the TOE
- The SVD is exported to the CGA by the CSP
- The CGA generates the certificate
- Optionally, the certificate is imported into the TOE

d) Signature Creation by the TOE
- The Signatory use his PIN (VAD) code to authenticate himself to the TOE
- The Signatory sends the DTBS representation to the TOE
- The TOE computes the signature
- The TOE sends the signature to the SCA

In this stage, the TOE could be used in the following mode of operation:
- VITALE1 and VITALE2 mode (bi-mode)
- VITALE2 mode
- ADELE mode

The AIP in this phase is desactivated.

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

Stage	**Role**	**Actor**	**Site**	**Covered by**
7	Signatory or Administrator	Signatory or Administrator	N/A	AGD_OPE

5 Conformance Claims

5.1 CC Conformance

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

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 [CC1].
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [CC2].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, CCMB-2017-04-003, Version 3.1, Revision 5, April 2017 [CC3].
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017 [CEM].

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

- Part 1: conformant
- Part 2: extended with
  - FPT_EMS.1 TOE Emanation
  - FIA_API.1 Authentication proof of identity

  All the other security requirements have been drawn from the catalogue of requirements in [CC2].
- Part 3: EAL4 augmented with
  - ALC_DVS.2 (Sufficiency of security measures)
  - AVA_VAN.5 (Advanced methodical vulnerability analysis)

The TOE also includes:

- Integrated Circuit IC: Chips Infineon M7892 B11 [ST-IC]. The IC ST claims strict conformance to the security IC platform PP [PP-IC]. The assets, threats, objectives, SFR and security functions specific to the chips M7892 B11 are described in [ST-IC] and are not repeated in the current ST.
- Java Card Platform: IDeal Citiz™ v2.16-i [ST-PL]. The PL ST claims strict conformance to the security JC platform PP [PP-PL]. The assets, threats, objectives, SFR and security functions specific to the Platform are described in [ST-PL] and are not repeated in the current ST.

5.2 PP Claims

This security target is strict compliant with the following PPs:

- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation" [PP-SSCD2].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 3: Device with key Import" [PP-SSCD3].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 4: Extention for Device with key generation and Trusted Communication with CGA" [PP-SSCD4].

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

5.3 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. A detailed justification is given in the following:

1) There are two additional assets D.VAD, D.RAD and D.SECRET comparing to SSCD Protections Profiles
2) The SPD of this ST contains the security problem definition of PPs [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6]. The SPD for this ST is described by the same threats, organisational security policies and assumptions as for the TOE in PPs. This ST adds A.SEC_PERSO (Protection during Pre-Personalisation & Personalisation).

3) 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 objective OT.TOE_SSCD_Auth (Authentication proof as SSCD) and OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export) from the [PP-SSCD4].
   b. the security objective OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import) and OT.TOE_TC_DTBS_Imp (Trusted channel for DTBS) from PPs [PP-SSCD5] and [PP-SSCD6].

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

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 CGA from [PP-SSCD4]: FTP_ITC.1/SVD, FDP_DAU.2/SVD, FIA_API.1
   b. 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.

6) This ST provides refinements for the SFR FIA_UAU.1 of the core PPs [PP-SSCD2] and [PP-SSCD3] according to [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6].

7) The security assurance requirements (SARs) are originally taken from SARs of CC 3.1 Part 3 [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 CC part 3 [CC3] and to the CEM [CEM]. This document specifies the additional information to be provided by a developer, and the additional checks to be performed by the ITSEF (Information Technology Security Evaluation Facility) when performing a "composite evaluation".

This security target is compliant with the SPD of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6] as shown in the following table. Additional elements are highlighted in red.

TOE SPDs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
Assets						
D.SCD	×	×	×	×	×	×
D.SVD	×	×	×	×	×	×
D.DTBS/R	×	×	×	×	×	×
D.VAD						×
D.RAD						×
D.SECRET						×
Assumptions						
A.CGA	×	×	×	×	×	×
A.SCA	×	×	×	×	×	×
A.CSP		×			×	×
A.SEC_PERSO						×
Threats						

T.SCD_Divulg	×	×	×	×	×	×
T.SCD_Derive	×	×	×	×	×	×
T.Hack_Phys	×	×	×	×	×	×
T.SVD_Forgery	×	×	×	×	×	×
T.SigF_Misuse	×	×	×	×	×	×
T.DTBS_Forgery	×	×	×	×	×	×
T.Sig_Forgery	×	×	×	×	×	×
Organisational Security Policies						
P.CSP_QCert	×	×	×	×	×	×
P.QSign	×	×	×	×	×	×
P.Sigy_SSCD	×	×	×	×	×	×
P.Sig_Non-Repud	×	×	×	×	×	×

Table 1 PP SPDs vs. ST

This security target is compliant with the security objectives of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6] as shown in the following table. Additional elements are highlighted in red.

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

OE.Signatory	×	×	×	×	×	×
OE.DTBS_Intend	×	×	×	×	×	×
OE.SVD_Auth	×	×	×	×	×	×
OE.CGA_QCert	×	×	×	×	×	×
OE.DTBS_Protect	×	×	×			×
OE.HID_VAD	×	×	×			×
OE.SSCD_Prov_Service	×	×		×	×	×
OE.SCD_SVD_Corresp		×			×	×
OE.SCD_Unique		×			×	×
OE.SCD_Secrecy		×			×	×
OE.SCD/SVD_Auth_Gen		×			×	×
OE.Dev_Prov_Service			×			×
OE.CGA_TC_SVD_Imp			×			×
OE.CGA_SSCD_Auth			×			×
OE.HID_TC_VAD_Exp				×	×	×
OE.SCA_TC_DTBS_Exp				×	×	×
OE.SEC_PERSO						×

Table 2 PP Security Objectives vs. ST

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

TOE SFRs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
FPT_EMS.1	×	×	×	×	×	×
FPT_FLS.1	×	×	×	×	×	×
FPT_PHP.1	×	×	×	×	×	×
FPT_PHP.3	×	×	×	×	×	×
FPT_TST.1	×	×	×	×	×	×
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_SDI.2/DTBS	×	×	×	×	×	×
FDP_SDI.2/Persistent	×	×	×	×	×	×
FDP_RIP.1	×	×	×	×	×	×
FDP_ACC.1/Signature_Creation	×	×	×	×	×	×
FDP_ACF.1/Signature_Creation	×	×	×	×	×	×
FCS_COP.1	×	×	×	×	×	×
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	×		×	×		×
FTP_ITC.1/SCD		×			×	×
FDP_UCT.1/SCD		×			×	×
FDP_ITC.1/SCD		×			×	×
FDP_ACC.1/SCD_Import		×			×	×
FDP_ACF.1/SCD_Import		×			×	×
FTP_ITC.1/SVD			×			×
FDP_DAU.2/SVD			×			×
FIA_API.1			×			×
FDP_UIT.1/DTBS				×	×	×
FTP_ITC.1/VAD				×	×	×
FTP_ITC.1/DTBS				×	×	×

Table 3 PP SFRs vs. ST

6 Security Problem Definition

6.1 Assets

6.1.1 From PPs

D.SCD

Signature Creation Data

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

D.SVD

Signature Verification Data

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

D.DTBS/R

Data to be signed or its unique Representation

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

6.1.2 Additional Assets

D.VAD

PIN code entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed are required).

D.RAD

Reference PIN code used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained).

D.SECRET

This Asset covers the following sensitive data:

- Cryptographic keys Symmetric (AES and TDES) or Asymmetric (DH, RSA) used for the authentication mechanisms and the generation of session keys. The confidentiality, integrity of these keys must be maintained.
- Security Environment SE. The integrity of these SE must be maintained.

6.2 Users / Subjects

6.2.1 Threat agents

S.Attacker

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

6.2.2 Miscellaneous

S.User

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

S.Admin

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

S.Signatory

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

6.3 Threats

T.SCD_Divulg

Storing, copying and releasing of the signature creation data

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

T.SCD_Derive

Derive the signature creation data

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

T.Hack_Phys

Physical attacks through the TOE interfaces

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

T.SVD_Forgery

Forgery of the signature verification data

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

T.SigF_Misuse

Misuse of the signature creation function of the TOE

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

T.DTBS_Forgery

Forgery of the DTBS/R

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

T.Sig_Forgery

Forgery of the electronic signature

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

6.4 Organisational Security Policies

P.CSP_QCert

Qualified certificate

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. the directive, article 2, clause 9, and Annex I [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.

6.5 Assumptions

6.5.1 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.

6.5.2 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.

6.5.3 Additional Assumption

Appropriate 'Protection during Pre-Personalisation & Personalisation (A.SEC_PERSO)' must be ensured after TOE Delivery up to the end of Stage 6 as specified below.

A.SEC_PERSO

Protection during Pre-Personalisation & Personalisation

It is assumed that security procedures are used after delivery of the TOE up to Stage 6 to maintain confidentiality and integrity of the TOE and of its data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Stages 5 & 6 after TOE Delivery are assumed to be protected appropriately.

7 Security Objectives

7.1 Security Objectives for the TOE

7.1.1 All SSCD parts

OT.Tamper_Resistance

Tamper resistance

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

OT.Tamper_ID

Tamper detection

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

OT.EMSEC_Design

Provide physical emanations security

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

OT.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.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.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.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.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.

7.1.2 SSCD parts 2, 4 and 5 only

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.

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_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.

7.1.3 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.

7.1.4 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.

7.1.5 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.

7.2 Security Objectives for the Operational Environment

7.2.1 All SSCD parts

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.

OE.DTBS_Intend

SCA sends data intended to be signed

The signatory shall use a trustworthy SCA that

- o 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,
- o sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
- o 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.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)

- o the name of the signatory controlling the TOE,
- o the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
- o 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.

7.2.2 SSCD parts 3 and 6 only

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.

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_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/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.

7.2.3 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.

7.2.4 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.

7.2.5 Additional OE

Appropriate 'Protection during Pre-Personalisation & Personalisation (OE.SEC_PERSO)' must be ensured after TOE Delivery up to the end of Stage 6 as specified below.

OE.SEC_PERSO

Protection during Pre-Personalisation & Personalisation

Stages after TOE Delivery up to the end of Stage 6 must be protected appropriately to maintain confidentiality and integrity of the TOE and of its data (to prevent any possible copy, modification, retention, theft or unauthorised use).

Application Note:

The Pre-personalizer and the Personalizer have to use adequate measures to fulfil OE.SEC_PERSO for instance by using appropriate authentication mechanisms for pre-personalization and personalisation functions during Stage 5 and Stage 6.

7.3 Security Objectives Rationale

7.3.1 Threats

T.SCD_Divulg addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in 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_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 [DIR]. 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. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. 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. 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.

7.3.2 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:

- 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;
- 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;
- OT.SCD_Unique, 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;

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

OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised TOE from an SSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD In the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA_SSCD_Auth and the received SVD is sent by this SSCD as required by OE.CGA_TC_SVD_Imp. Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

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

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 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.

7.3.3 Assumptions

7.3.3.1 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.

7.3.3.2 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).

7.3.3.3 Additional Assumption

A.SEC_PERSO Since OE.SEC_PERSO requires the Pre-personalizer and the Personalizer to use adequate measures assumed in A.SEC_PERSO, the assumption is covered by this objective.

7.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.SCD_Divulg	OT.SCD_Secrecy, OT.SCD_Auth_Imp, OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy	Section 7.3.1
T.SCD_Derive	OT.SCD/SVD_Gen, OT.Sig_Secure, OE.SCD_Unique	Section 7.3.1
T.Hack_Phys	OT.SCD_Secrecy, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance	Section 7.3.1
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 7.3.1

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	Section 7.3.1
T.DTBS_Forgery	OT.DTBS_Integrity_TOE, OE.DTBS_Intend, OT.TOE_TC_DTBS_Imp, OE.SCA_TC_DTBS_Exp	Section 7.3.1
T.Sig_Forgery	OT.SCD_Unique, OT.Sig_Secure, OE.CGA_QCert, OE.SCD_Unique	Section 7.3.1

Table 4 Threats and Security Objectives - Coverage

Security Objectives	Threats	Rationale
OT.Tamper_Resistance	T.Hack_Phys	
OT.Tamper_ID	T.Hack_Phys	
OT.EMSEC_Design	T.Hack_Phys	
OT.DTBS_Integrity_TOE	T.SigF_Misuse, T.DTBS_Forgery	
OT.Sigy_SigF	T.SigF_Misuse	
OT.Sig_Secure	T.SCD_Derive, T.Sig_Forgery	
OT.SCD_Secrecy	T.SCD_Divulg, T.Hack_Phys	
OT.Lifecycle_Security	T.SigF_Misuse	
OT.SCD_SVD_Corresp	T.SVD_Forgery	
OT.SCD_Unique	T.Sig_Forgery	
OT.SCD/SVD_Gen	T.SCD_Derive	
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.Signatory	T.SigF_Misuse	
OE.DTBS_Intend	T.SigF_Misuse, T.DTBS_Forgery	
OE.SVD_Auth	T.SVD_Forgery	
OE.CGA_QCert	T.Sig_Forgery	
OE.SCD_SVD_Corresp	T.SVD_Forgery	
OE.SCD_Unique	T.SCD_Derive, T.Sig_Forgery	
OE.SCD_Secrecy	T.SCD_Divulg	
OE.SCD/SVD_Auth_Gen	T.SCD_Divulg	

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	
OE.SEC_PERSO		

Table 5 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 7.3.2
P.QSign	OT.Sig_Secure, OT.Sigy_SigF, OE.CGA_QCert, OE.DTBS_Intend	Section 7.3.2
P.Sigy_SSCD	OT.Lifecycle_Security, OT.SCD/SVD_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	Section 7.3.2
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	Section 7.3.2

Table 6 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies	Rationale
OT.Tamper_Resistance	P.Sigy_SSCD, P.Sig_Non-Repud	
OT.Tamper_ID	P.Sig_Non-Repud	

OT.EMSEC_Design	P.Sigy_SSCD, P.Sig_Non-Repud	
OT.DTBS_Integrity_TOE	P.Sigy_SSCD, P.Sig_Non-Repud	
OT.Sigy_SigF	P.QSign, P.Sigy_SSCD, P.Sig_Non-Repud	
OT.Sig_Secure	P.QSign, P.Sigy_SSCD, P.Sig_Non-Repud	
OT.SCD_Secrecy	P.Sigy_SSCD, P.Sig_Non-Repud	
OT.Lifecycle_Security	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud	
OT.SCD_SVD_Corresp	P.CSP_QCert, P.Sig_Non-Repud	
OT.SCD_Unique	P.Sigy_SSCD, P.Sig_Non-Repud	
OT.SCD/SVD_Gen	P.Sigy_SSCD	
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.Signatory	P.Sig_Non-Repud	
OE.DTBS_Intend	P.QSign, P.Sig_Non-Repud	
OE.SVD_Auth	P.Sig_Non-Repud	
OE.CGA_QCert	P.CSP_QCert, P.QSign, P.Sig_Non-Repud	
OE.SCD_SVD_Corresp	P.CSP_QCert, P.Sig_Non-Repud	
OE.SCD_Unique	P.Sigy_SSCD, P.Sig_Non-Repud	
OE.SCD_Secrecy	P.Sigy_SSCD, P.Sig_Non-Repud	
OE.SCD/SVD_Auth_Gen	P.CSP_QCert, P.Sigy_SSCD, 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	
OE.SEC_PERSO		

Table 7 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.CGA	OE.CGA_QCert, OE.SVD_Auth	Section 7.3.3
A.SCA	OE.DTBS_Intend	Section 7.3.3

A.CSP	OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OE.SCD_SVD_Corresp	Section 7.3.3
A.SEC_PERSO	OE.SEC_PERSO	Section 7.3.3

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

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

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

8 Extended Requirements

8.1 Extended Families

8.1.1 Extended Family FPT_EMS - TOE Emanation

8.1.1.1 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.

8.1.1.2 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.

8.1.2 Extended Family FIA_API - Authentication Proof of Identity

8.1.2.1 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.

8.1.2.2 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.

8.1.2.3 Rationale

This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

9 Security Requirements

9.1 Security Functional Requirements

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

9.1.1 All SSCD parts

9.1.1.1 Protection of the TSF (FPT)

FPT_EMS.1 TOE Emanation

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

FPT_EMS.1.2 The TSF shall ensure **that unauthorized users** are unable to use the following interface **external 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:

- **(1) self-test according to FPT_TST fails**
- **(2) power shortage**
- **(3) over and under voltage**

- **(4) over and under clock frequency**
- **(5) over and under temperature**
- **(6) integrity problems**
- **(7) 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 and periodically during normal operation** 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**.

9.1.1.2 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:

- **(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**
- **(3) 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.**
- **(4) 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 [Editorially Refined] The TSF shall restrict the ability to **create** the **RAD** to **R.Admin**.

FMT_MTD.1/Signatory Management of TSF data

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

9.1.1.3 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,**

- **Read EF.CardAccess,**
- **Execute Authentication Procedure,**
- **Select File,**
- **Verification of the RAD**
- **Establishing a trusted channel between a trusted IT product generating the SCD/SVD pair for import of the SCD as described by FDP_UCT.1/SCD and FDP_ITC.1/SCD and the TOE by means of TSF required by FTP_ITC.1/SCD (not applicable for SSCD KG).**
- **Establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD to export the SVD to the CGA ([PP-SSCD4]).**
- **Establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD to send the VAD ([PP-SSCD5], [PP-SSCD6]).**
- **Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS to send the DTBS ([PP-SSCD5], [PP-SSCD6])**

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 byte [0-255]** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall

- **Block the PIN**
- **Block the PUK**
- **When the RAD is blocked, any new authentication attempt fails**.

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**
- **Read EF.CardAccess,**
- **Execute Authentication Procedure,**
- **Select File,**

- **Verification of the RAD**
- **Establishing a trusted channel between a trusted IT product generating the SCD/SVD pair for import the SCD as described by FDP_UCT.1/SCD and FDP_ITC.1/SCD and the TOE by means of TSF required by FTP_ITC.1/SCD (not applicable for SSCD KG).**
- **Establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD to export the SVD to the CGA ([PP-SSCD4]).**
- **Establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD to send the VAD ([PP-SSCD5], [PP-SSCD6]).**
- **Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS to send the DTBS ([PP-SSCD5], [PP-SSCD6])**

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.

9.1.1.4 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 following data temporarily stored by the TOE shall have the user data attribute "integrity checked stored data":

- **DTBS/R**.

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"**.

9.1.1.5 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 usage	Algorithms	Key size	Norms
Data ciphering VITALE (PSO ENCIPHER)	**AES-CBC**	**128bits**	**NIST SP 800638B**
Card authentication VITALE (INTERNAL AUTHENTICATE)	**TDES and MAC RETAIL AES and AES CMAC**	**TDES: 112bits AES: 128bits**	**TDES: ISO 9797, AES: NIST SP 800638B**
Signature computation VITALE (PSO CCC)	**MAC RETAIL AES CMAC**	**TDES: 112bits AES: 128bits**	**TDES: ISO 9797, AES: NIST SP 800638B**
Symmetric Card authentication (Secure Messaging)	**Secure Messaging Ciphering/ Deciphering: 3DES AES**	**TDES: 112bits AES: 128bits**	**TDES: ISO 9797, AES: NIST SP 800638B**
	Mac computation: MAC RETAIL AES CMAC	**TDES: 112bits AES: 128bits**	**TDES: ISO 9797, AES: NIST SP 800638B**
	Session keys SHA-1 Session keys SHA-256	**N/A**	**SHA-1 and SHA-2**
Asymmetric Card authentication (Secure Messaging)	**Secure Messaging Ciphering/ Deciphering:**	**AES: 128bits**	**AES: NIST SP 800638B**

	AES		
	Mac computation: AES CMAC	**AES: 128bits**	**AES: NIST SP 800638B**
	Session keys SHA-256	**N/A**	**SHA-2**
	DH key exchange	**2048bits**	**ISO IAS-Premium v1.0.1**
	Signature: ISO 9796-2 with SHA-256	**2048bits**	**ISO 9796-2**
Client/Server authentication (SSL)	**RSASSA-PKCS1-V1_5 without formatting RSASSA-PSS with formatting SHA-256**	**1024bits 1536bits 2048bits**	**ISO IAS-Premium v1.0.1 PKCS#1 v2.1**
Signature computation	**RSASSA-PSS with formatting SHA-256**	**1024bits 1536bits 2048bits**	**PKCS#1 v2.1**
Certificate verification	**ISO 9796-2 with SHA-256**	**2048bits**	**ISO 9796-2**
Message key deciphering	**RSA OAEP with SHA-256**	**1024bits 1536bits 2048bits**	**PKCS#1 v2.1**
Asymmetric External Role Authentication	**Signature verification: ISO 9796-2 with SHA-256**	**2048bits**	**ISO 9796-2**
	RSASSA-PSS avec SHA-256	**2048bits**	**PKCS#1 v2.1**
Symmetric External Role Authentication	**TDES et MAC Retail AES et AES CMAC**	**TDES: 112bits AES: 128bits**	**TDES: ISO 9797, AES: NIST SP 800638B**
Hash computation	**SHA-1 SHA-256**	**N/A**	**SHA-1 SHA-2**
Asymmetric Key Pair Generation	**RSA CRT**	**1024bits 1536bits 2048bits**	**RSA**

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Key overwriting with zero** that meets the following: **none**.

9.1.2 SSCD parts 2, 4 and 5 only

9.1.2.1 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 algorithm	**Use**	**key sizes**	**list of standards**
RSA CRT Key pair generation	**SCD/SVD Generation**	**2048 bits**	**RSA PKCS#1 v2.1**

.

9.1.2.2 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**.

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 is allowed to export SVD**.

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

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

FDP_ACC.1/SCD/SVD_Generation Subset access control

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

- **subjects: S.User,**
- **objects: SCD, SVD,**
- **operations: generation of SCD/SVD pair**.

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

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

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

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

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

9.1.3 SSCD parts 3 and 6 only

9.1.3.1 Trusted path/channels (FTP)

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**.

9.1.3.2 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**.

9.1.4 SSCD part 4 only

9.1.4.1 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 [Editorially Refined] The TSF shall permit **the CGA** to initiate communication via the trusted channel.

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

- **data Authentication with Identity of Guarantor according to FIA_API.1 and FDP_DAU.2/SVD**.

9.1.4.2 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.

9.1.4.3 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**.

9.1.5 SSCD parts 5 and 6 only

9.1.5.1 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.

9.1.5.2 Trusted path/channels (FTP)

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 HID** 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**

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 SCA** to initiate communication via the trusted channel.

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

9.2 Security Assurance Requirements

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

9.3 Security Requirements Rationale

9.3.1 Objectives

9.3.1.1 Security Objectives for the TOE

All SSCD parts

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

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

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

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.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.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.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.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.

SSCD parts 2, 4 and 5 only

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.

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.

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

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.

9.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.Tamper_Resistance	FPT_PHP.3	Section 9.3.1
OT.Tamper_ID	FPT_PHP.1	Section 9.3.1
OT.EMSEC_Design	FPT_EMS.1	Section 9.3.1
OT.DTBS_Integrity_TOE	FDP_SDI.2/DTBS	Section 9.3.1
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 9.3.1
OT.Sig_Secure	FDP_SDI.2/Persistent, FPT_TST.1, FCS_COP.1	Section 9.3.1
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 9.3.1
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,	Section 9.3.1

	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	
OT.SCD_SVD_Corresp	FCS_CKM.1, FDP_SDI.2/Persistent, FMT_MSA.4, FMT_SMF.1	Section 9.3.1
OT.SCD_Unique	FCS_CKM.1	Section 9.3.1
OT.SCD/SVD_Gen	FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FIA_UAU.1, FIA_UID.1, FMT_MSA.1/Admin, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4	Section 9.3.1
OT.SCD_Auth_Imp	FIA_UID.1, FIA_UAU.1, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import	Section 9.3.1
OT.TOE_SSCD_Auth	FIA_UAU.1, FIA_API.1	Section 9.3.1
OT.TOE_TC_SVD_Exp	FDP_ACF.1/SVD_Transfer, FDP_ACC.1/SVD_Transfer, FDP_DAU.2/SVD, FTP_ITC.1/SVD	Section 9.3.1
OT.TOE_TC_VAD_Imp	FTP_ITC.1/VAD	Section 9.3.1
OT.TOE_TC_DTBS_Imp	FDP_UIT.1/DTBS, FTP_ITC.1/DTBS	Section 9.3.1

Table 10 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives	Rationale
FPT_EMS.1	OT.EMSEC_Design, OT.SCD_Secrecy	
FPT_FLS.1	OT.SCD_Secrecy	
FPT_PHP.1	OT.Tamper_ID	
FPT_PHP.3	OT.Tamper_Resistance, OT.SCD_Secrecy	
FPT_TST.1	OT.Sig_Secure, OT.SCD_Secrecy, OT.Lifecycle_Security	
FMT_SMR.1	OT.Sigy_SigF, OT.Lifecycle_Security	
FMT_SMF.1	OT.Sigy_SigF, OT.Lifecycle_Security, OT.SCD_SVD_Corresp	
FMT_MOF.1	OT.Sigy_SigF, OT.Lifecycle_Security	
FMT_MSA.1/Admin	OT.Lifecycle_Security, OT.SCD/SVD_Gen	

FMT_MSA.1/Signatory	OT.Sigy_SigF, OT.Lifecycle_Security	
FMT_MSA.2	OT.Sigy_SigF, OT.Lifecycle_Security, OT.SCD/SVD_Gen	
FMT_MSA.3	OT.Sigy_SigF, OT.Lifecycle_Security, OT.SCD/SVD_Gen	
FMT_MSA.4	OT.Sigy_SigF, OT.Lifecycle_Security, OT.SCD_SVD_Corresp, OT.SCD/SVD_Gen	
FMT_MTD.1/Admin	OT.Sigy_SigF, OT.Lifecycle_Security	
FMT_MTD.1/Signatory	OT.Sigy_SigF, OT.Lifecycle_Security	
FIA_UID.1	OT.Sigy_SigF, OT.SCD/SVD_Gen, OT.SCD_Auth_Imp	
FIA_AFL.1	OT.Sigy_SigF	
FIA_UAU.1	OT.Sigy_SigF, OT.SCD/SVD_Gen, OT.SCD_Auth_Imp, OT.TOE_SSCD_Auth	
FDP_SDI.2/DTBS	OT.DTBS_Integrity_TOE, OT.Sigy_SigF	
FDP_SDI.2/Persistent	OT.Sig_Secure, OT.SCD_Secrecy, OT.SCD_SVD_Corresp	
FDP_RIP.1	OT.Sigy_SigF, OT.SCD_Secrecy	
FDP_ACC.1/Signature_Creation	OT.Sigy_SigF, OT.Lifecycle_Security	
FDP_ACF.1/Signature_Creation	OT.Sigy_SigF, OT.Lifecycle_Security	
FCS_COP.1	OT.Sig_Secure, OT.Lifecycle_Security	
FCS_CKM.4	OT.SCD_Secrecy, OT.Lifecycle_Security	
FCS_CKM.1	OT.SCD_Secrecy, OT.Lifecycle_Security, OT.SCD_SVD_Corresp, OT.SCD_Unique	
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_Gen	
FDP_ACF.1/SCD/SVD_Generation	OT.Lifecycle_Security, OT.SCD/SVD_Gen	
FTP_ITC.1/SCD	OT.SCD_Secrecy, OT.Lifecycle_Security	
FDP_UCT.1/SCD	OT.SCD_Secrecy, OT.Lifecycle_Security	
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/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/VAD	OT.TOE_TC_VAD_Imp	
FTP_ITC.1/DTBS	OT.TOE_TC_DTBS_Imp	

Table 11 SFRs and Security Objectives

9.3.3 Dependencies

9.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied 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/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_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory,

	(FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/SCD_Import
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, FDP_ACC.1/SCD_Import
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) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SCD/SVD_Generation
FTP_ITC.1/SCD	No Dependencies	
FDP_UCT.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FTP_ITC.1/SCD, FDP_ACC.1/SCD_Import
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/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/VAD	No Dependencies	
FTP_ITC.1/DTBS	No Dependencies	

Table 12 SFRs Dependencies

9.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.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 13 SARs Dependencies

9.3.4 Rationale for the Security Assurance Requirements

The assurance level for this Security Traget is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing

product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. Augmentation results from the selection of:

9.3.4.1 AVA_VAN.5 Advanced methodical vulnerability analysis

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

9.3.4.2 ALC_DVS.2 Sufficiency of security measures

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

10 TOE Summary Specification

10.1 TOE Summary Specification

This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The summary is structured in security functions.

The security functionalities concerning the IC and the JC Platform are described in [ST-IC], [ST-PL] and are not redefined in this security target, although they must be considered for the TOE.

10.1.1 Chip security functionalities

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

10.1.2 Platform security functionalities

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

10.1.3 Application security functionalities

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, such as:

- The signatory entitled to use the services offered by the card. It is called "User Authentication".
- The device communicating with the card, to establish a trusted channel (secure messaging) and protect the communication. It is called "Device authentication".
- The administrator of a service, to administrate some features. It is called "Role 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.
  - Generate two temporary keys that will be further used to compute session keys for the secure messaging in the subsequent commands.
  - 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.

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).

This security functionality allows the following operations to be performed before the user is authenticated:

- Identification of the user,
- 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.APP_CRYPTO

This SF performs high level cryptographic operations:

- key generation:
  - SF.APP_CRYPTO performs RSA key generation of size 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 [AIS31],
- Digital signature generation:

- the signature generation function shall have an access condition based upon previous authentication of user.
- signature generation by using RSA algorithm with cryptographic key sizes of 2048 bits (provided by the JC Platform).

- Key destruction
- 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 TDES and AES in order to achieve encryption and decryption in secure messaging.
- 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.
- 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
- Data Hashing: SF.APP_CRYPTO performs SHA-1 or SHA-256 in conformance with NIST FIPS PUB 180-2, in order to calculate a hash value.
- Certificate Calculation and verification.
- RSA based key decipherment: SF.APP_CRYPTO uses RSA for deciphering an encrypted secret imported in the card.
- Certificate calculation and verification:
  - VITALE1 certificate calculation based on MAC Retail (112 bits) according to ISO 9797-1
  - VITALE2 certificate calculation based on CBC TDES (112 bits) according to ISO 9797-1
  - VITALE2 certificate verification based on RSA (2048 bits) according to ISO IAS-Premium v1.0.1
- Random Number Generation according to [AIS31]

It enables to perform e-Services such as

- Client/Server authentication
- Decryption key decipherment
- Certificate verification

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

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.

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, 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 security environment of the application and:

- Maintains the roles of Signatory and Administrator.
- Controls if the authentication required for a specific operation has been performed with success.
- Manages restriction to security function access and to security attribute modification.
- Ensures that only secure values are accepted for security attributes. This security functionality restricts the ability to perform the function Signature creation SFP to Signatory. 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:

- Export of SVD to CGA
- Generation of SCD/SVD pair by the Signatory
- Creation of RAD by the Administrator
- Signing of DTBS/R by S.Signatory

This SF manages:

- Session key generation

- Session keys are protected in integrity and confidentiality during generation. This SF enforces secure storage of the session keys during generation
- The creation of any kind of keys and the DH parameters
- 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 Secret destruction when:

- A key value is updated (by import or generation), the former key value is destroyed
- This SF calls the security function from the JC Platform to erase keys

This SF manages Secret loading:

- 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.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.

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:

- Mutual authentication used to establish session keys for secure messaging.
- Encryption and decryption of the transmitted message.
- MAC generation and verification for secure messaging.
- DH key agreement.
- Secure hash computation.
- 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.

SF.APP_INTEGRITY

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

- Prohibit the use of the altered data, and
- Inform the S.Signatory about integrity error. 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.

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.

10.2 SFRs and TSS

10.2.1 SFRs and TSS - Rationale

All SSCD parts

Protection of the TSF (FPT)

FPT_EMS.1 is met by SF.APP_CRYPTO and SF.MANAGEMENT which ensure secure execution of cryptographic operations on keys.

FPT_FLS.1 is met by JC Platform and the IC that ensure that failures in the TSF are detected and that the proper actions (reset, card termination) are taken in order to preserve a secure sate of the TOE. It is also met by SF.APP_INTEGRITY that monitors the integrity of sensitive user data and the integrity of the DTBS/R.

FPT_PHP.1 is met by SF.APP_INTEGRITY, 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.APP_INTEGRITY 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, (5) none. 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 RSA key pair consistency check.
- is met by SF.APP_CRYPTO that provides electronic signature generation compliant with RSA PKCS#1 v2.1.
- is met by SF.APP_CRYPTO that provides TDES in CBC mode or AES in CBC mode for encryption and decryption.
- is met by SF.APP_CRYPTO that provides ISO/IEC 9797-1 algorithm 3 padding 2 (3DES) or CMAC (AES) for integrity.
- is met by SF.AUTHENTICATION that provides Symmetric and Asymmetric Mutual Authentications.
- is met by SF.TRUSTED_CHANNEL that provides secure messaging with CGA and SCA.

FCS_CKM.4 is met by SF.MANAGEMENT, as SF.MANAGEMENT manages the secure destruction of secret, 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

Trusted path/channels (FTP)

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.

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.

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

- The TOE supports RSA calculations in order to generate signatures (SF.APP_CRYPTO).
- The TOE supports the establishment of a trusted channel/path based on 3DES or AES mutual authentication with negotiation of symmetric cryptographic keys used for the protection of the communication data with respect to confidentiality and integrity (SF.TRUSTED_CHANNEL, SF.APP_CRYPTO).

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/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.

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.

10.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FPT_EMS.1	SF.APP_INTEGRITY, SF.MANAGEMENT
FPT_FLS.1	SF.APP_INTEGRITY
FPT_PHP.1	SF.APP_INTEGRITY
FPT_PHP.3	SF.APP_INTEGRITY
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
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
FTP_ITC.1/SCD	SF.MANAGEMENT, SF.APP_CRYPTO, SF.TRUSTED_CHANNEL, 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/SVD	SF.MANAGEMENT, SF.TRUSTED_CHANNEL, SF.APP_CRYPTO, SF.AUTHENTICATION
FDP_DAU.2/SVD	SF.AUTHENTICATION, SF.TRUSTED_CHANNEL
FIA_API.1	SF.APP_INTEGRITY, SF.TRUSTED_CHANNEL
FDP_UIT.1/DTBS	SF.TRUSTED_CHANNEL, SF.APP_CRYPTO
FTP_ITC.1/VAD	SF.TRUSTED_CHANNEL, SF.APP_CRYPTO, SF.AUTHENTICATION, SF.MANAGEMENT
FTP_ITC.1/DTBS	SF.TRUSTED_CHANNEL, SF.APP_CRYPTO, SF.MANAGEMENT, SF.AUTHENTICATION

Table 14 SFRs and TSS - Coverage