IDEMIA

HiCOS PKI Applet

Public Security Target

About IDEMIA

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

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

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

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

IDEMIA

DOCUMENT MANAGEMENT

Business Unit – Department	**CI – R&D**
Document type	**FQR**
Document Title	**HiCOS PKI Applet – Public Security Target**
FQR No	**110 8502**
FQR Issue	**1**

CONTRIBUTORS

Name	Role	Author	Reviewer	Approver
MESTIRI, Sarra	Security Manager	Yes		
YAP Abraham	Project Leader			

DOCUMENT REVISION

Date	Revision	Modification	Modified by
2018/02/08	1.0	Creation	MESTIRI Sarra

IDEMIA

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

This document is the Security Target of a Smartcard embedding a HiCOS PKI Applet.

HiCOS PKI Applet provides a Secure Signature Creation Device as defined in the 2 PPs [8] and [9].

The Security Target on HiCOS PKI Applet aims to satisfy the requirements of Common Criteria level EAL5+, augmented with AVA_VAN.5 and ALC_DVS.2 in defining the security enforcing functions of the Target Of Evaluation and describing the environment in which it operates.

1.1. Security Target Reference

The Security target is identified as follows:

Title: Security Target CASTOR
Name: HiCOS PKI Applet
Oberthur Technologies registration: FQR 110 8141 Issue 4
Authors: Oberthur Technologies
ST Lite reference: FQR 110 8502 Issue 1
Publication Date for the Public ST-Lite: January 2018

1.2. TOE Reference

TOE Name	HiCOS PKI Applet E2prom on Cosmo v8.1-N	HiCOS PKI Applet E2prom on Cosmo v8.1-N R2
Code Identification	202832	202832
GIT CODE	V1.1-RC1	V1.1-RC1
ST Cosmo v8.1-N reference	ERATO Security Target FQR 110 7986 Ed4	ERATO Security Target FQR 110 7986 Ed5
Cosmo v8.1-N reference Security Target Lite	FQR 110 8240 Ed1	FQR 110 8240 Ed2
Cosmo v8.1-N reference Certificate	ANSSI-CC-2017/47 ANSSI-CC-2017/49	ANSSI-CC-2017/49-M1

Table 1: TOE REFERENCES

1.3. TOE Identification

The aim of the paragraphs is to allow the user to identify uniquely the TOE.

The TOE is composed of application [HiCOS] and a COSMO v8-1n (R1 and R2) platforms and an IC.

1.3.1. TOE Identification

This chapter presents the means to identify the evaluated application and the Platform.

The **[**HiCOS**]** installation command **shall** use the executable load File AID and module AID.

Name	Value
Executable Load File (ELF) AID	A0 00 00 02 83 00 00 06 22 01 69 64 00 01
Executable Module AID	A0 00 00 02 83 00 00 06 22 01 69 64 00 01 01
Application AID	Custom AID, Default is A0 00 00 02 83 00 00 06 22 01 69 64 00 01 01 01

Table 2: AID HiCOS PKI Applet

1.3.2.Platform Identification

In order to assure the authenticity of the card, the product identification shall be verified by analysing:.

TOE Name	ID-One Cosmo v8.1-N - Standard LDS Platform	ID-One Cosmo v8.1-N Large Platform	ID-One Cosmo v8.1-N R2 Large Platform
Mask / Hardware Identification	083621	084021	084022
Label PVCS code	COSMO_V81N_LDS_STANDARD_PLATFORM_R1	COSMO_V81N_LARGE_PLATFORM_R1	COSMO_V81N_LARGE_PLATFORM_R2
Patch for the Generic	089051	089041	NA
Additional Patch	086694	086684	NA
IC reference version	NXP P60D081	NXP P60D145	NXP P60D145
IC ST identification	NXP Secure Smart Card Controller P6021y VB Security Target Lite Rev. 1.51 BSI-DSZ-CC-0955-V2-2016	NXP Secure Smart Card Controller P6022y VB Security Target Lite Rev. 1.52 BSI-DSZ-CC-0973-V2-2016	NXP Secure Smart Card Controller P6022y VB Security Target Lite Rev. 1.52 BSI-DSZ-CC-0973-V2-2016
IC EAL	EAL5 with augmentations: AVA_VAN.5, ALC_DVS.2, ASE_TSS.2	EAL5 with augmentations: AVA_VAN.5, ALC_DVS.2, ASE_TSS.2	EAL5 with augmentations: AVA_VAN.5, ALC_DVS.2, ASE_TSS.2
IC certificate	BSI-DSZ-CC-0955-V2-2016	BSI-DSZ-CC-0973-V2-2016	BSI-DSZ-CC-0973-V2-2016
Date of IC certification	11 October 2016	11 October 2016	11 October 2016
Reference of the Cosmo Platform certificate	ANSSI-CC-2017/47	ANSSI-CC-2017/49	ANSSI-CC-2017/49-M01

Table 3: Platform Identification

The evaluated platform allows the loading of patch. The patch reference is specified in the platform ST for ID-One Cosmo v8.1-N and the associated platform certificate. The ID-One Cosmo v8.1-N R2 doesn't include any patch.

1.3.3. Configuration of the platform

At use phase, the loading of applications is forbidden.

1.4. Reference documents

[1] Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", September 2012, Version 3.1 revision 4.

[2] Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements", September 2012, Version 3.1 revision 4.

[3] Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance requirements", September 2012, Version 3.1 revision 4.

[4] Composite product evaluation for Smart Cards and similar devices", September 2007, Version 1.0, CCDB-2007-09-001.

[5] PP SUN Java Card™ System Protection Profile Open Configuration V2.6, April 19, 2010.

[6] IC Platform Protection Profile, Version 1.0, reference BSI-PP-0035 (15.06.2007).

[7] JIL - Certification of "open" smart card products - Version 1.1 - 4 February 2013

[8] [SSCD2] Protection Profile Secure Signature-Creation Device – Part 2: Device with key generation prEN 14169-2:2012.

[9] [SSCD3]] Protection Profile Secure Signature Creation Device - Part 3, Device with key import prEN 14169-3:2012.

[10] Joint Interpretation Library - Composite product evaluation- for Smart Cards and similar devices – v1.2

[11] Java Card - API" Application Programming Interfaces, Classic Edition, Version 3.01, February 23, 2009, Sun Microsystems.

[12] Java Card – JCRE" Runtime Environment Specification, Classic Edition, Version 3.01, February 23, 2009, Sun Microsystems.

[13] Java Card - Virtual Machine Specifications" Classic Edition, Version 3.01, February 23, 2009, Sun Microsystems.

[14] GlobalPlatform Card Specification – Version 2.2.1 – January 2011.

[15] GlobalPlatform Card Mapping Guidelines of existing GP v2.1.1 implementations on v2.2.1 – Version 1.0.1 – January 2011.

[16] GlobalPlatform Card Confidential Card Content Management – Card Specification v 2.2 – Amendment A – Version 1.0.1 – January 2011.

[17] Global Platform Card Technology, Secure Channel Protocol 03, Card - Specification v 2.2 - Amendment D- Version 1.1 - September 2009.

[18] GlobalPlatform Card UICC Configuration – Version 1.0.1 – January 2011.

[19] GlobalPlatform Card Contactless Services Card Specification v 2.2 – Amendment C Version 1.0– February 2010.

[20] Visa GlobalPlatform 2.1.1 Card Implementation Requirements – Version 2.0 – July 2007.

[21] Identification cards - Integrated Circuit(s) Cards with contacts, Part 6: Inter industry data elements for interchange", ISO / IEC 7816-6 (2004).

[22] FIPS PUB 46-3 "Data Encryption Standard", October 25, 1999, National Institute of Standards and Technology

[23] FIPS PUB 81 "DES Modes of Operation", December, 1980, National Institute of Standards and Technology

[24] FIPS PUB 140-2 "Security requirements for cryptographic modules", May 2001, National Institute of Standards and Technology

[25] FIPS PUB 180-3 “Secure Hash Standard”, October 2008 , National Institute of Standards and Technology

[26] FIPS PUB 186-3 “Digital Signature Standard (DSS)”, June 2009, National Institute of Standards and Technology

[27] FIPS PUB 197, “The Advanced Encryption Standard (AES)”, November 26, 2001, National Institute of Standards and Technology

[28] SP800_90 “Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)”, March 2007, National Institute of Standards and Technology

[29] NIST Special Publication 800-38B, Recommendation for Block, Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, May 2005

[30] CEN/EN14890:2013 Application Interface for smart cards used as Secure Signature Creation

[31] ANSI X9.31 “Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)”, 1998, American National Standards Institute

[32] ISO/IEC 9796-1, Public Key Cryptography using RSA for the financial services industry", annex A, section A.4 and A.5, and annex C (1995)

[33] ISO/IEC 9797-1, “Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher”, 1999, International Organization for Standardization

[34] PKCS#1 The public Key Cryptography standards, RSA Data Security Inc. 1993

[35] IEEE Std 1363a-2004, “Standard Specification of Public Key Cryptography – Amendment 1: Additional techniques”, 2004, IEEE Computer Society.

[36] Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard N° 2741/SGDN/DCSSI/SDS/LCR Version 1.10

[37] European Card for e-Services and national e-ID Applications - IAS ECC v1.0.1

[38] ISO/IEC 7816-4:2013, Identification Cards — Integrated circuit cards— Part 4 : Organization, security and commands for interchange

[39] ISO/IEC 9797-1:2011, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher

[40] ISO 11568-2:2012, Financial services - Key management (retail) - Part 2 : symmetric ciphers, their key management and life cycle

[41] Technical Guideline TR-03111- Elliptic Curve Cryptography Version 2.0

[42] Référentiel général de sécurité, version 2.0 du 21 février 2014 - Annexe B1 - Mécanismes cryptographiques

[43] ERATO Security Target FQR 110 7986, Issue 4 and Issue 5, Oberthur Technologies, 2017

[44] ID-One Cosmo V8.1-n, Application Loading Protection Guidance, FQR: 110 8001, Issue 1, Oberthur Technologies, 2016

[45] ID-One Cosmo V8.1, Applet Security Recommendations, FQR: 110 7999, Issue 2, Oberthur Technologies, 2016

[46] ID-One Cosmo V8.1, Pre-Perso Guide, FQR: 110 7743, Issue 4, Oberthur Technologies, 2016

[47] ID-One Cosmo V8.1, Reference Guide, FQR 110 7744, Issue 5, Oberthur Technologies, 2016

[48] HiCOS PKI Applet, HiCOS PKI Applet SOFTWARE REQUIREMENTS SPECIFICATIONS - TL ICS-2016-622-001-Secure Token-SRS(Cosmov8-Perso_Manual)-04

[49] HICOS PKI Applet – Personalization Manual, TL ICS-2016-622-001-Secure Token-UM(Cosmov8-Perso-manual)-04

[50] HICOS PKI Applet – User Manual, TL ICS-2016-622-001-Secure Token-UM(Cosmov8)-05

[51] [PLT] Javacard Open platform certified under reference ANSSI-CC-2017/49 or ANSSI - 2017/47

[52] [HiCOS] HiCOS PKI Applet, the current evaluated application (name code CASTOR)

[53] "Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange." - 2013-04-15 - Third edition – ISO/IEC 14443-3 (2009-11-19)

[54] "Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anti-collision" – ISO/IEC 14443-3 (2009-11-19)

[55] "Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol" – ISO/IEC 14443-4 Second Edition (2008-07-15)

[56] [SP 800-90A] Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)", March 2007, National Institute of Standards and Technology

[57] [SP 800-67] NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, version 1.2, July 2011

[58] [FIPS 197] The Advanced Encryption Standard (AES)", November 26, 2001, National Institute of Standards and Technology

[59] [SP 800-38F] NIST Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012

[60] [SP 800-38B] NIST Special Publication 800-38B, Recommendation for Block, Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, May 2005

[61] [FIPS 180-2] "Security requirements for cryptographic modules", May 2001, National Institute of Standards and Technology

[62] [FIPS 186-4] NIST, Digital Signature Standard (DSS), FIPS Publication 186-4, July, 2013

[63] [SP 800-108] NIST, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009

[64] [SP 800-56B] Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, National Institute of Standards and Technology, August 2009.

[65] [AIS31] A German acronym referring to standard for functionality and evaluation of random number generation

1.5. Definitions

ADF	Application Dedicated File
AES	Advanced Encryption Standard
AID	Application Identifier
AMB	Access Mode Byte
APDU	Application Protocol Data Unit (command received/Data sent by the chip)
API	Application Programming Interfaces
CA	Certification authority
CBC	Cipher Block Chaining
CGA	Certificate Generation Authority/an application that generates the certificate (link between the name and the public key)
DES	Data Encryption Standard
DF	Dedicated File
DH	Diffie Hellman
DTBS	Data to be signed (Sent by the SCA)
DTBS Representation	Representation of the Data to be signed/HASH
EAL	Evaluation Assurance Level
EF	Elementary File
EEPROM	Electrically Erasable Programmable Read Only Memory
FID	File identifier
GP	Global Platform
HI	Human Interface (used to enter the RAD and VAD by the user)
IC	Integrated Chip
ICC	Integrated Chip card
IFD	Interface Device
MAC	Message Authentication code
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RAD	Reference Authentication Data (PIN stored)
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
RSA CRT	Rivest Shamir Adleman – Chinese Remainder Theorem
SCA	Signature creation Application
SCB	Security Condition Byte
SCD	Signature Creation Data (Signature key) Private key
SCP	Secure Channel Procotol
SDO	Security Data Object/Key object or Pin Object
SHA	Secure hashing Algorithm
SSCD	Secure Signature Creation Device
SVD	Signature Verification Data (Signature Verification key)/Public key
TOE	Target of evaluation
VAD	Verification Authentication Data (PIN submitted by the holder)

1.6. Technical Terms Definition

Administrator
user who performs TOE initialization, TOE personalization, or other TOE administrative functions.

Advanced electronic signature
digital signature which meets specific requirements: *a digital signature qualifies as an electronic signature if it:*
is uniquely linked to the signatory;
is capable of identifying the signatory;
is created using means that the signatory can maintain under his sole control, and
is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

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

Certificate
digital signature used as electronic attestation binding an SVD to a person confirming the identity of that person as legitimate signer

Certificate info
information associated with a SCD/SVD pair that may be stored in a secure signature creation device
Note: Certificate info is either
a signer's public key certificate or,
one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values.
Certificate info may be combined with information to allow the user to distinguish between several certificates.

Certificate generation application CGA
collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate

Certification service provider CSP
entity that issues certificates or provides other services related to electronic signatures.

Data to be signed DTBS
all electronic data to be signed including a user message and signature attributes

Data to be signed or its unique representation DTBS/R
data received by a secure signature creation device as input in a single signature-creation operation
Note: DTBS/R is either
a hash-value of the data to be signed (DTBS), or
an intermediate hash-value of a first part of the DTBS complemented with a remaining part of the DTBS, or
the DTBS.

Legitimate user
user of a secure signature creation device who gains possession of it from an SSCD-provisioning service provider and who can be authenticated by the SSCD as its signatory

Notified body
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 this standard and for determining admissible algorithms and algorithm parameters

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)

Qualified electronic signature
advanced electronic signature that has been created with an SSCD with a key certified with a qualified certificate (**The Directive:** 5.1)

Reference authentication data RAD data persistently stored by the TOE for authentication of a user as authorized for a particular role

Secure signature-creation device
Personalized device that meets the requirements laid down in Annex III by being evaluated according to a security target conforming to this PP (**The Directive:** 2.5 and 2.6)

Signatory
legitimate user of an SSCD associated with it in the certificate of the signature-verification and who is authorized by the SSCD to operate the signature-creation function (**The Directive:** 2.3)

Signature attributes additional information that is signed together with a user message

Signature creation application SCA
application complementing an SSCD with a user interface with the purpose to create an electronic signature

Note: A signature creation application is software consisting of a collection of application components configured to:

present the data to be signed (DTBS) for review by the signatory,
obtain prior to the signature process a decision by the signatory,
if the signatory indicates by specific unambiguous input or action its intent to sign send a DTBS/R to the TOE
process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.

Signature creation data SCD
private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature .

Signature creation system SCS
complete system that creates an electronic signature consists of the SCA and the SSCD

Signature verification data SVD
public cryptographic key that can be used to verify an electronic signature

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. TARGET OF EVALUATION

2.1. Overview

2.1.1. TOE Type

The Target of Evaluation is a smartcard which is configured as a Secure Signature Creation Device (SSCD), [HiCOS], used to create a secure signature, import and generate keys.

The [HiCOS], designed for use on Java Card 3.0.4 and Global Platform 2.2 compliant smart cards, provides security for stored user data and credentials and an easy to use interface to PKI services(e.g. for strong authentication, encryption and digital signatures).

The TOE is a composite product made up of an embedded software developed using javacard technology, composed on a javacard open platform. Both are developed by Oberthur Technologies.
The embedded software is made up of four javacard components:

- a javacard Applet ([HiCOS]);
- a javacard API;
- a javacard Interface ;

The applet may be used on a contact mode compliant to ISO/IEC 7816-3 specification or on contactless mode compliant to ISO/IEC 14443 specification.

The Applet is capable of saving a PKCS#15 file structure and performing PKI related operations using the asymmetric key algorithm, such as signing or decrypting. Asymmetric key pairs can be generated directly on the smartcard or imported from the host computer.

The Applet performs identity-based authentication using PIN and cryptographic keys. A unique index value is associated with the PIN or the cryptographic key to uniquely identify the off-card entity performing the authentication.

The HiCOS PKI Applet relies on

- API which provides a wide range of services enabling to manage the files and cryptographic objects;
- Interface which provides the mechanisms for data sharing with other applets;
- API Javacard API provided by the underlying Javacard open platform;

Some parts of the TOE are already evaluated: The Cosmo v8.1-N Platform with the IC. It means that the evaluation is a composition between this Platform and the HICOS application;

2.1.2. Logical scope

The logical scope of the TOE is depicted in figure 1 below.

Some TOE part is masked on the ROM IC and other loaded at manufacturing phase. The distinction is depicted in the figure 2

The loaded package is Taiwan eID Applet (LDS Applet for CHT) with the HiCOS PKI Applet. This LDS package is only a small portion of the LDS Applet as the majority of the LDS applet is in ROM.

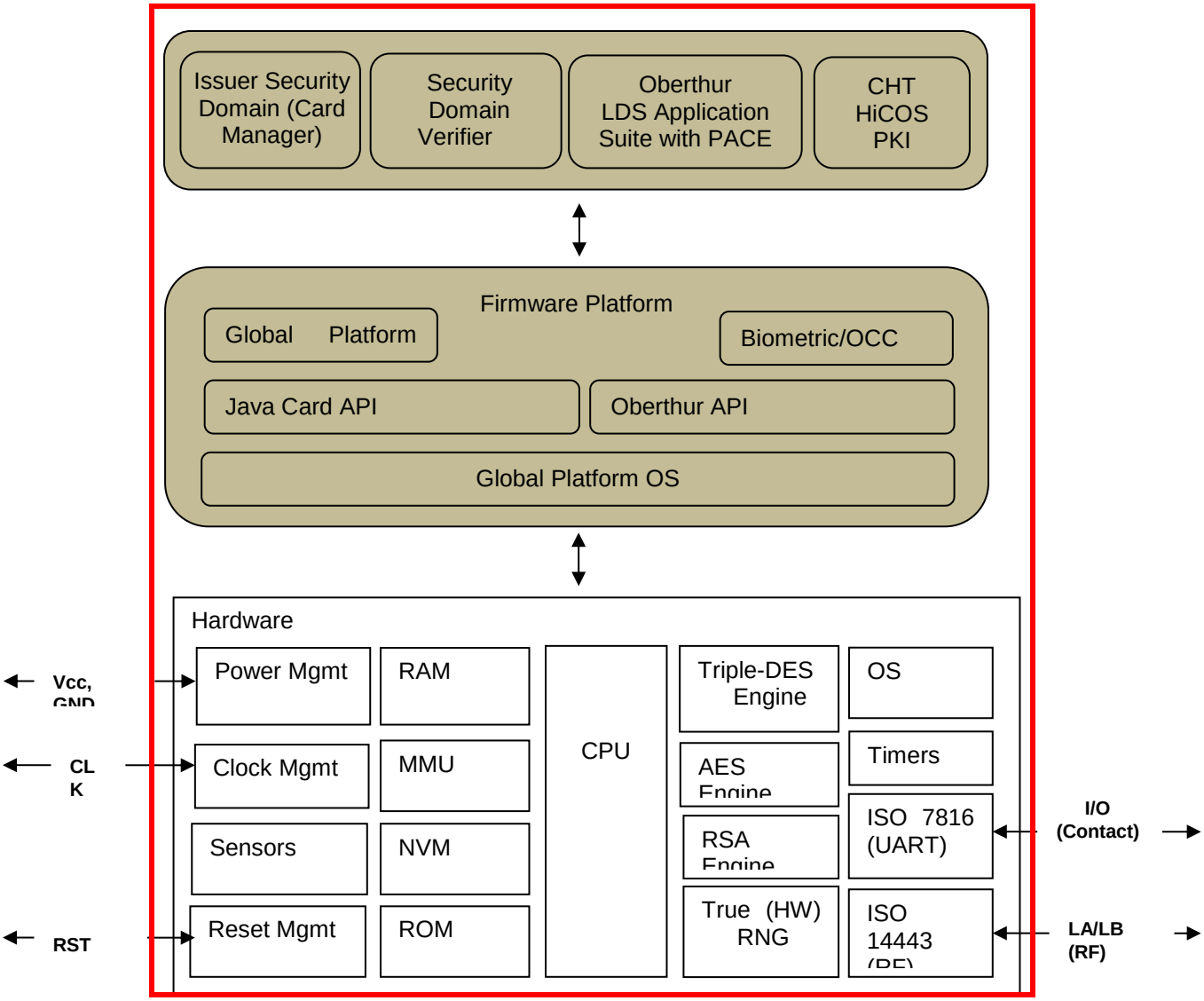

Figure 1: The logical scope of the TOE

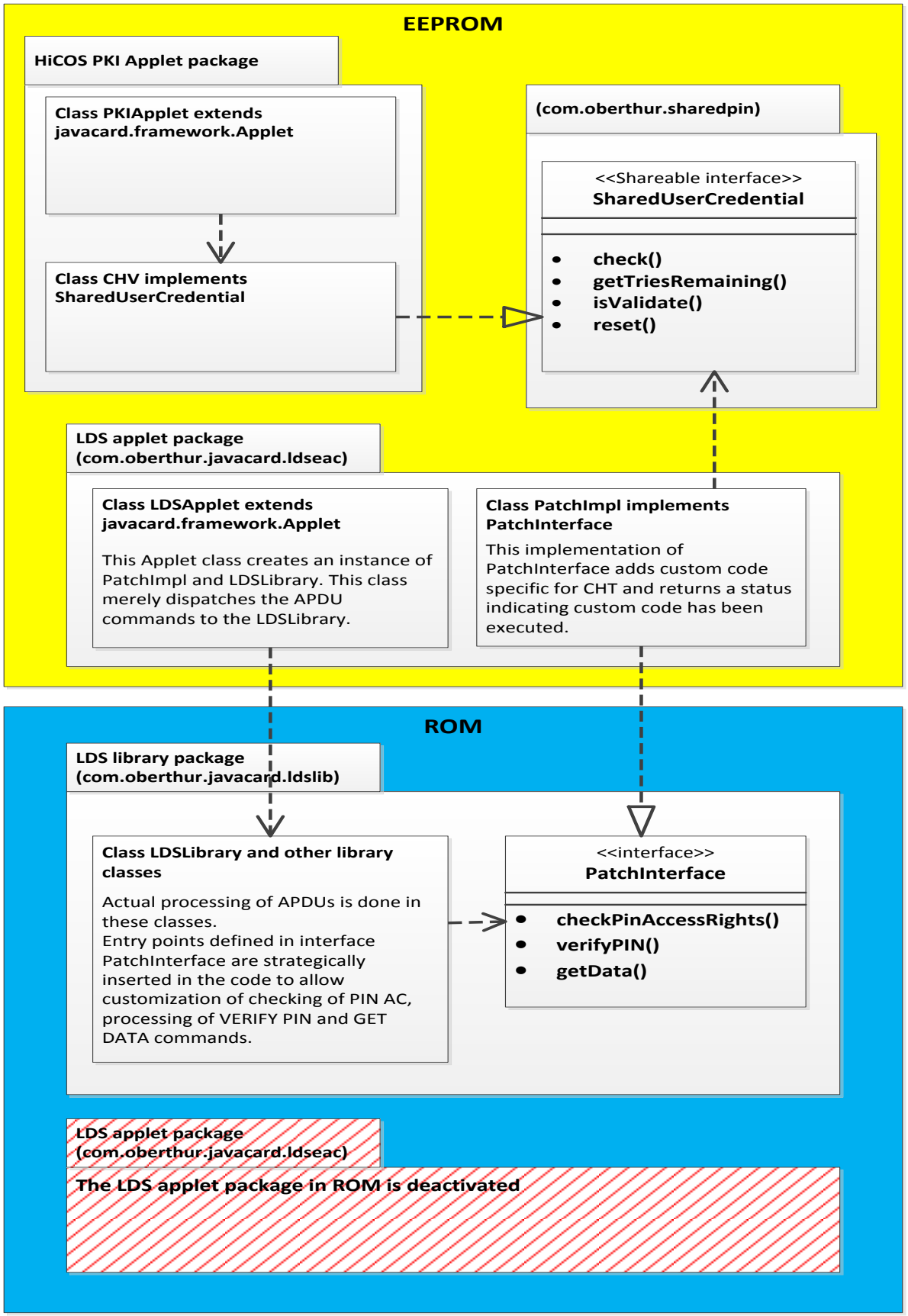

Figure 2: HiCOS Application: in ROM and in E2PROM

2.1.3. Physical scope

The TOE is physically made up of several components hardware and software. Once constructed, the TOE is a bare microchip with its external interfaces for communication. The physical medium on which the microchip is mounted is not part of the target of evaluation because it does not alter nor modify any security functions of the TOE.
The TOE may be used on several physical medium within an inlay, or eCover; in a plastic card; ...

The physical form of the module is depicted in Figure below. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads, shown as circles in the following figure.

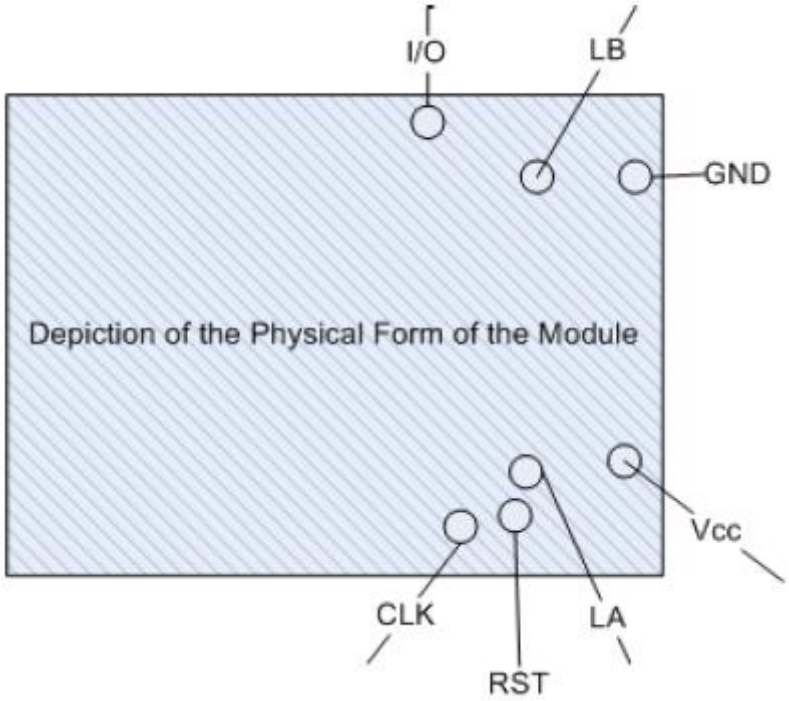

Figure 3: Physical Form

The contactless ports of the module require connection to an antenna. The module relies on [ISO7816] and [ISO14443] card readers and antenna connections as input/output devices.

Port	Description	Logical Interface Type
VCC, GND	ISO 7816: Supply voltage	Power (not available in contactless-only configurations)
RST	ISO 7816:Reset	Control in (not available in contactless-only configurations)
CLK	ISO 7816: Clock	Control in (not available in contactless-only configurations)
I/O	ISO 7816: Input/ Output	Control in, Data in, Data out, Status out (not available in contactless-only configurations)
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out (Not available in Contact-only configurations)

Table 4: Ports and Interfaces

2.1.4. Required non-TOE hardware/software/firmware

The TOE is a Secure Signature Creation Device. It is an independent product and does not need any additional hardware/software/firmware to ensure its security.

In order to be powered up and to be able to communicate the TOE needs a card reader.

2.1.5. Usage and major security features

The TOE intended usage is to be used as a “secure signature creation device” (SSCD). The TOE allows to

- To perform electronic qualified signature
- authenticate the cardholder based on a PIN verification;
- authenticate the administrator of the TOE, that may have special rights to administrate the SCD and SVD (generation, import), using symmetric mechanisms, or PIN verification;
- establish trusted channel, protected in integrity and confidentiality, with remote entities such as a SCA, a CGA or a SSCD type 1. It may be realized by means of symmetric mechanisms;

The scope of [8] and [9] is extended in several ways:

- The Administrator has special rights to administrate the signature creation function and the type of cryptographic mechanisms to use.
- The TOE may hold more than one SCD (keys). Several SCDs may be used by the holder to sign documents
- SCD/SVD pairs and other cryptographic objects may be generated and/or imported after issuance at any time, and in particular, they may be updated during the TOE life cycle.
- RAD is created at personalization phase and can be updated at any time according to the required access rules.
- The TOE may be used to realize digital signature in contact and/or contactless mode. To do so, the Personalization Agent shall ensure a correct security policy is applied to each object/data.
- A complete access control over object is ensured, whatever their type is: File or cryptographic objects (PIN, keys,…), ensuring it is not possible to bypass the access rules.

The TOE may be used for various use cases requiring qualified signature:

- Electronic signature application;
- Electronic health card;
- Electronic services cards;
- ……;

Depending on the use case and or the ability of the underlying javacard open platform, the TOE may be used

- in contact mode (T=1 protocol),
- in contactless protocol (T=CL).

2.2. Description

The TOE is presented in the Figure 1: HICOS application on Cosmo v8.1-N Platform (R1 and R2). The TOE physical interfaces and the description of the platform are available the public STs.

The platform provides an operational environment for the HICOS Applet: all cryptographic algorithm implementations and associated self-tests, random number and key generation, card lifecycle management, and key storage and protection are provided by the platform. The code for this functionality is contained in the platform ROM. However, the factory configuration of the module constrains the module to the set of services provided by the platform’s Card Manager (implementing a standard set of GlobalPlatform services),

Some functionality and options present on the Cosmo v8.1-N Platform are not usable on this module such as the PIV applet which is deactivated in this module.

The applet may be used on a contact mode compliant to ISO/IEC 7816-3 specification or on contactless mode compliant to ISO/IEC 14443 specification.

The Applet is capable of saving a PKCS#15 file structure and performing PKI related operations using the asymmetric key algorithm, such as signing or decrypting. Asymmetric key pairs can be generated directly on the smartcard or imported from the host computer.

The Applet performs identity-based authentication using PIN and cryptographic keys. A unique index value is associated with the PIN or the cryptographic key to uniquely identify the off-card entity performing the authentication

The TOE supports the following mechanisms:
- Entity authentication with password.
- Symmetric key authentication Protocol for card administrator authentication and card authentication.
- Asymmetric key generation, key unwrap and signature.

The **[HiCOS]** have the following functions with their specific details.

Function	Name	Size / Supported characteristics
ASYMMETRIC ALGORITHM	RSA	Key size: 2048 bits
SIGNATURE	RSA PKCS#1 V1.5	RSA PKCS#1 v1.5(Key size: 2048 bits)
	ECDSA	Key size: /224 / 256 / 384 / 521 bits
	SHA-256	
	SHA-384	
	SHA-512	
SECURE MESSAGING	Global Platform Secure Channel Protocol SCP03	AES 128,192,256
KEY AGREEMENT	ECDH	Key size: 224 / 256 / 384 bits
Authentication Protocol (EXTERNAL AUTHENTICATE)	3Key-TDES	Key size: 192 bits
	AES	Key size: 128,192,256 bits

Table 5 – HiCOS Cryptographic Functions

2.2.1. Data structure

The TOE manages two types of structures:
- The File, compliant with [38]
- The Security Data Objects, which are secure container storing cryptographic data (PINs, Keys,….)

2.2.1.1. File and File System

The TOE handles the following type of file (described in [48]):
- Transparent File – EF
- Key File – EF (stores an asymmetric private key or asymmetric public key)
- Application Dedicated File - ADF
- Dedicated File – DF (may contain DFs and/or Transparent Files)
- Key Container Dedicated File – DF (may contain DFs, Transparent Files and up to 15 asymmetric public key file and 15 asymmetric private key file)

All these files are organized within a File System compliant to [38]. It represents the hierarchy between all the files.

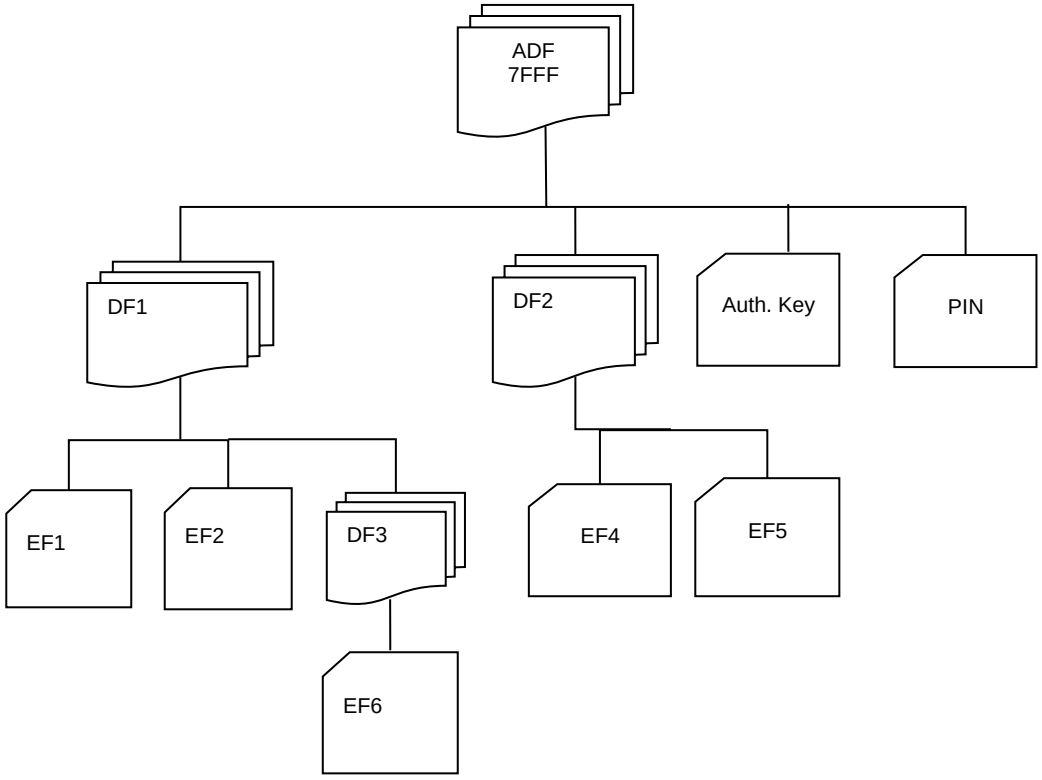

Figure 4: File System Representation

The ADF and DF, may contain Elementary File (EF) and/or Dedicated Files (DF) se figure below. Each of them may contain up to 254 files (EF or DF).

The TOE allows to

- Create any type of file (except the Application dedicated file), which update the File System.
- Read, update any transparent file (EF)

Each file is characterised by its own attributes, such as:

- Access conditions
- File identifier
- Location within the File System
- Size (for EF)
- File type

The management of the file system is fully described in [48].

2.2.1.2. Access Conditions

The access conditions are defined by couple of cryptographic data, each of them containing:

- One or several key identifier : KEY_ID
- an algorithm identifier : ALGO_ID
- a mode of usage : USE

These cryptographic data may be used to:

- define an access condition to fulfil before granting an access right: the key defined by the identifier KEY_ID shall be used with the algorithm ALGO_ID and with the mode USE to grant an access right. It is the case of a SSESP.

See chapter 7 of [48] for additional details.

2.2.1.3. Security Data Objects

The TOE handles as well cryptographic data objects, called Security Data Objects (SDO), dedicated to store the keys, the PIN and the Diffie Hellmann parameters as well as their attributes. The following types of SDO are available:

- SDO PIN contains a Personal identification Number
- SDO RSA Public Key contains a RSA Public Key
- SDO RSA Private Key contains a RSA Private Key
- SDO ECC Public Key contains an ECC Public Key
- SDO ECC Private Key contains an ECC Private Key
- SDO Symmetric DES Key Set contains a Symmetric DES Key Set
- SDO Symmetric AES Key Set contains a Symmetric AES Key Set
- SDO Diffie Hellmann parameters contains a set of Diffie Hellmann Domain parameters

The SDO may be located in any dedicated file (DF) or Application Dedicated file (ADF).

The TOE enables to create, update and use any of these SDO. The way the SDO may be used depends on its type:

- SDO PIN may be changed, reset, verified
- SDO RSA Private Key and SDO ECC Private key may be used to sign or decrypt a cryptogram
- SDO Symmetric DES Key Set and SDO Symmetric AES Key Set may be used to perform an external authentication or an internal authentication.
- SDO Diffie Hellmann parameters may be used to establish a secure channel (without authentication).

Each SDO is characterised by its own attributes, such as:

- Access conditions,
- Location within the File System,
- Size,
- Type,
- Secret value,
- Usage counter and tries counter,
- Algorithm to be used.

The management of SDO is fully described in [48].

The TOE provides access points to any other applet willing to use authentication services based on a PIN stored in the SDO PIN. In particular it is possible to:

- Check a PIN
- Retrieve the remaining tries counter
- Retrieve the validation status

This feature is used for instance when the PIN(s) is shared with a legacy application. Even though the TOE offers these entry points, it does still enforce access control in the same way it does when it receives incoming APDU to use a PIN.

2.2.2. Access Control Management

One of the Core features of the TOE is to provide access control management on any operations on any objects it handles (Files or SDO).

The Access conditions are defined in the in [48].

Prior to granting access to a given operation, the TOE checks that the requested access rights are fulfilled. Basically, an Access condition is granted if the security conditions are fulfilled. An access condition is a combination of security conditions based on identified keys/PIN/secrets:

- User Authentication (by PIN). It is used to authenticate the cardholder or a remote administrator
- Authentication of the administrator
- Communication protected in integrity and confidentiality.

2.2.3. Authentication of Entities

The TOE allows the authentication of several entities in order to grant them some rights:

- Mutual authentication is required with the establishment of a trusted channel protected in integrity and confidentiality (based on symmetric scheme) for any user of the TOE.
- User Authentication (by PIN). It is used to authenticate the cardholder
- Personalisation Agent authentication (for the phase 6) by the External Authentication key
- TOE Administrator authentication (in phase 7) using Global Platform Keys.

These authentication mechanisms are the cornerstone for the access control mechanisms use to grant access to resources (Files or SDO).

2.2.4. Secure Channel

Symmetric AES Key Set is used to perform a mutual authentication by using the Global Platform services to establish secure channel.

2.2.5. Cryptographic Function

The TOE implements cryptographic functions listed in **Erreur ! Source du renvoi introuvable.** below:

Algorithm	Description
DRBG	[SP 800-90A] AES-128 CTR_DRBG. Does not support prediction resistance, supports re-seed operation and concatenation to provide security strength greater than 128 bits.
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The module supports 3-Key option only, and CBC and ECB modes.
AES	[FIPS 197] Advanced Encryption Standard algorithm. The module supports AES-128, AES-192- and AES-256 keys, and ECB and CBC modes.
AES Key Wrap	[SP800-38F] AES Key Wrap (key establishment method provides 128-256 bits of encryption strength).
AES CMAC	[SP800-38B] AES CMAC. The module supports AES-128, AES-192 and AES-256 keys.
SHA-256	[FIPS 180-2] Secure Hash Standard compliant one-way (hash) algorithms: SHA-224, SHA-256.
SHA-512	[FIPS 180-2] Secure Hash Standard compliant one-way (hash) algorithms: SHA-384, SHA-512.
RSA STD	[FIPS 186-4] RSA signature verification. The module supports 2048-bit RSA keys.
RSA CRT	[FIPS 186-4] RSA key generation and signature generation. The module supports 2048-bit RSA keys.
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm. The module supports the NIST defined P-224, P-256, P-384, and P-521 curves for key pair generation, signature and signature verification.

KDF	[SP 800-108] AES CMAC-based KDF with AES-128, AES-192, AES-256.
RSADP	[SP 800-56B] SP 800-56B Section 7.1.2 RSA decryption primitive (as used by the PIV specification). The module supports the RSA-2048 key pair size, key decryption only.
True (HW) RNG	[AIS 31] Class P2 Hardware True RNG used to seed the FIPS approved DRBG.
Key wrap	Symmetric key wrap using AES 128, 192, 256 (key establishment method provides 128-256 bits of encryption strength). Method not compliant to SP 800-38F.

Table 6 – List of Cryptographic Functions used by the TOE

2.3. Reference

The TOE is identified as follows:

Application Guidance	
TOE name (commercial name)	HiCOS PKI Applet on ID-One Cosmo v8.1-N
Guidance document for preparation	Personalization Manual [49]
Guidance document for operational use	User Manual [50]
Platform Guidance	
Guidance document for Platform Pre-personalisation	COSMO V8.1-N Pre-Perso Guide[46]
Developer of sensitive applications*	COSMO V8.1-N Security Recommendations [45]
Guidance for application developer*	COSMO V8.1-N Reference Guide [47]
Guidance to Issuer of the platform that aims to load applications*	COSMO V8.1-N Application Loading Protection Guidance [44]

Table 7 – TOE Guidance REFERENCES

*: the loading of application in post issuance is not possible for the present product, the platform is closes at post issuance. The loading of application can occur issuing the product in use phase (before phase7).

2.4. TOE Life Cycle Overview

With respect to the Life cycle envisioned in [43], seven different phases may be sorted out. The life cycle of the composite TOE may be depicted as follows:

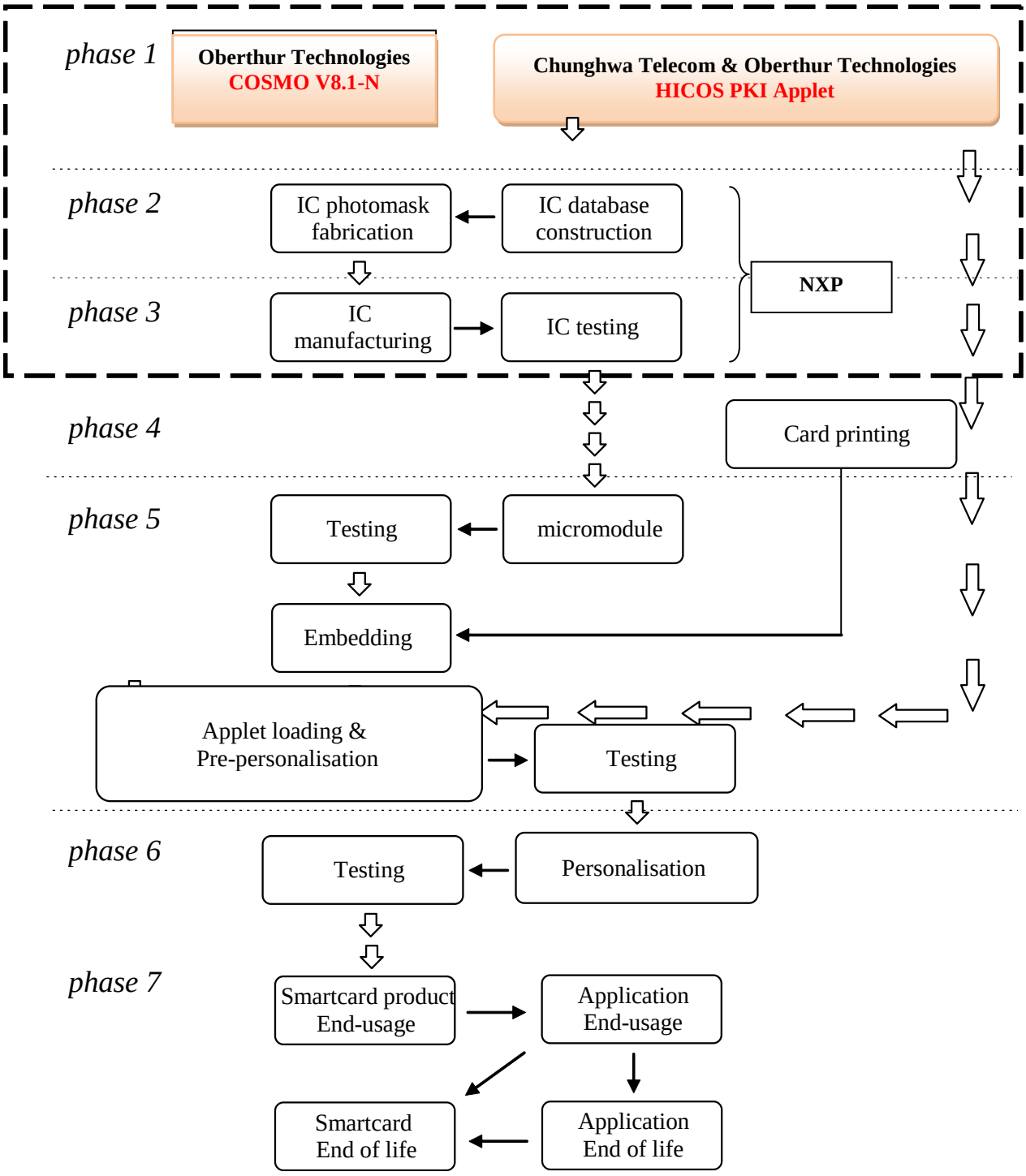

Figure 5: TOE Life Cycle

The point of delivery of the Platform is the end of phase 3. At this moment, the platform is protected, but the HICOS application not yet loaded. The loading of the application is done at phase 5 following AGD measures by Platform secured functions and ALC Organisational measures.

The TOE Life cycle may be decomposed in three steps:

- Development (phase 1 to 3);
- Applet loading and Production (phase 4 and 5);
- Operational state (phase 6 and 7);

2.4.1. Development

The development of the TOE takes place in phase 1 to 3. In this step, all parts of TOE are designed and tested. This step is covered by ALC tasks.

2.4.1.1. Software Development (Phase 1)

This development environment of the Javacard Applet [HiCOS] is done in 2 sites:
- Chunghwa Telecom development site at Taiwan
- and Oberthur technologies development at Manila.

The development of Javacard Open Platform is done at OBERTHUR TECHNOLOGIES sites: Pessac and Colombes.

The sites are audited following MSSR last requirements.

The confidentiality and integrity of the application Cap files and of the javacard open platform are covered by the evaluation of the development premises of Chunghwa Telecom and Oberthur Technologies.

At the end of this phase, the Cap File of the javacard applet is delivered to the Oberthur sites in order to be loaded in the E2PROM of the Cosmo V8 -1N Platform.
The Java card open platform with romed part of the application is sent to IC manufacturer, step 3. This step is covered by the Platform evaluation.

This Cap File application loading is done at Oberthur Technologies location. This step is covered by:
-Evaluated Platform secured functions
-Audited ALC Organisational measures.

2.4.1.2. Hardware Development (Phase 2)

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

The confidentiality and integrity of the javacard packages and javacard open platform is covered by the evaluation of the development premises of the IC manufacturer (see references in [43]).

2.4.1.3. Javacard Open Platform Development (Phase 3)

In this phase, the code of the javacard open platform is masked on the IC. This phase takes place at the manufacturing site of the IC provider.

The confidentiality and integrity of the javacard packages and javacard open platform is covered by the evaluation of the development premises of the IC manufacturer (see references in [43]).

At the end of phase 3, the javacard open platform is self protected: all platform security functions are activated. The point of delivery of the platform is the end of phase 3.

2.4.2. Production

The production environment encompasses the loading of the application, the preparation of the TOE and the management of the personalisation key used to personalize it.

During this step, the following operations are made:

- The chip is mounted on a physical layout
- The javacard open platform is prepersonalized
- The javacard open platform is personalized
- The application is loaded in E2prom
- The personalisation key is loaded on the TOE
- The applet is instantiated
- The applet is prepersonalized.

This step is covered by AGD_PRE [[49], [46]] tasks for the TOE, and by ALC for the management of the personalisation key in its environment.

2.4.2.1. Javacard Open Platform Packaging and Initialization (Phase 4)

This phase is performed by the Manufacturing Agent, which controls the platform and is in charge of the packaging and initialization of the Javacard open platform.

The platform is self-protected as it requires the authentication of the Manufacturing Agent prior to any operation.

2.4.2.2. Javacard Open Platform Pre-personalization (Phase 5)

This phase is performed by the Manufacturing Agent, which controls the platform before loading the applet, in the Oberthur manufacturing sites. The procedures and the IT infrastructure ensure the integrity and authenticity of the keys used to get authenticated with the platform.

The following process is applied during this phase

- the javacard open platform is switched in phase 5 and the applet is loaded and may be instantiated in this phase;
- the javacard open platform is switched in phase 6 and the applet may be instantiated in this phase;
- the javacard open platform is switched in phase 7 and the platform is closed.

During this phase, any other applet may be loaded at any time (phase 5 or 6 of the javacard open platform).

At the end of this phase, the javacard open platform is switched in phase 7 and the loading then is enabled.

All along this phase, the TOE is self-protected as it requires the authentication of the Manufacturing Agent prior to any operation.

2.4.2.3. Loading of Application

The platform can host 2 kinds of applications: Evaluated sensitive applications and validated basic applications. Once the application is evaluated or validated, it is securely delivered to manufacturing site. This delivery ensures the integrity and confidentiality of the application code and data. Then applications code and data are securely stored.

Once HiCOS application is evaluated it is encrypted by Oberthur Technologies and sent to the

manufacturing. It is then stored encrypted. The delivery, storage and loading of the application (HICOS and any additional application) are covered by audited Organisational measures (ALC).

The HICOS application loading occurs in step 5. Some other applications can also be loaded at step 5 or at step 6.

2.4.3. Operational state

2.4.3.1. Applet pre-personalisation (phase 6)

This phase is performed by the Personalisation Agent, which controls the TOE. During this phase, the javacard applet is prepared as required by P.TOE_Construction.
All along this phase, the TOE is self-protected as it requires the authentication of the Personalisation Agent prior to any operation.

2.4.3.2. TOE personalisation (phase 6)

This phase is performed by the Personalisation Agent, which controls the TOE, which is in charge of the javacard applet personalisation.

All along this phase, the TOE is self-protected as it requires the authentication of the Personalisation Agent prior to any operation.

This phase may not necessarily take place in a manufacturing site, but may be performed anywhere. The Personalisation Agent is responsible for ensuring a sufficient level of security during this phase.

The javacard applet is personalized according to guidance document [46], and the following operations are made: creation of applicative data (SCD, SVD, RAD, File,…) and the TOE_Administrator Agent key is loaded.

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

2.4.3.3. TOE Usage (phase 7)

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

During this phase, the TOE may be used to create a secure signature and manage the SCD, the SVD and the RAD.

The product is closed. The loading of application is disabled.

2.4.4. Coverage of the different Life cycle state by the assurance components AGD & ALC

The following phases of the life cycle are covered as follows:

Steps	Life cycle State	TOE : covered by	Personalisation key : covered by
Development	**Phase 1**	**ALC [PLT] ALC [HiCOS]**	**N/A**
	Phase 2	**ALC [HiCOS]**	**N/A**

	Phase 3	**ALC (IC scope)**	**N/A**
Point of delivery of the Platform			
Loading of the application and Production	**Phase 4**	**AGD_PRE [PLT]**	**N/A**
	Phase 5	**AGD_PRE [PLT] AGD_OPE [PLT] ALC [HiCOS] for application loading**	**AGD [HiCOS]**
Point of delivery of the personalisation key			
Operational	**Phase 6**	**AGD_OPE [PLT] AGD_PRE [HiCOS]**	**N/A**
	TOE is constructed		
	Phase 6	**AGD_OPE [PLT] AGD_PRE [HiCOS]**	**N/A**
	Phase 7	**AGD_OPE [PLT] AGD_PRE [HiCOS]**	**N/A**

Table 8 – TOE life Cycle

Notation in the table:

- ALC is covered by audit
- AGD covered by guidance
- PLT in the scope of the platform evaluation
- NXP in the scope of the IC evaluation
- HICOS in the scope of the present evaluation

The point of delivery of the Platform is the end of phase 3, and the point of delivery of the personalisation key is the end of phase 5. Phases 4 to 6 are fully covered by [49], [46], [HiCOS] and ALC (audit)

2.4.5. Mapping with the Users

For each of these phases, the following subjects may interact with the TOE

Life cycle phase	Subject interacting with the TOE
Phase 1	OBERTHUR TECHNOLOGIES CHT
Phase 2	OBERTHUR TECHNOLOGIES
Phase 3	OBERTHUR TECHNOLOGIES
Platforme is self protected	
Phase 4	Manufacturing Agent Offcard
Phase 5	Manufacturing Agent Offcard
The TOE is self protected	
Phase 6	Personalisation Agent Offcard
TOE is constructed	
Phase 7	Users

Table 9 – Mapping of phases and the TOE users

3. CONFORMANCE CLAIM

3.1. Conformance claim

This security target claims conformance to the Common Criteria version 3.1, revision 4 ([1][2][3]).
The conformance to the Common Criteria is claimed as follows:

CC	Conformance rationale
Part 1	Strict conformance
Part 2	Conformance to the extended part. ▪ FCS.RNG.1: “Random number generation” ▪ FPT_EMS.1: “TOE Emanation”
Part 3	The product claims conformance to EAL 5, augmented with: ALC_DVS.2 “Sufficiency of security measures” AVA_VAN.5 ”Advanced methodical vulnerability analysis”

Table 10: Conformance Rationale

Moreover the security target claims compliance with Application note 10 [7].

3.2. Protection Profile

This security target is based on the Secure Signature Creation Device (SSCD) Protection Profile [8] and [9].

4. SECURITY PROBLEM DEFINITION

4.1. Assets

The assets to be protected by the TOE and its environment within phase 6 and 7 of the TOE's life-cycle are the user data and TSF data defined as follows:

User Data	Property	Definition
SCD	Integrity, confidentiality	Private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).
SVD	Integrity	Public key linked to the SCD and used to perform an electronic signature verification (integrity of the SVD when it is exported must be maintained).
DTBS and DTBS-representation	Integrity	DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.

TSF Data	Property	Definition
RAD	Integrity, confidentiality	Reference PIN code used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)
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)
Keys (secret or private)	Integrity, confidentiality	Private or Secret keys used to authenticate an external user or entity

Table 11 – TOE assets

4.2. Users

The table below identifies the different users that can interact with the TOE. For each of them, this table indicates:

- The phase in which the user is active

Users	**Remark**	**Phases in which it is active**	**Mapping with** [8] and [9]	**Drawn from** [8] and [9] ?
Signatory	Natural user to which the signature functionality is reserved	7	User Signatory	Y
Personalisation Agent	User in charge of the personalisation in phase 6	6	User Administrator	Y

User_Admin	User with administrative right in phase 7	7	User Administrator	Y
SCA	Signature creation application	7	Depending on the use case, and the TOE preparation (see [49]), this user may be a User, Administrator	Y
CGA	Certificate Generation Application	7	Depending on the use case, and the TOE preparation (see [49]) , this user may be a User, Administrator	Y
SSCD Type 1	Secure Signature Creation Device of Type 1	7	Depending on the use case, and the TOE preparation (see [49]) , this user may be a User, Administrator	Y
SCA	Signature creation application Signature creation application. In phase 6, this remote IT entity is mingled with the Personalisation Agent.	7	Supplemental_User	
CGA	Certificate Generation Application. In phase 6, this remote IT entity is mingled with the Personalisation Agent.			
SSCD Type 1	Secure Signature Creation Device of Type 1		Supplemental_User	
IFD	Interface Device. This user is a generic user that may be the SCA, the CGA or the SSCD type 1 This remote IT entity is a generic one that may be the SCA, the CGA or the SSCD type 1		Supplemental_User	

TOE_Administrator	Administrator of the TOE in phase 7	7	Supplemental_User	

Table 12 – TOE Users

4.3. Assumption

4.3.1. Assumptions drawn from [8] and [9]

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-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

A.CSP	Secure SCD/SVD management by CSP

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

4.4. Threats

4.4.1. Threats drawn from [8] and [9]

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

An attacker can store, copy 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 public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated 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 with the TOE interfaces 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 TOE. 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 Signed Data Object 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-representation

An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intends 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 generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

4.4.2. Complementary Threats

T.Key_Derive	**Derive a key**
An attacker derives an authentication key (of the TOE or an external entity) from public known data, such as the corresponding public key or cryptogram created by means of the key or any other data communicated outside the TOE, which is a threat against the secrecy of the key.	

4.5. Organizational security policies

4.5.1. Organizational security policies

P.CSP_QCert	**Certificate**
The CSP uses a trustworthy CGA to generate the certificate 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 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, which is a qualified electronic signature if it is based on a valid qualified certificate. 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.	

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

4.5.2. Complementary organizational security policies

P.LinkSCD_QualifiedCertificate	**Link between a SCD stored in the TOE and the relevant qualified certificate**
The Subject in charge of creating and updating the SCD (**Personalisation Agent**, **Administrator**, **Signatory**), or the remote IT entity involved in the updating process (the **SSCD,** the **CGA)** shall ensure an unambiguous link between the (qualified) certificate(s) and the matching SCD(s). This link might be figured out by a PKCS#15 structures, an XML structure, an identifier; linking the file containing the (qualified) certificate or the URL hosting them to the SCD(s) loaded in the TOE. In particular, it implies this link updated, each time the SCD(s) is created, imported, erased or generated.	

P.TOE_Construction	Construction of the TOE by the Personalisation Agent
The recommendations indicated in [49]required to construct the TOE are correctly applied.	

4.6. Security Objectives for the TOE

4.6.1. Security objectives of the TOE drawn from [8] and [9]

OT.Lifecycle_Security	Lifecycle security
The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide functionality to securely destroy the SCD.	

OT.SCD_Auth_Imp	Authorized SCD import
The TOE shall provide security features to ensure that authorized users only may invoke the import of the SCD.	

OT.SCD_Secrecy	Secrecy of the signature-creation data
The secrecy of the SCD (used for signature generation) is reasonably assured against attacks with a 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 reconstructed using the digital signatures or any other data exploitable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.	

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

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

OT.EMSEC_Design	Provide physical emanations security
The TOE shall be designed and build in such a way as to control the production of intelligible emanations within specified limits.	

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

OT.Tamper_Resistance	Tamper resistance
The TOE shall prevent or resists physical tampering with specified system devices and components.	

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 an unambiguous reference of created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD.	

OT.SCD/SVD_Authe_Gen	Authorized SCD/SVD generation

The TOE shall provide security features to ensure that authorized users only may invoke the generation of the SCD and the SVD.

OT.SCD_Unique	Uniqueness of the signature-creation data

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

4.6.2. Complementary security objectives

OT.SCD/SVD_Management	Management of SCD/SVD

The TOE enables to manage SCD/SVD. Each key (pair) and RAD may be created at any time and used to perform qualified signature during the TOE life time. Several SCD, SVD, and RAD may be present on the TOE and used by the same holder. The TOE guarantees the SCD, SVD and RAD are independent from each other.

OT.TOE_AuthKey_Unique	Uniqueness of the TOE authentication key(s)

The TOE shall ensure the cryptographic quality of the authentication key pair used for the TOE authentication. The private key used for TOE authentication can practically occur only once and cannot be reconstructed from the public key. In that context 'practically occur once' means that the probability of equal TOE authentication key is negligible low.

OT.SVD_Auth_TOE	TOE ensures authenticity of the SVD

The TOE provides means to enable the CGA to verify the authenticity SVD that has been exported by that TOE.

OT.LifeCycle_Management	Management of the life cycle

The TOE provides a life cycle management enabling to separate its life cycle in two main phases.
The first one (phase 6) is the one during the TOE is under the sole control of the Personalization Agent.
The following operation may be realized:

- The **SCD**, **SVD** and keys may be created, generated, imported or erased
- The **RAD** (s) may be created and loaded
- **SVD** and public keys may be exported

Once performed, the Personalisation Agent switches the TOE in phase 7. This transition is irreversible leaving the TOE under the sole control of the signatory and the administrator (including the SCA, CGA, SSCD, IFD) and the TOE_Administrator according to the security rules set by the Personalisation Agent.

4.7. Security objectives for the Environment

4.7.1. Security objectives of the Environment drawn from [8] and [9]

OE.SCD/SVD_Auth_Gen	Authorized SCD/SVD generation

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

OE.SCD_Secrecy	SCD secrecy

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

OE.SCD_Unique	Uniqueness of the signature creation data

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

OE.SCD_SVD_Corresp	**Correspondence between SCD and SVD**

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

OE.SVD_Auth	**Authenticity of the SVD**

The operational environment shall ensure the authenticity 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)

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

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

OE.SSCD_Prov_Service	**Authentic SSCD provided by SSCD-provisioning service**

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

OE.HID_VAD	**Protection of the VAD**

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

OE.DTBS_Intend	**SCA sends data intended to be signed**

The signatory shall use a trustworthy SCA that

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

OE.DTBS_Protect	**SCA protects the data intended to be signed**

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

OE.Signatory	**Security obligation of the signatory**

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

4.7.2. Complementary security objectives of the Environment

OE.LinkSCD_QualifiedCertificate Link between a SCD stored in the TOE and the relevant qualified certificate

The Subject in charge of creating and updating the SCD (**Personalisation Agent**, **Administrator**, **Signatory**), or the remote IT entity involved in the updating process (the **SSCD,** the **CGA)** shall ensure an unambiguous link between the (qualified) certificate(s) and the matching SCD(s). This link might be figured out by a PKCS#15 structures, an XML structure, an identifier .linking the file containing the (qualified) certificate or the URL hosting them to the SCD(s) loaded in the TOE. In particular, it implies this link is updated, each time the SCD(s) is created, imported, erased or generated.

OE.TOE_Construction Construction of the TOE by the Personalisation Agent

The Personalization Agent in charge of administrating the TOE in phase 6 shall be a trusted person and shall be skilled enough to correctly apply the recommendations indicated in [49]. These recommendations are required to construct the TOE.

5. EXTENDED REQUIREMENTS

5.1. Extended Component Definition

5.1.1. Extended Family FPT_EMS - TOE Emanation

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. The definition of the family FPT_EMS is taken from the Protection Profile Secure Signature Creation Device [8].

FPT_EMS.1 TOE Emanation

Family Behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS TOE Emanation	1

Audit:
There are no actions defined to be auditable

Management:
There are no management activities foreseen

Hierarchical to:

No other components.

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.

5.1.2. Extended Family FCS_RNG - FCS_RNG: Random Number Generation

Family behaviour

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

Extended Components

Extended Component FCS_RNG.1

Description

A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs.

Component levelling:
Generation of random numbers requires that random numbers meet a defined quality metric

Audit:
There are no actions defined to be auditable

Management:
There are no management activities foreseen

Hierarchical to:
No other components.

Definition

FCS_RNG.1 Random Number Generation

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

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

Dependencies: No dependencies.

6. SECURITY REQUIREMENTS

6.1. Security Functional Requirements

The following SFRs are drawn from [8] and [9]. To easy the read all sfrs are reproduced even if there some duplications.

6.1.1. SFR drawn from the Protection Profile type 2

Underlined parts correspond to instantiations, where the ones referenced by a footnote are the instantiations of this Security Target and the ones without instantiations of the Protection Profile.

6.1.1.1. Cryptographic support (FCS)

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

FCS_CKM.1.1/RSA The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm RSA key generation and specified cryptographic key sizes RSA 2048 bits[1] that meet the following:

- FIPS 186.3

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

FCS_CKM.1.1/ECDSA The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm ECDSA key generation and specified cryptographic key sizes 224 up to 521 bits that meet the following:

- ECDSA – Elliptic Curve Digital Signature Scheme (TR 3111),
- FIPS 186-4.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method automatically delated when re-import or re- generation of the key that meets the following: none[2].

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

[1] *[assignment*: cryptographic key sizes*]*

[2] [assignment*: list of standards*].

FCS_COP.1.1 The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm

- Hash: SHA256, SHA384, SHA512
- Signature based on RSA and elliptic curve signature scheme:
  - RSA PKCS#v1.5
  - RSA PSS

and cryptographic key sizes RSA 2048 bits and EC 224 up to 521 bits that meet the following:

- RSA Digital Signature Schemes with Appendix (RSA labs)
  - PKCS version 1.5 RSASSA-PKCSv1_5
  - PKCS version 2.1 Probabilistic Signature Scheme RSASSA-PSS
- ECDSA – Elliptic Curve Digital Signature Scheme (TR 3111) X9.62 format3.

6.1.1.2. User data protection (FDP)

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

S.User	Role	R.Admin R.Sigy
	SCD/SVD Management	Authorized Not authorized
SCD	SCD Operational	No Yes
	SCD identifier	Arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

[3] *[assignment:* list of standards*]*

FDP_ACC.1/SCD/SVD_Generation *Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

(1) subjects: S.User,

(2) objects: SCD, SVD,

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

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

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 "authorized" is allowed to generate SCD/SVD pair.

FDP_ACF.1.3/ SCD/SVD_Generation The TSF shall explicitly authorize 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 authorized" is not allowed to generate SCD/SVD pair.

FDP_ACC.1/SVD_Transfer Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

(1) subjects: S.User,

(2) objects: SVD

(3) operations: export.

FDP_ACF.1/SVD_Transfer Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/ SVD_Transfer The TSF shall enforce the SVD_Transfer SFP to objects based on the following:
(1) the S.User is associated with the security attribute Role,
(2) the SVD.

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

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

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

Application note: The CSP (Certificate Service Provider) is a refinement of R.Admin and the one responsible for fulfilling the SFR.

FDP_ACC.1/Signature_Creation Subset access control
Hierarchical to: No other components
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Signature_Creation The TSF shall enforce the Signature Creation SFP on
(1) subjects: S.User,
(2) objects: DTBS/R, SCD,
(3) operations: signature creation.

FDP_ACF.1/Signature creation Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ Signature_Creation The TSF shall enforce the Signature Creation SFP to objects based on the following:
(1) the user S.User is associated with the security attribute “Role” and
(2) the SCD with the security attribute “SCD Operational”.

FDP_ACF.1.2/ Signature_Creation The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
R.Sigy is allowed to create electronic signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “yes”.

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

FDP_ACF.1.4/ Signature_Creation The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute “SCD operational”

is set to “no”.

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

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

FDP_SDI.2/Persistent Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/ Persistent The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored data.

FDP_SDI.2.2/ Persistent Upon detection of a data integrity error, the TSF shall

(1) prohibit the use of the altered data

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

Application note: The following data persistently stored by the TOE has the user data attribute "integrity checked persistent stored data":

1. SCD
2. SVD

FDP_SDI.2/DTBS Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/DTBS The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored DTBS.

FDP_SDI.2.2/DTBS Upon detection of a data integrity error, the TSF shall

(1) prohibit the use of the altered data

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

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

6.1.1.3. Identification and authentication (FIA)

FIA_UID.1 Timing of identification
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow
1) Self-test according to FPT_TST.1
2) Read EF.CardAccess
3) Execute Authentication Procedure
4) Select File
5) Verification of the RAD[4]

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

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

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow
1) Self-test according to FPT_TST.1,
2) Identification of the user by means of TSF required by FIA_UID.1.

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

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

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when _3_ 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 RAD.

6.1.1.4. Security Management (FMT)

FMT_SMR.1 Security roles
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles R.Admin and R.Sigy.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FMT_SMF.1 Security management functions
Hierarchical to: No other components.

[4] [assignment: *list of additional TSF-mediated actions*]

Dependencies: No dependencies.

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

- Creation and modification of RAD,
- Management of data related to the Authentication Procedure
- 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.

FMT_MOF.1 Management of security functions behavior
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions.

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

FMT_MSA.1/Admin Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/ Admin The TSF shall enforce the SCD/SVD Generation SFP to restrict the ability to modify[5] the security attributes SCD/SVD management to R.Admin.

FMT_MSA.1/Signatory Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

FMT_MSA.2 Secure security attributes
Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

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

[5] *[assignment*: other operations*]*

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1 The TSF shall enforce the SCD/SVD Generation SFP, SVD_Transfer SFP and Signature Creation SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the R.Admin to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.4 Security attribute value inheritance

Hierarchical to: No other components.

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

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes:

- If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation.
- If S.Sigy successfully generates an SCD/SVD pair the security attribute "SCD operational of the SCD" shall be set to "yes" as a single operation.

FMT_MTD.1/Admin Management of TSF data

Hierarchical to: No other components.

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

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

FMT_MTD.1/Signatory Management of TSF data

Hierarchical to: No other components.

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

FMT_MTD.1.1/Signatory The TSF shall restrict the ability to modify[6] the RAD to R.Sigy.

6.1.1.5. Protection of the TSF (FPT)

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

[6] *[assignment*: other operations*]*

FPT_EMS.1.1 The TOE shall not emit power variations, timing variations during command execution in excess of unuseful information[7] enabling access to RAD and SCD.

FPT.EMS.1.2 The TSF shall ensure unauthorized users[8] are unable to use the following interface IC contacts[9] to gain access to RAD and SCD.

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
- self-test according to FPT_TST fails
- Exposure to out-of-range operating conditions that could lead to malfunction[10]

FPT_PHP.1 Passive detection of physical attack
Hierarchical to: No other components.
Dependencies: No dependencies.

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

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

FPT_PHP.3 Resistance to physical attack
Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[11] to the TSF[12] by responding automatically such that the SFRs are always enforced.

FPT_TST.1 TSF testing
Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self-tests at reset
- for the crypto functions(CRC-16, RNG, TDES, AES, SHA 256 are tested)
- NVM memories integrity (Java packages, Loaded patch)

to demonstrate the correct operation of the TSF.

[7] *[assignment*: specified limits*]*
[8] *[assignment*: type of users*]*
[9] *[assignment*: type of connection*]*
[10] [assignment*: list of other types of failures in the TSF*]
[11] *[assignment:* physical tampering scenarios*]*
[12] *[assignment:* list of TSF devices/elements*]*

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of TSF.

6.1.2. SFR drawn from the Protection Profile type 3

Underlined parts correspond to instantiations, where the ones referenced by a footnote are the instantiations of this Security Target and the ones without instantiations of the Protection Profile.
Bold parts correspond to editorial refinements.

6.1.2.1. Cryptographic support (FCS)

FCS_CKM.4 Cryptographic key destruction
Already defined in the chapter before.

FCS_COP.1 Cryptographic operation
Already defined in the chapter before.

6.1.2.2. User data protection (FDP)

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

S.User	Role	R.Admin R.Sigy
	SCD/SVD Management	Authorized Not authorized
SCD	SCD Operational	No Yes

FDP_ACC.1/SCD_Import *Subset access control*
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/SCD_Import The TSF shall enforce the SCD Import SFP[13] on
(1) subjects: S.User,
(2) objects: SCD,
(3) operations: import of SCD[14].

FDP_ACF.1/SCD_Import Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/SCD_Import The TSF shall enforce the SCD Import SFP[15] to objects based on the following: the user S.User is associated with the

[13] *[assignment :* access control SFP*]*

[14] *[assignment :* list of subjects, objects and operations among subjects and objects covered by the SFP*]*

[15] *[assignment :* access control SFP*]*

	security attribute “SCD/SVD Management“[16].
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[17].
FDP_ACF.1.3/ SCD_Import	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[18].
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[19].
FDP_ACC.1/Signature_Creation Already defined in the chapter before.	*Subset access control*
FDP_ACF.1/Signature creation Already defined in the chapter before.	Security attribute based access control

FDP_ITC.1/SCD	Import of user data without security attributes
Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
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	The TSF shall ignore any security attributes associated with the ~~user data~~ **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. [20]

FDP_UCT.1/SCD	Basic data exchange confidentiality
Hierarchical to:	No other components
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1/SCD	The TSF shall enforce the SCD Import SFP to receive **SCD** in a manner protected from unauthorised disclosure.

Application note: The component FDP_UCT.1/SCD requires the TSF to ensure the confidentiality of

[16] *[assignment:* list of subjects and objects controlled under the indicated SFP, and for each, the SFP- relevant security attributes, or named groups of SFP-relevant security attributes*]*

[17] *[assignment:* rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]*

[18] *[assignment:* rules, based on security attributes, that explicitly authorise access of subjects to objects*]*

[19] *[assignment:* rules, based on security attributes, that explicitly deny access of subjects to objects*]*

[20] *[assignment: additional importation control rules].*

the SCD during import. The refinement substituting “user data” by “SCD” highlights that confidentiality of other imported user data like DTBS is not required.

FDP_RIP.1 Subset residual information protection
Already defined in the chapter before

FDP_SDI.2/Persistent Stored data integrity monitoring and action
Already defined in the chapter before

FDP_SDI.2/DTBS Stored data integrity monitoring and action
Already defined in the chapter before

6.1.2.3. Identification and authentication (FIA)

FIA_UID.1 Timing of identification
Already defined in the chapter before

FIA_UAU.1 Timing of authentication
Already defined in the chapter before

FIA_AFL.1 Authentication failure handling
Already defined in the chapter before

6.1.2.4. Security Management (FMT)

FMT_SMR.1 Security roles
Already defined in the chapter before

.

FMT_SMF.1 Security management functions
Already defined in the chapter before

FMT_MOF.1 Management of security functions behavior
Already defined in the chapter before

FMT_MSA.1/Admin Management of security attributes
Already defined in the chapter before

FMT_MSA.1/Signatory Management of security attributes
Already defined in the chapter before

FMT_MSA.2 Secure security attributes
Already defined in the chapter before

FMT_MSA.3 Static attribute initialisation
Already defined in the chapter before

FMT_MSA.4 Security attribute value inheritance
Already defined in the chapter before

FMT_MTD.1/Admin Management of TSF data

Already defined in the chapter before

FMT_MTD.1/Signatory Management of TSF data
Already defined in the chapter before

6.1.2.5. Protection of the TSF (FPT)

FPT_EMS.1 *TOE Emanation*
Already defined in the chapter before

FPT_FLS.1 Failure with preservation of secure state
Already defined in the chapter before

FPT_PHP.1 Passive detection of physical attack
Already defined in the chapter before

FPT_PHP.3 Resistance to physical attack
Already defined in the chapter before

FPT_TST.1 *TSF testing*
Already defined in the chapter before

6.1.2.6. Trusted Path/Channels

FTP_ITC.1/SCD Inter-TSF trusted channel
Hierarchical to: No other components.
Dependencies: No dependencies.

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
(1) Data exchange integrity according to FDP_UCT.1/SCD,
(2) Receiving SCD by means of TSF required by FDP_ITC.1/SCD[21].

6.1.3. Additional SFRs

6.1.3.1. Phase 6

6.1.3.1.1 FCS_COP Cryptographic operation

[21] [assignment: *list of other functions for which a trusted channel is required*]

FCS_COP.1.1/ GP secret data protection

The TSF shall perform [***GP secret data encryption***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key size***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	*cryptographic key sizes*	*list of standards*
SCP03 using AES	128, 192 and 256 bits	[17]
Proprietary SCP03 using AES	128, 192 and 256 bits	Proprietary

Application Note: The type of algorithm used by the TOE depends on the configuration set during the javacard open platform personalisation (For more details see [46]).

6.1.3.1.2 FMT_MTD Management of TSF data

6.1.3.1.2.1 TOE Serial number

FMT_MTD.1.1/ TOE Serial number
The TSF shall restrict the ability to [***set***] the [***Serial number of the TOE***] to [***Personalisation Agent***].

6.1.3.1.2.2 TOE State

FMT_MTD.1.1/ TOE State
The TSF shall restrict the ability to [***switch***] the [***TOE from phase 6 to phase 7***] to [***Personalisation Agent***].

6.1.3.2. Phase 7

6.1.3.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 / Session keys

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***assignment : cryptographic algorithm***] and specified cryptographic key sizes [***assignment : cryptographic key sizes***] that meet the [***assignment : list of standards***]

Refinement:

cryptographic algorithm	*cryptographic key sizes*	*list of standards*
Key Derivation function	Two AES keys of 128, 192 and 256 bits	[25]
Key Derivation function	Three AES keys of 128, 192 and 256 bits	[25]

6.1.3.2.2 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 / Session keys

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

6.1.3.2.3 FCS_COP Cryptographic operation

FCS_COP.1.1/ Secure Messaging in Confidentiality

The TSF shall perform [***Secure Messaging in confidentiality***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	***cryptographic key sizes***	***list of standards***
Encryption with AES in CBC mode	128, 192 and 256 bits	[17]

Application Note: This algorithm is used during secure Messaging to ensure confidentiality of incoming and outgoing data.

FCS_COP.1.1/ Secure Messaging in Integrity

The TSF shall perform [***Secure Messaging in integrity and authenticity***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	***cryptographic key sizes***	***list of standards***
CMAC CMAC with pre padding method 2 and AES bloc Cipher with a length of eight bytes	128, 192 and 256 bits	[29]

Application Note: This algorithm is used during secure Messaging to ensure integrity and authenticity of incoming and outgoing data.

FCS_COP.1.1/ Symmetric Role Authentication

The TSF shall perform [***Symmetric Role Authentication***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic algorithm***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	***cryptographic key sizes***	***list of standards***
Encryption using Triple DES EDE in mode CBC Signature using Retail MAC	128 bits	[23]
Encryption using AES in mode CBC Signature using CMAC	128, 192 and 256 bits	[25]
Encryption using Triple DES EDE in mode CBC	128 bits	[22]

FCS_COP.1.1/ Symmetric Device Authentication

The TSF shall perform [***Symmetric Device Authentication***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic algorithm***] that meet the following: [***assignment : list of standards***].

Refinement:

cryptographic algorithm	***cryptographic key sizes***	***list of standards***
Encryption using Triple DES EDE in mode CBC Signature using Retail MAC	128 bits	[23]
Encryption using AES in mode CBC Signature using EMAC	128, 192 and 256 bits	[25]
Encryption using AES in mode CBC Signature using CMAC	128, 192 and 256 bits	[25]

6.1.3.2.4 FMT_MTD Management of TSF data

6.1.3.2.4.1 Association between SCD and SCD_ID

FMT_MTD.1.1/ Association between SCD and SCD_ID
The TSF shall restrict the ability to [***select***] the [***SCD using a SCD_ID***] to [***Any User***].

Application note:
At creation, the SCD is given a SCD identifier that will be permanently associated to it and used by the TOE to select it.

6.1.3.2.4.2 Unblocking of RAD

FMT_MTD.1.1/ Unblock
The TSF shall restrict the ability to [***unblock***] the [***RAD***] to [***Administrator***].

Application note:
This SFR apply to any RAD (belonging to Signatory or Administrator).

6.1.3.3. Phase 6&7

FCS_COP Cryptographic operation

FCS_COP.1.1/ Data hashing

The TSF shall perform [***data hashing***] in accordance with a specified cryptographic algorithm [***SHA-256, SHA-384, and SHA-512***] and cryptographic key sizes [***none***] that meet the following: [***FIPS 180-3***].

FCS_COP.1.1/ GP Authentication

The TSF shall perform [***Mutual Authentication***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	*cryptographic key sizes*	*list of standards*
SCP03 using AES	128, 192 and 256 bits	[17]
Proprietary SCP03 using AES	128, 192 and 256 bits	Proprietary

Application Note:
The type of algorithm used by the TOE depends on the configuration set during the javacard open platform personalisation (For more details see [46]).

FCS_RNG Random Number Generation

FCS_RNG.1 / Random Number Generation

FCS_RNG.1.1
The TSF shall provide a [***hybrid***] random number generator that implements: [***none***].

FCS_RNG.1.2
The TSF shall provide random numbers that meet [42].

FDP_ACC Access Control Policy

FDP_ACC.1.1/ECC Administration SFP

The TSF shall enforce the [***ECC Administration SFP***] on [***Management of Medium, HashOffCard and SymAuthMechanisms by the TOE Administrator (in phase 7) or Personalisation Agent (in phase 6)***].

FDP_ACC.1.1/Key Management SFP

The TSF shall enforce the [***Key Management SFP***] on
[***Import of key and Diffie Hellman Domain parameters by the User***]

Application note:
This SFP applies to the all the Diffie Hellman Domain parameters and keys handled by the TOE other than the SCD and SVD.

FDP_ACF Security attribute based access control

For the definition of the attribute, refer to 8.1

ECC Administration SFP

FDP_ACF.1.1/ ECC Administration SFP
The TSF shall enforce the [***ECC Administration SFP***] to objects based on [***Administration group***].

FDP_ACF.1.2/ ECC Administration SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
(a) [***In phase 6, subject with the security attribute "role" set to "Personalisation Agent" is allowed to modify the TOE attributes***]
(b) [***In phase 7, subject with the security attribute "role" set to "TOE_Administrator" is allowed to modify the TOE attributes***]

FDP ACF.1.3/ ECC Administration SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]

FDP_ACF.1.4/ ECC Administration SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
(a) [***In phase 6, subject without the security attribute "role" set to "Personalisation Agent" is not allowed to modify the TOE attributes***]
(b) [***In phase 7, subject without the security attribute "role" set to "TOE_Administrator" is not allowed to modify the TOE attributes***]

Key Management SFP

FDP_ACF.1.1/ Key Management SFP
The TSF shall enforce the [***Key Management SFP***] to objects based on [***Key Management group***].

FDP_ACF.1.2/ Key Management SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
(a) [*In phase 7, the user with the security attribute "role" set to "Signatory", "User_Admin", "SCA", CGA", "IFD" or "SSCD type 1" and with the security attribute "Key import Management" set to "authorised" is allowed to import key and Diffie Hellman Domain parameters]*
(b) [*In phase 6, the user with the security attribute "role" set to "Personalisation Agent" is allowed to import key and Diffie Hellman Domain parameters*]
(c) [*In phase 7, the user with the security attribute "role" set to "Signatory", "User_Admin", "SCA", CGA", "IFD" or "SSCD type 1" and with the security attribute "Key generation Management" set to "authorised" is allowed to generate a key pair*]
(d) [*In phase 6, the user with the security attribute "role" set to "Personalisation Agent" is allowed to generate a key pair*]
(e) [*In phase 7, the user with the security attribute "role" set to "Signatory", "User_Admin", "SCA", CGA", "IFD" or "SSCD type 1" and with the security attribute "Key export Management" set to "authorised" is allowed to export a public key and Diffie Hellman Domain parameters*]
(f) [*In phase 6, the user with the security attribute "role" set to "Personalisation Agent" is allowed to export a public key and Diffie Hellman Domain parameters*]
(g) [*In phase 7, if the import, export or generation operation is set to Never, any user will not be allowed to perform the operation*]
(h) [*In phase 7, if the export operation is set to Always, any user will be allowed to perform the operation*]

Application note:
In phase 6, the entity with the role "Personalisation Agent" always has the security attribute "Key export Management, "Key import Management", and "Key generation Management" set to "authorized".
In phase 7, depending on the use case, the "role" allowed to import, generate or export the keys

may be restricted to "Signatory", “User_Admin”, “SCA”, CGA”, “IFD” or “SSCD type 1”, or any combination of them.

FDP ACF.1.3/ Key Management SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]

FDP_ACF.1.4/ Key Management SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***none***]

FDP_ETC: Export to outside TSF control

Keys Transfer

FDP_ETC.1.1/ Keys transfer
The TSF shall enforce the [***Key Management SFP***] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/ Keys transfer
The TSF shall export the user data without the user data's associated security attributes.

FDP_ITC Import from outside TSF control

Keys import

FDP_ITC.1.1/ Keys
The TSF shall enforce the [***Key Management SFP***] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/ Keys
The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/ Keys
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [***Keys shall be sent by the User with the “role” set to “Signatory”, “User_Admin”, “Personalisation Agent”, “SCA”, “CGA”, “IFD” or “SSCD type 1”***].

Application note:
In phase 7, depending on the use case, the “role” allowed to import, generate or export the keys may be restricted to "Signatory", “User_Admin”, “SCA”, CGA”, “IFD” or “SSCD type 1”, or any combination of them.

FIA_AFL Authentication failure

FIA_AFL apply to the authentication mechanisms based on cryptographic keys. The following authentication mechanisms are concernend:

- Authentication of the role “Personalisation Agent”
- Authentication of the role “TOE_Administrator”
- Authentication of the role “User_Admin”
- Authentication of the role “SCA”, “CGA”, “SSCD type 1” and “IFD”.
- Authentication of the remote IT entities “SCA”, “CGA”, “SSCD type 1” and “IFD”

FIA AFL.1.1/ Authentication keys
The TSF shall detect when [***selection :[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]***] unsuccessful

authentication attempts occur related to [***consecutive failed authentication attempts***].

FIA AFL.1.2/ Authentication keys
When the defined number of unsuccessful authentication attempts has been [***met or surpassed***], the TSF shall [***assignment : list of actions***].

Refinements:

Type of entity	***Entity***	***Selection for FIA_AFL.1.1***	***list of actions***
User	"Personalisation Agent"	***Positive integer number '1'***	***Time of next authentication increases***
User	"TOE_Administrator"	***Positive integer number '1'***	***Time of next authentication increases***
User	"User_Admin" (when using symmetric role authentication)	***Administrator configurable positive integer 'N' 0 ≤ N ≤ 15***	***If N= '0', no actions are taken. If N != '0', the key is blocked***
User	"SCA", "CGA", "SSCD type 1" and "IFD" (when using symmetric device authentication)	***Administrator configurable positive integer 'N' 0 ≤ N ≤ 15***	***If N= '0', no actions are taken. If N != '0', the key is blocked***
Remote IT entity	"SCA", "CGA", "SSCD type 1" and "IFD" (when using symmetric device authentication)	***Administrator configurable positive integer 'N' 0 ≤ N ≤ 15***	***If N= '0', no actions are taken. If N != '0', the key is blocked***

FIA_ATD.1 User attribute definition

FIA ATD.1.1 / S.Admin, S.TOE_Admin, S.Personalizer
The TSF shall maintain the following list of security attributes belonging to individual users [***Authentication key***]

Application Note:
Each role is authenticated using an authentication protocol with a dedicated authentication key. The key to use is a TSF data that is either permanently stored in the TOE, or an ephemeral key extracted from a certificate.

FMT_MSA Management of security attributes

FMT_MSA.1.1/ Key Management
The TSF shall enforce the [***Key Management SFP***] to restrict the ability to [***modify***] the security attributes [***Key import management, Key generation management and Key export Management***] to [***"Signatory", "User_Admin", "personalisation Agent", "SCA", "CGA", "SSCD type 1", "IFD"***].

FMT_MSA.1.1/ Management of TOE
The TSF shall enforce the [***ECC Administration SFP***] to restrict the ability to [***modify***] the security attributes [***Medium, HashOffCard***] to [***"TOE_Administrator" or "personalisation Agent"***].

FMT_MTD Management of TSF data

FMT_MTD.1/ Admin

This SFR defined previously is applicable in step 6.

FMT_SMF Specification of Management Functions

FMT_SMF.1

This SFR defined previously is applicable in step 6.

6.2. Security Assurance Requirements

This chapter defines the list of the assurance measures required for the TOE security assurance requirements. The EAL5 + is claimed.

6.2.1. Evaluation Assurance Level rationale

The following assurance packages are required:

Measures	Name
ADV	Development
AGD	Guidance
ALC	Life Cycle
ASE	Security target
ATE	Tests
AVA	Vulnerability

6.2.1.1. ADV: Development

The following components are included:

Measures	Level
ADV_ARC	1
ADV_FSP	5
ADV_IMP	1
ADV_INT	2
ADV_SPM	N/A
ADV_TDS	4

6.2.1.2. AGD: Guidance

The following components are included:

Measures	Level
AGD_OPE	1
AGD_PRE	1

6.2.1.3. ALC: Life cycle

The following components are included:

Measures	Level
ALC_CMC	4
ALC_CMS	5
ALC_DEL	1
ALC_DVS	2 - augmented
ALC_FLR	N/A
ALC_LCD	1
ALC_TAT	2

6.2.1.4. ASE: Security target

The following components are included:

Measures	Level
ASE_CCL	1
ASE_ECD	1
ASE_INT	1
ASE_OBJ	2
ASE_REQ	2
ASE_SPD	1
ASE_TSS	1

6.2.1.5. ATE: Tests

The following components are included:

Measures	Level
ATE_COV	2
ATE_DPT	3
ATE_FUN	1
ATE_IND	2

6.2.1.6. AVA : Vulnerability

The following components are included:

Measures	Level
AVA_VAN	5 - augmented

6.2.2. Rationale for augmentation

6.2.2.1. AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component. Independent vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication.

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

- ADV_ARC.1
- ADV_FSP.4
- ADV_TDS.3
- ADV_IMP.1

- AGD_OPE.1
- AGD_PRE.1
- ATE_DPT.1

6.2.2.2. ALC_DVS.2 Sufficiency of security measures

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

ALC_DVS.2 does not have any dependencies.

6.2.3. Security Objectives Rationale

Rationales are not provided in this public version.

7. TOE SECURITY SPECIFICATION

7.1. Description

The TOE inherits all the security functions provided by the underlying javacard open platform [43](see the Security target). On top of these, it adds some supplemental security functions that are described hereafter.

SF.RAD_MGT

This security function is involved in the management of the RAD, PIN based. It ensures the link between each RAD(s) and its associated role (Signatory and Administrator).

It enforces access control over any management operation on the RAD:

- In phase 6, it only allows the RAD(s) to be created by the Personalisation Agent. It requires the RAD to be encrypted in order to ensure its confidentiality. This security function ensures the Personalisation Agent can not verify the RAD, and impersonate the role “Signatory”.
- In phase 7, it only allows the RAD(s) to be created by the administrator. Once loaded, the RAD can only be changed under control of the signatory and unblocked by the Administrator.
- In phase 7, it allows the TOE to authenticate any Role using a RAD comparison (Signatory, and Administrator if it uses a RAD).

This security function manages the validation process of the role associated to the RAD (Signatory or Administrator). It performs the comparison of the VAD with the RAD, and upon successful comparison it authenticates the associated role. Each RAD is associated to an error counter which aims at ensuring its protecting against brute force attacks. Upon each submission of an incorrect VAD, it decrements the error counter, and restores it to its maximum value upon a successful VAD submission. When the error counter has reached ‘00’, the security function blocks the usage of the RAD, and in particular bans the authentication of the associated role, and the ability to change the RAD value (for both the Signatory and the Administrator). Once blocked, the security function allows the unblocking of the RAD after the successful authentication of the role Administrator (please note that the administrator role required to unblock the RAD may be different from the one associated to the blocked RAD if ever).

This security function also ensures secure deallocation of VAD after verification and RAD after update.

This security function allows managing the RAD either through APDU commands, or through shared interfaces (using sharing mechanism). They enable other applets potentially present on the javacard platform to manage the RAD. The security function ensures the same security policy is applied on both interfaces, so that there are no logical backdoor on the RAD management.

This security function relies on SF.DEV_AUTH and SF.ADM_AUTH to authenticate the role “Administrator” required to create the RAD.

SF.SIG

This security function manages the signature creation service.

It enforces access control over the signature creation service:

- In phase 6, it ensures the signature computation function is not accessible, and in particular that the Personalization Agent cannot sign on behalf of the Signatory.
- In phase 7, it ensures the signature creation feature is activated only by the signatory.
- In phase 7, it enforces the DTBS to be sent by an authenticated SCA, in a manner ensuring its integrity, and ensures the role signatory is successfully authenticated before creating the signature.

The security function enables to select the signature key to be used for the signature creation among all the signature key hold by the TOE.

The security function ensures the data hashing (if hash on card, or partial hashing is used), and the secure signature computation using either a RSA or ECDSA private key (SCD). During the signature creation, the coherency with the matching signature public key (SVD) is verified.

This security function relies on:

- SF.DEV_AUTH to establish a trusted channel with the SCA
- SF.RAD_MGT to authenticate the Signatory
- SF.SM to transmit the DTBS

SF.DEV_AUTH

This security function manages the device authentication between the TOE and an external entity.

The device authentication is a mutual authentication between the TOE and an external entity that may be either realized using symmetric cryptography. Upon successful mutual authentication, the security function computes a shared secret (called the seed) from random numbers generated by both the TOE and the external entity and known only to them. The seed is then used by SF.SM to generate session keys to protect communication in integrity, authenticity and confidentiality, and then maintain the trusted channel. As such, this security function allows generating a trusted channel with an external entity.

This security function allows the mutual authentication with the following external entities:

- Personalisation Agent (phase 6)
- SCA (phase 6 & 7), mingled with the personalisation agent in phase 6
- CGA (phase 6 & 7), mingled with the personalisation agent in phase 6
- SSCD type 1 (phase 6 & 7), mingled with the personalisation agent in phase 6
- IFD (phase 7)

This security function manages as well the validation process of the role associated to the authentication key used by the remote IT entity. Upon successful device authentication, the associated role is authenticated. Each key is associated to an error counter (it may be infinite) which aims at ensuring its protecting against brute force attacks. Upon each wrong authentication, it decrements the error counter (if present), and restores it to its maximum value upon a successful authentication. When the error counter has reached ‘00’, the security function blocks the usage of the key, and bans the authentication of the associated role.

SF.ADM_AUTH

This security function manages the authentication of external entities by the TOE. It is only active in phase 7.

This security function enables the TOE to authenticate external entities and may be either realized using symmetric cryptography.

This security function manages as well the validation process of the role associated to the authentication key used by the external entity. Upon successful authentication, the associated role is authenticated. Each key is associated to an error counter (it may be infinite) which aims at ensuring its protecting against brute force attacks. Upon each wrong authentication, it decrements the error counter (if present), and restores it to its maximum value upon a successful authentication. When the error counter has reached ‘00’, the security function blocks the usage of the key, and bans the authentication of the associated role.

This security function allows the authentication of the following roles:

- TOE_Administrator
- User_Admin

SF.SM

This security function ensures the protection of communication between the TOE and an external entity. As such, this security function maintains a trusted channel.

This security function requires the TOE and the external entity to establish first a trusted channel using a device authentication (mutual) with SF.DEV_AUTH.

It ensures the following properties:

- In phase 6, it maintains the confidentiality, integrity and authenticity of the private keys (including the SCD), the symmetric keys (DES and AES), and the RAD (PIN)
- In phase 6, it maintains the integrity and authenticity of the asymmetric public key (including the SVD) when being exported to the outside
- In phase 7, it maintains the confidentiality, integrity and authenticity of communication exchanged between the TOE and the external entity.

In phase 7, the confidentiality, integrity and authenticity of data is ensured by cryptographic means based on symmetric cryptography. Data are encrypted and signed using the symmetric session keys generated from the seed agreed during the device (mutual) authentication (see SF.DEV_AUTH). Moreover, the protection against replay attacks is ensured by the signature which is computed using a dynamic ICV, incremented at each new command.
In phase 6, the confidentiality (for the SCD), integrity and authenticity (for the SVD), is ensured by cryptographic means based on symmetric cryptography. Data are encrypted using the symmetric session keys generated from the seed agreed during the device (mutual) authentication (see SF.DEV_AUTH). The integrity of the SVD is ensured by the
This security function is also in charge of building the session keys from the seed computed by SF.DEV_AUTH. These session keys are ephemeral and unique, as the seed is computed from random numbers generated by the TOE and the external entity.
This security function is also in charge of destroying the session keys in case an error is detected (data not authentic or not integer), or when a command in plan text is sent.

SF.KEY_MGT

This security function is involved in the management of the keys (including SCDs and SVDs).
It enforces access control over any management operation on the keys:

- In phase 6, it only allows the key (including the SCD and SVD, and the DH parameters) to be loaded, generated and exported (for the public keys) by the Personalisation Agent. It also requires the private and secret keys to be encrypted in order to ensure their confidentiality. This security function ensures the Personalisation Agent can not use the keys it has loaded or generated. It ensures the personalisation Agent can not impersonate the associated role (in case of authentication keys), or create a signature with the SCD.
- In phase 7, it enforces access control over the management operations on the SCD and SVD (import, generation and export) and ensures the SCD is loaded in an encrypted form to ensure its confidentiality.
- In phase 7, it enforces access control over the management operations on the authentication (import, generation, and export of public keys) and the DH parameters (loading). It ensures that any loading, generation or public export operation is performed by an authenticated entity (Signatory, IFD, SCA, CGA, SSDD type 1, User_Admin), according to the TOE configuration.

This security function also ensures that after update or generation, the key (including SCD and SVD) are securely destroyed.

This security function relies on:

- SF.DEV_AUTH to establish the trusted channel with the SSCD type 1
- SF.RAD_MGT to authenticate the Signatory
- SF.DEV_AUTH and SF.ADM_AUTH to authenticate the roles entitled to perform the operations
- SF.SM to maintain the trusted channel and transmit the DTBS

SF.CONF

This security function manages the configuration of the TOE.

1) It allows the modification of the following TOE attributes in both phase 6 and 7:
- Communication medium : contact and/or contactless
- Type of cryptography to be used for the remote IT entities and remote subject authentication (symmetric)
- Type of DTBS to be used: the DTBS representation fully computed outside the TOE may be used

This security function ensures their initialization to a default values when the applet instance is created, and apply an access control over modification. Only the successfully authenticated Personalisation Agent (in phase 6) or “TOE_Administrator” (phase 7) can modify these attributes.

2) It also allows the modification of the following TOE attributes in phase 6:
- TOE serial number
- TOE State

This security function ensures an access control over these operations. Only the successfully authenticated Personalisation Agent can modify these attributes.

3) It also allows the modification in phase 5 of the ability to retrieve the identification data of the TOE. The security function ensures an access control over this operation. Only the successfully authenticated Manufacturing Agent (phase 5) can modify this attributes.

4) It also allows the creation of the container in which the secure data (SCD, SVD, RAD and keys) are stored. The security function ensures an access control over the creation operation. Only the successfully authenticated Personalisation Agent (phase 6) or Administrator (phase 7) can perform this operation.

This security function relies on
- SF.DEV_AUTH to authenticate the role personalisation Agent
- SF.ADM_AUTH to authenticate the role TOE_Administrator

SF.SAFESTATE_MGT

This security function ensures the TOE is always in a safe state. It monitors the integrity of the TOE, its assets and the TSF data (RAD, keys, DTBS) by performing selftests. When an unexpected event occurs (loss of power, loss of integrity, tearing,…), it ensures
- the TOE returns in a safe state
- all sensitive data are erased
- the TOE returns in a restrictive secure state

When a major issue is detected, the security function ensures the destruction of the TOE, so that the assets are not accessible anymore.

SF.PHYS

This security function ensures the protection of the TOE against physical manipulation aiming at getting access to its assets. In particular, it ensures that the TOE
- detects physical manipulation (I/O manipulation, EM perturbation, temperature perturbation,…) and takes countermeasures.
- is protected against probing and that there is no information leakage that my be used to reconstruct sensitive data

When a major issue is detected, the security function ensures the destruction of the TOE, so that the assets are not accessible anymore.

7.2. Coverage Matrix

SFR\SF	SF.RAD_MGT	SF.SIG	SF.DEV_AUTH	SF.ADM_AUTH	SF.SM	SF.KEY_MGT	SF.CONF	SF.SAFE STATE_	SF.PHYS
FCS_CKM.1 (/RSA and /ECDSA)						X			
FCS_CKM.1 / Session keys					X				
FCS_CKM.4						X			
FCS_CKM.4 / Session keys					X				
FCS_COP.1		X							
FCS_COP.1 / Secure Messaging in confidentiality					X				
FCS_COP.1/ Secure Messaging in integrity					X				
FCS_COP.1 / Data hashing					X				
FCS_COP.1 / Symmetric Role Authentication				X					
FCS_COP.1 / Symmetric Device Authentication			X						
FCS_COP.1 / GP Authentication			X	X					
FCS_COP.1 / GP secret data protection	X				X				
FCS_RNG.1			X	X					
FDP_ACC.1 / SVD_Transfer SFP						X			
FDP_ACC.1 / Signature creation SFP		X							
FDP_ACC.1 / SCD import SFP						X			
FDP_ACC.1 / Key Management SFP						X			
FDP_ACF.1 / SVD_Transfer SFP						X			
FDP_ACF.1 / Signature creation SFP		X							
FDP_ACC.1/SCD/SVD_Generation	X					X			
FDP_ACF.1/SCD/SVD_Generation	X					X			
FDP_ACC.1.1ECC Administration SFP						X			
FDP_ACF.1 / SCD import SFP						X			
FDP_ACF.1 / Key Management SFP						X			
FDP_ACF.1/ECC Administration SFP						X			
FDP_ETC.1 / Keys Transfer						X			
FDP_ITC.1 / SCD						X			
FDP_ITC.1 / Keys						X			
FDP_RIP.1.1								X	
FDP_SDI.2 / Persistent								X	
FDP_SDI.2 / DTBS								X	

SFR\SF	SF.RAD_MGT	SF.SIG	SF.DEV_AUTH	SF.ADM_AUTH	SF.SM	SF.KEY_MGT	SF.CONF	SF.SAFE STATE_	SF.PHYS
FDP_UCT.1/SCD					X	X			
FIA_AFL.1	X								
FIA_AFL.1 / Authentication keys			X	X					
FIA_ATD.1 / S.Admin, S.TOE_Admin, S.Personalizer			X	X					
FIA_UAU.1	X	X	X	X		X			
FIA_UID.1.1	X	X	X	X		X			
FMT_MOF.1		X							
FMT_MSA.1 / Admin	X		X	X					
FMT_MSA.1 / Signatory	X								
FMT_MSA.1 / Key Management						X			
FMT_MSA.1 / Management of TOE						X			
FMT_MSA.2	X		X	X		X	X		
FMT_MSA.3	X		X	X		X	X		
FMT_MSA.4	X		X	X		X	X		
FMT_MTD.1 / Signatory	X								
FMT_MTD.1 / Admin							X		
FMT_MTD.1 / Association between SCD and SCD_ID		X							
FMT_MTD.1 / TOE Serial Number							X		
FMT_MTD.1 / TOE State							X		
FMT_MTD.1 / Unblock	X								
FMT_SMF.1	X								
FMT_SMR.1	X	X	X	X					
FPT_EMS.1									X
FPT_FLS.1								X	
FPT_PHP.1									X
FPT_PHP.3									X
FPT_TST.1								X	
FTP_ITC.1/SCD			X		X				

Table 13 – Matrix between SFRs and SF

8. ANNEX A: ATTRIBUTES FOR FDP_ACF SECURITY ATTRIBUTE BASED ACCESS CONTROL

8.1. General Attribute

General Attribute

Subject	Attribute	Status	Remark
User	**Role**	**Administrator**	The role “Administrator” may be granted to several external entities of the TOE. Please refer to §4.2 for more details. The role Admin may be granted upon successful authentication based on a cryptographic mean (authentication) or on a RAD verification (PIN). This subject can interact in phase 6 or 7 of the life cycle
		Signatory	The role “Signatory” may be granted upon successful authentication based on a RAD verification (PIN) This role can only interact in phase 7 of the life cycle

Table 14 – General attributes for FDP_ACF Security attribute based access control

8.2. Initialisation attribute group

Initialisation attribute group

Subject	Security Attribute	Status	Remark
User	**SCD/SVD Management**	**Authorized**	The TOE controls the access on every object it possess, in particular the SCD and the SVD. In phase 6, the personalisation Agent is the user Admin, and as such always has the attribute “SCD/SVD Management” set to “Authorized”. In phase 7, two access mode may be distinguished by the TOE • SCD/SVD generation (SSCD type 3) • SCD/SVD import (SSCD type 2) The access condition is granted to a User if the following conditions are met: • The User is successfully authenticated • The User was given the right to manage the SCD & SVD (import and/or generation). If theses two conditions are fulfilled, the attribute “SCD/SVD management” is set to “authorized”, otherwise it is set to “not authorized”.
		Not authorized	

User Data	Security Attribute	Status	Remark
SCD	**Secure SCD Import Allowed**	**No**	The TOE controls the access on every object it possesses, in particular the SCD. In phase 6, the key is imported from a SSCD type 1 that is mingled with the “Personalisation Agent”. The security attribute “Secure SCD import” is set to “Yes” when the role “Personalisation Agent” is validated. In phase 7, the access mode SCD Import may be refined to ensure the SCD is imported • from an entitled entity (SSCD type 1) • through a trusted channel ensuring the confidentiality and integrity of the key This refinement does not conflict with SCD/SVD Management The access condition is granted to a remote entities if the following conditions are fulfilled: • The remote entities is successfully authenticated • The remote entities sends the SCD through a secure channel ensuring confidentiality and integrity If theses two conditions are fulfilled, the attribute “Secure SCD Import Allowed” is set to “Yes”, otherwise it is set to “No”.
		Yes	

Table 15 – Initialisation attributes for FDP_ACF

8.3. Signature creation attribute group

Signature-creation attribute group

User Data	Security Attribute	Status	Remark
SCD	**SCD operational**	**No**	The attribute “SCD operational” is granted by the submission of the RAD by the User Signatory. The RAD is a PIN.
		Yes	
DTBS	**Sent by an authorized SCA**	**No**	As the TOE controls the access on every object it possess, it ensures the attribute “Sent by an authorized SCA” for the DTBS is controlled.
		Yes	

Table 16 – signature creation attributes

8.4. Administration group

Administration group

TOE Attributes	Meaning	Status	Remark
Medium	Communication medium allowed	**Contact**	The TOE may be configured to allow communication in contact and/or contactless mode. The communication to be used by the TOE may be changed in phase 6 by the "Personalisation Agent", and in phase 7 by "TOE_Administrator"
		Contactless	
HashOffCard	Qualified signature computed over hash computed off card	**Authorized**	The TOE may be configured to allow the qualified signature to be computed from a hash off card. It may be changed in phase 6 by the "Personalisation Agent", and in phase 7 by "TOE_Administrator"
		Not authorized	
SymAuthMechanisms	Authentication mechanisms based on symmetric scheme allowed	**Authorized**	The TOE may be configured to enable/disable the authentication mechanism based on symmetric scheme. It may be changed in phase 6 by the "Personalisation Agent", and in phase 7 by "TOE_Administrator"
		Not authorized	
		Not authorized	

Table 17 – Administration attributes

8.5. Key Management group

Key Management group

Subject	Security Attribute	Status	Remark
Signatory User_admin SCA CGA SSCD type 1 IFD Personalisation agent	**Key import Management**	**Authorized**	In phase 6, the Personalisation Agent has the attribute Key import Management set to Authorized In phase 7, the TOE controls the access on every object it holds, in particular key and Diffie Hellman Domain parameters. The access condition is granted to User, SCA, CGA, SSCD type 1 or IFD if the following conditions are fulfilled: • The Subject is successfully authenticated • The Subject was given the right to import a key (belonging to groups indicated above) When theses two conditions are fulfilled, the attribute Key import management is set to authorized, otherwise it is set to not authorized
		Not authorized	
	Key generation Management	**Authorized**	In phase 6, the Personalisation Agent has the attribute Key generation Management set to Authorized In phase 7, the TOE controls the access on every object. The access condition is granted to User, SCA, CGA, SSCD type 1 or IFD if the following conditions are fulfilled: • The Subject is successfully authenticated • The Subject was given the right to generate a key (belonging to groups indicated) If these two conditions are fulfilled, the attribute Key generation management is set to authorized, otherwise it is set to not authorized
		Not authorized	
	Key export Management	**Authorized**	In phase 6, the Personalisation Agent has the attribute Key export Management set to Authorized In phase 7, the TOE controls the access on every object it holds, in particular public keys and Diffie Hellman Domain parameters The access condition is granted to User, SCA, CGA, SSCD type 1 or IFD if the following conditions are fulfilled: • The Subject is successfully authenticated • The Subject was given the right to export a key (belonging to groups indicated) If theses two conditions are fulfilled, the attribute Key export management is set to authorized, otherwise it is set to not authorized
		Not authorized	

Table 18 – Key management attributes

9. ANNEX B: COMPOSITION WITH THE UNDERLYING JAVACARD OPEN PLATFORM

This annex discusses the composition with the underlying javacard platform [43] according to [10]. This part is removed from the ST lite.