IAS ECC v1.0.1
On
ID-One™ Cosmo V7.0.1-n R2 Card

(Standard and standard Dual)

Public Security target

Info@oberthur.com | www.oberthur.com

TABLE OF CONTENTS

1 Introduction

1.1 Security Target Reference

The Security target is identified as follows:

Title:	**IAS ECC v1.0.1 on ID-One™ Cosmo V7.0.1-n R2 – Public Security target**
Reference:	FQR 110 6731 edition 1
Editor:	Oberthur Technologies
CC version:	3.1 revision 4
EAL:	EAL4 augmented with AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2

1.2 References

[SSCD2]	Secure Signature-Creation Device Type2, 1.04, EAL 4+
[SSCD3]	Secure Signature-Creation Device Type3, 1.05, EAL 4+
[AGD_PRE]	FQR 110 5171 Ed7 - AGD_PRE
[AGD_OPE]	FQR 110 5170 Ed5 - AGD_OPE
[AGD_PRE_PLATFORM]	FQR 110 6407 Ed2 - ID-One Cosmo V7.0.1-n R2.0 - Pre-Perso Guide
[AGD_OPE_PLATFORM]	FQR 110 6408 Ed2 - ID-One Cosmo V7.0.1-n R2.0 - Reference Guide
[PP9911]	Smart Card Integrated Circuit With Embedded Software Protection Profile, version 2.0, June 1999. Certified under the reference PP/9911, DCSSI
[AIS31]	Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik
[FIPS180-2]	FIPS PUB 180-2, Secure Hash Standard", August 2002 , National Institute of Standards and Technology

[CC31-1]	"Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", September 2012, Version 3.1 revision 4
[CC31-2]	"Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements", September 2012, Version 3.1 revision 4
[CC31-3]	"Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance requirements", September 2012, Version 3.1 revision 4
[PKCS#1]	PKCS#1 The public Key Cryptography standards, RSA Data Security Inc. 1993
[PKCS#3]	PKCS#3
[IASECC]	IAS ECC v1.0.1
[ISO7816-4]	Identification Cards - Integrated Circuits Card - Part 4 : Organisation, security and commands for interchange : 2005
[ST_PLATFORM]	The underlying javacard platform has not been evaluated on its own and therefore does not have any security target. However, the underlying javacard platform fulfils the same SFRs, TSFs ,… as [ANSSI-CC-2009/48], [ANSSI-CC-2010/40] and [ANSSI-CC-2012/30]. Therefore, the security target of these javacard platform can be considered
[GP]	Card Specification - Version 2.1.1 - Mars, 2003

1.3 Abbreviations

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 (Authority in charge of generating the qualified certificate(s))
C/S	Client / Server
CSE	Current Security Environment
DAP	Data Authentication Pattern (enable to ensure integrity & authenticity of javacard package when loaded)
DAPP	Device Authentication with Privacy Protection

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
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)
RCA	Root Certification Authority
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
RSA CRT	Rivest Shamir Adleman – Chinese Remainder Theorem
SCA	Signature creation Application (Application requiring a qualified signature to the chip)
SCB	Security Condition Byte
SCD	Signature Creation Data (Signature key)
SCP	Secure Channel Procotol
SDO	Security Data Object
SE	Security Environment
SHA	Secure hashing Algorithm
SSCD	Secure Signature Creation Device
SSE	Static Security Environment
SSESP	Static Security Environment for Security Policies
SSO	Single Sign On
SVD	Signature Verification Data (Signature Verification key)
TOE	Target of evaluation
URL	Uniform Resource Locator
USB	Universal Serial Bus
VAD	Verification Authentication Data (PIN submitted by the holder)
XML	eXtensible Markup Language

2 Target Of Evaluation Description

2.1 Target Of Evaluation Overview

2.1.1 TOE type

The Target of Evaluation is embedded software made of

- a javacard Applet ([Applet]) developed by Oberthur Technologies
- a javacard API ([API]) developed by Oberthur Technologies
- a javacard Interface ([Interface]) developed by Oberthur Technologies

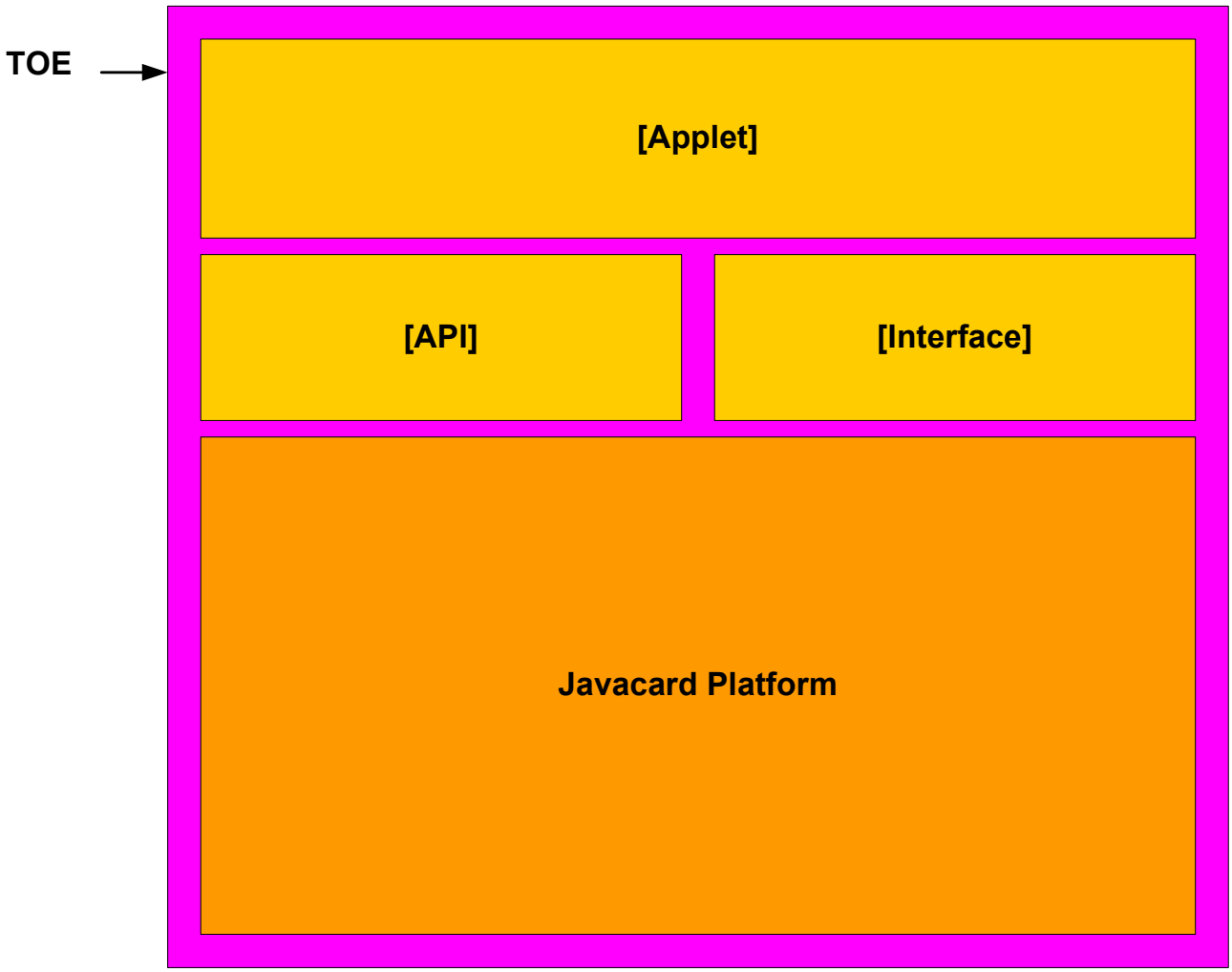
Composed with a javacard platform developed by Oberthur Technologies, on which it is running. The javacard platform is locked, i.e. it does not allow the loading of any other applets.

The javacard Applet provides to the outside the whole set of security services described herein. To do so, [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 applet
- Javacard API provided by the underlying javacard platform

2.1.2 Logical scope

The logical scope of the TOE may be depicted as follows:



Limits of the TOE

2.1.3 Physical scope

The TOE is made of a javacard platform **[PLATFORM],** set in Pre-personalization state, which contains in its ROM code the three javacard packages [**Applet**], [**API**] and [**Interface**]

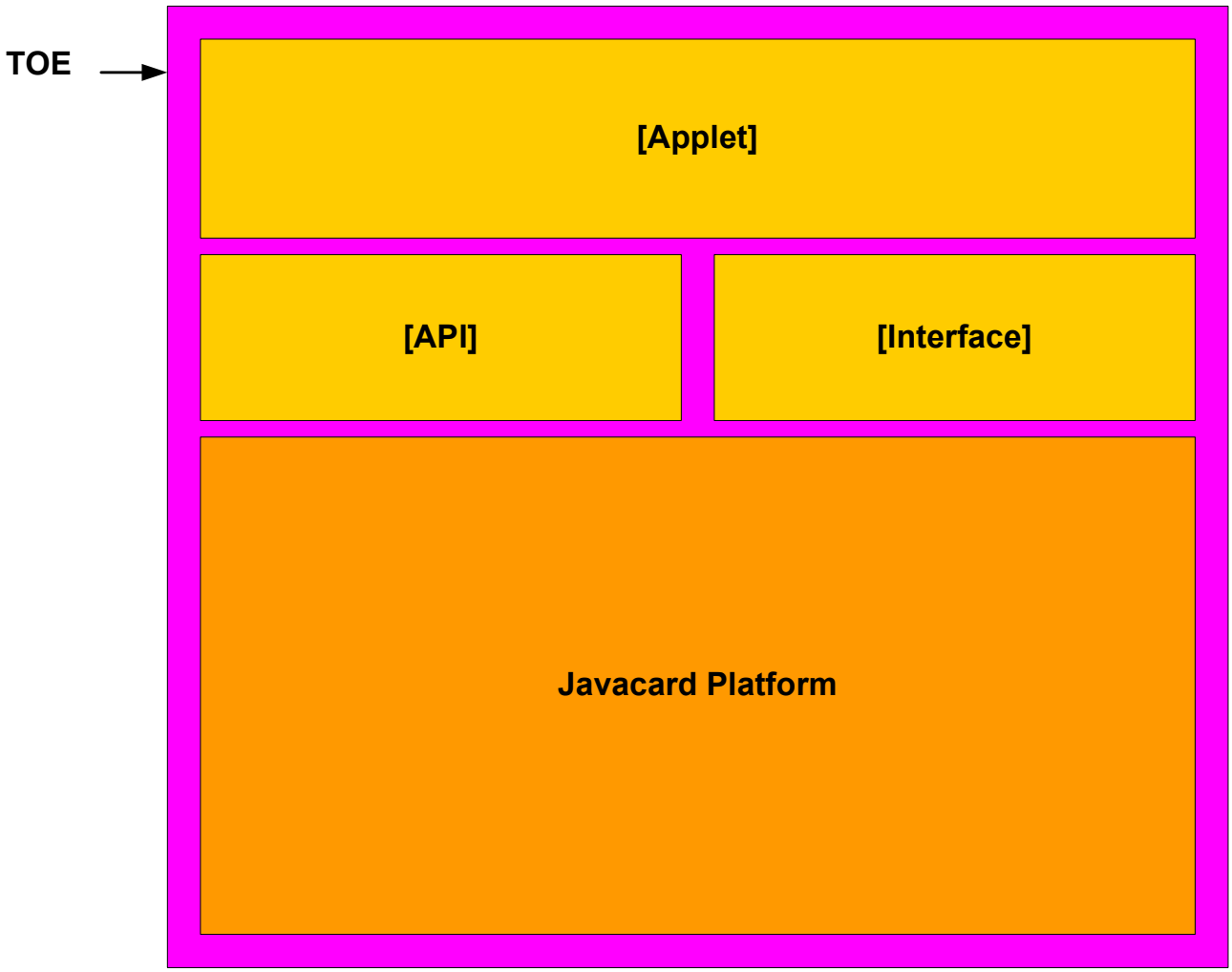
2.1.3.1 Physical overview

Once constructed, the TOE is a bare microchip with its external interfaces for communication.

It may be used on several physical medium

- within an inlay, or eCover
- in a plastic card
- within a USB key
- ….

The physical medium on which the microchip is mounted is not part of the target of evaluation



Limits of the TOE

2.1.4 Usage and major security features of the TOE

The TOE intended usage is to be used as a "secure signature creation device" of type 2 or 3, with respect to the European regulation EU/1999/93.
Within the framework described by [**SSCD2**] and [**SSCD3**], the TOE enables

- To perform qualified signature
- to authenticate the cardholder based on a RAD verification
- to authenticate one (or several) administrator(s) of the TOE, that may have special rights to administrate the **SCD** and **SVD** (generation, import), using either symmetric and/or asymmetric mechanisms or PIN verification
- to establish a 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 and/or asymmetric mechanisms

The scope of [**SSCD2**] and [**SSCD3**] is extended in several ways:

- **A super Administrator** has special rights to administrate the signature creation function, the mode of communication, and the type of cryptographic mechanisms to use.
- **The TOE may hold more than one SCD**. 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 according to the access rules required.**
- **RAD may be created at any time according to the access rules required.**
- **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.
- **eServices features are added,** enabling the cardholder to perform C/S authentication, Encryption key decipherment….
- **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 security functions the TOE provides are the following:

- **SF.PIN_MGT**: Management of the PIN. The TOE enable to create, set, change, reset the PIN both trought APDU commands or by Shared interfaces. In any case, the same security policy is applied.
- **SF.SIG** : Management of electronic signature according to the security requirement of [**SSCD2**] and [**SSCD3**]
- **SF.DEV_AUTH**: provision of cryptographic means to perform mutual authentication with remote entities such as the SCA, the CGA, the SSCD type 1 and initiate a trusted channel with them. It may use symmetric and asymmetric scheme.
- **SF.ADM_AUTH**: provision of cryptographic means to perform authentication of external entities to grant them some administration rights (on the TOE, personalization rights, on the SCD management…). It may use symmetric and asymmetric scheme.
- **SF.SM** : provision of cryptographic mechanisms to ensure a trusted channel with remote entities such as the **SCA**, the **CGA**, the **SSCD type 1**
- **SF.KEY_MGT**: provision of the keys management. It enables to create, import and generate the SCD and SVD, to export the SVD. It manages as well the authentications and the eServices keys stored in the TOE and enable their import, export and generation.
- **SF.CONF**: provides configuration management of the TOE. It enables to activate/deactivate the use of hash off card for signature computation, the use of symmetric and/or asymmetric authentication schemes, and the ability to communicate in contactless mode.
- **SF.ESERVICE**: provision of eServices. The TOE enables to perform C/S authentication, encryption key decipherment and certificate verification.
- **SF.EAVESDROPPING_PROTECTION**: Enforcement of the eavesdropping protection in contactless mode. When used in contactless mode, the TOE applies a restrictive security policy ensuring the sensitive data exchanged can not be read or sent by an unauthenticated entity.
- **SF.SAFESTATE_MGT** : Insurance of a safe state. The TOE always remains in a safe state, ensuring the protection of all the assets it contains.
- **SF.PHYS**: physical protection. The TOE provides protection against tampering and the assets it stores can not be retrieved or altered by physical manipulation

The TOE is compliant with the specification [**IASECC**] and may be used for various applications 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 platform, this embedded software may be used

- in contact mode (T=0 and/or T=1 protocol)
- in contactless protocol (T=CL)
- in USB protocol

2.2 Target Of Evaluation Reference

The TOE is identified as follows:

TOE name (commercial name)	IAS ECC v1.0.1 on ID-One™ Cosmo V7.0.1-n R2 Card (Standard and Standard Dual)
Software Identification	Javacard applet : "6179" Javacard platform mask = "7101"
Guidance document for preparation	FQR 110 5171 Ed7 - AGD_PRE
Guidance document for use	FQR 110 5170 Ed5 - AGD_OPE
Guidance document for preparation of PLATFORM	FQR 110 6407 Ed2 - ID-One Cosmo V7.0.1-n R2.0 - Pre-Perso Guide
Guidance document for operational user of PLATFORM	FQR 110 6408 Ed2 - ID-One Cosmo V7.0.1-n R2.0 - Reference Guide
Identification of the underlying IC	P5CD081, P5CC081
Reference of the CC certificates of the underlying IC	BSI-DSZ-CC-0555-2009, November 10th 2009

2.3 Description of the embedded software

2.3.1 Description of data structure

The IAS ECC application manages two types of structures:

- The File, compliant with [ISO7816-4]
- The Security Data Objects, which are secure container storing cryptographic data (PINs, Keys,….)

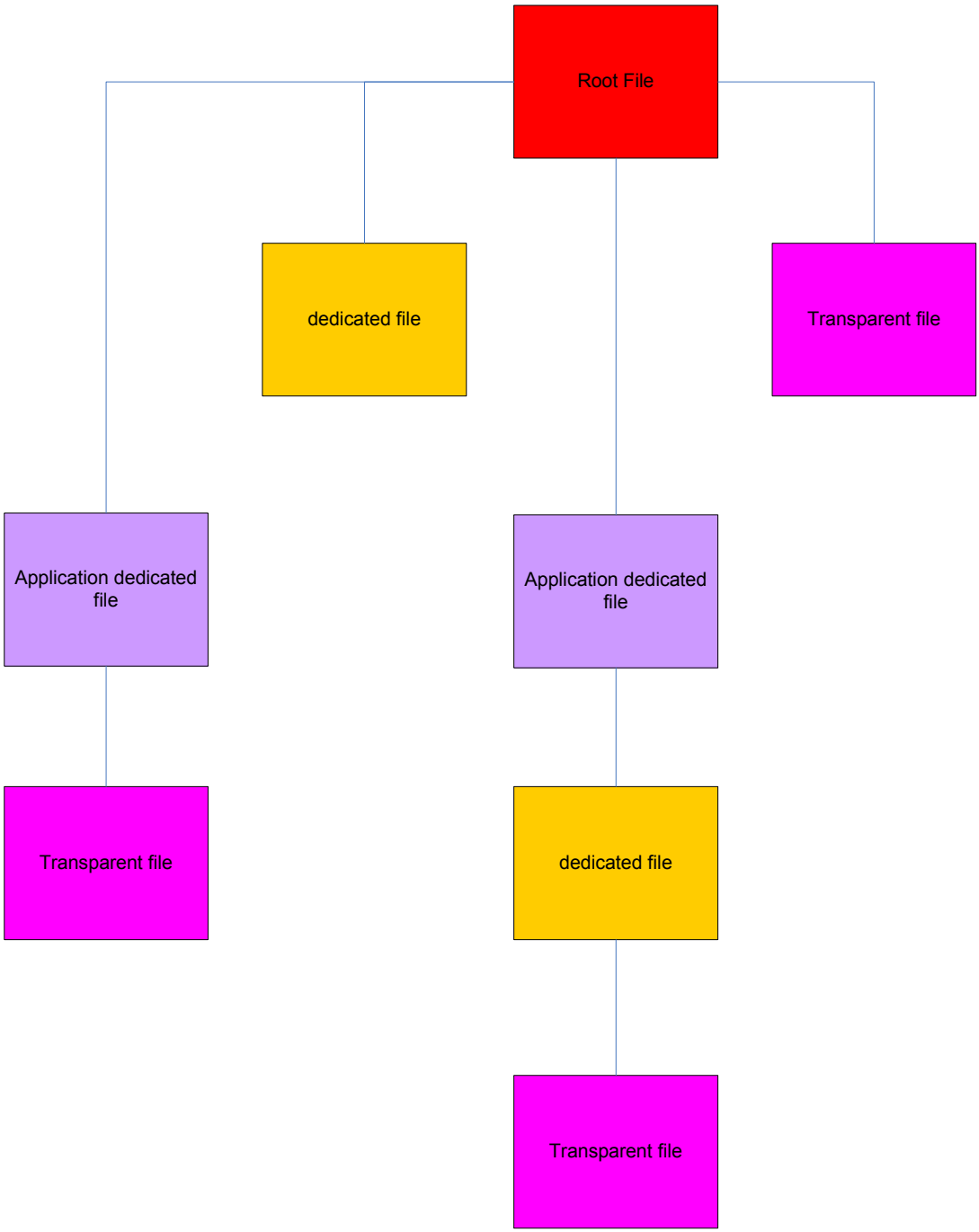
2.3.1.1 File and File System

The IAS ECC Application handles the following type of file (described in [ISO7816-4]):

- **Transparent File** - EF
- **Application Dedicated File** - ADF
- **Dedicated File** - DF

All these files are organized within a so called **File System**. It represents the hierarchy between all the files. This Structure is compliant with [ISO7816-4].

At the top of the structure stands the Root, it is the default selected file at reset. Under the Root, are located the Application Dedicated File.



Example of FileSystem Structure

The ADF and the Root may be selected by Application Identifier (**AID**) or by File identifier (**FID**).

The Root, as well as each ADF and DF, may contain up to 255 files (EF or DF).

The Application enables to

- create, delete, activate, deactivate terminate all type of file (except the Application dedicated file) to update the File System
- read, update, resize any transparent file (EF)
- Move within the File Structure by use of file selection.

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

- Access conditions
- File identifier
- Location within the File System
- Size (for transparent file)

All the action to be performed on file is fully described in [IASECC].

2.3.1.2 Security Environment

The IAS ECC Application handles Security Environments. Three types of Security Environment may be identified:

- **Static Security Environment** - SSE
- **Static Security Environment for Security Policies** – SSESP
- **Current Security Environment** - CSE

Basically a security environment contains several couple of cryptographic data. Each cryptographic data contains:

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

These cryptographic data may be used

- to set up a ready to use cryptographic context to perform a cryptographic operation (for signature, for C/S authentication,…). It is the case of **SSE**
- to define an access condition to fulfil: 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 the **SSESP**
- to define the current cryptographic context to apply to realize a given service. It is the case of the **CSE.** In particular, the CSE may be initialized from a SSE

The **SSESP** and **SSE** are attributes of the ADF and are stored in security Data Objects located within an Application dedicated file (ADF)

The **CSE** is unique for the TOE at any moment

2.3.1.3 Security data Objects

The IAS ECC Application handles as well cryptographic data objects, called Security Data Objects (**SDO**), dedicated to store the keys, the PIN, the Diffie Hellmann parameters and the Security Environments, as well as their attributes. The following types of SDO exist

- **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 Security Environment** contains a Security Environment
- **SDO Symmetric Key Set** contains a Symmetric Key Set
- **SDO Diffie Hellmann parameters** contains a set of Diffie Helmann Domain parameters

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

The Application 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 Public Key** may be used to verify a certificate
- **SDO RSA Private Key** may be used to sign, perform a C/S authentication or decrypt a cryptogram
- **SDO Security Environment** may be changed, reset, verified
- **SDO Symmetric Key Set** may be used to verify an external authentication or to perform a mutual authentication and establish a trusted channel.
- **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
- Content (Key, PIN or Diffie Hellman Parameters)
- Usage counter and tries counter
- Algorithm to be used

All the action to be performed on file is fully described in [IASECC].

2.3.2 Access Control Management

One of the Core features of IAS ECC is to provide access condition management on any access mode of any objects it handles:

- Files
- Security Data Objects

Access condition may be assigned to access mode on any of these objects.

The **Access conditions** encoding is the compact encoding described in [ISO7816-4], enhanced as described in [IASECC]. It relies on access rules encoded by means on **Access Mode Bytes** (AMB) and **Security Conditions Bytes** (SCB) described in [ISO7816-4] and [IASECC].

Prior to any operation, the application checks the requested access rights are fulfilled.

Basically, the Access condition is granted if the security conditions are fulfilled.

Any access condition to fulfil is a combination of security conditions based on identified keys/PIN/secrets:

- User Authentication (by PIN). May be used to authenticate the cardholder or a remote administrator.
- Authentication of a remote administrator
- Mutual authentication with a remote IT
- Communication protected in integrity and confidentiality

2.3.3 Authentication of entities

The IAS ECC application enables to authenticate several entities to grant them some rights:

- User Authentication (by PIN). May be used to authenticate the cardholder or a remote administrator.
- Authentication of a remote administrator (based on symmetric or asymmetric scheme)
- Mutual authentication with a remote IT and establishment of a trusted channel protected in integrity and confidentiality (based on symmetric or asymmetric scheme)
- Personalization Agent authentication (for the phase 6)
- TOE Administrator authentication (in phase 7)

These features of authentication are key factor as they are needed to grant access to resources (Files or SDO) the IAS ECC application holds.

2.3.4 eServices

The IAS ECC application offers as well eServices features:

- **C/S authentication**: this feature enables to authenticate the TOE on behalf of the cardholder's PC to a remote web server.
- **Digital signature**: this feature enables the cardholder to electronically signs documents. The signature may be either advanced or qualified (compliant with [SSCD2] and [SSCD3]).
- **Encryption key decipherment**: this feature enables the cardholder to store secret data on an electronic vault. The key needed to decipher the key encrypting these data is securely stored in the TOE. The cardholder's PC sends the encrypted encryption key to the TOE to get the plain encryption key.
- **Certificate verification:** this feature enables the TOE to verify a certificate issued by a certification authority the TOE trusts. The trust is established by the transfer to the TOE of a public RSA key of an authority certified by an authority whose public key is present in the TOE (either permanently stored, either imported through a certificate). This feature is used when the authentication key of a remote entity is certified by a Root certification Authority (RCA)

2.3.5 Administration of the TOE

The IAS ECC application offers administration services. Upon successful authentication, the TOE Administrator may modify the following attributes

- **Communication medium**: the administrator may restrict the ability to communicate with the TOE in contact and/or contactless mode. If the TOE is to be used in contactless mode, the TOE issuer shall ensure the security policy applied to files and SDO is relevant. In particular, there should not be any free readable data that could be used to track the holder, and any sensitive data shall be transmitted through a trusted channel ensuring protection against eavesdropping.

- **Hashing method to be used for digital signature**: the administrator may restrict the ability to perform electronic signature (advanced or qualified) on DTBS-representation partly computed by the TOE. In such case, the digital signature will only be done with last round of data hashing done on the TOE.
- **Authentication mechanism to be used**: the administrator may restrict the cryptographic means to be used by the TOE to authenticate remote entities (Administrator or Remote IT): either symmetric and/or asymmetric cryptography.
- **Identification of the TOE** : the administrator is entitled to identify the TOE

2.3.6 Single Sign on feature (SSO)

The IAS ECC application may behave as a Single Sign on (SSO). It provides access points to any other applet willing to use a PIN stored in the Root. In particular it is possible to:

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

This feature is very convenient when the PIN(s) will be shared with a legacy application

Even though the IAS ECC application offers these entry points, it does still perform access control it the same way it does when it receives incoming APDU to manage a PIN. The access conditions on the PINs that are accessed by these entry points are still enforced.

2.3.7 Scope of evaluation

The scope of evaluation encompasses all the features of the TOE. The File System management is out of the scope of the evaluation, even though the access control management (common to SDO and File) is covered.

2.4 Intended Usage

The TOE intended usage is to be used as a "secure signature creation device" of type 2 or 3, with respect to the European regulation EU/1999/93.
Within the framework described by [**SSCD2**] and [**SSCD3**], the TOE enables

- To perform electronic qualified signature
- to authenticate the cardholder based on a RAD verification
- to authenticate one (or several) administrator(s) of the TOE, that may have special rights to administrate the **SCD** and **SVD** (generation, import), using either symmetric and/or asymmetric mechanisms or PIN verification
- to establish a 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 and/or asymmetric mechanisms

The scope of [**SSCD2**] and [**SSCD3**] is extended in several ways:

- **A super Administrator** has special rights to administrate the signature creation function, the mode of communication, and the type of cryptographic mechanisms to use.

- **The TOE may hold more than one SCD**. 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 according to the access rules required.**
- **RAD may be created at any time according to the access rules required.**
- **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.
- **eServices features are added,** enabling the cardholder to perform C/S authentication, Encryption key decipherment….
- **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 is compliant with the specification [IASECC] and may be used for various applications requiring qualified signature:

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

2.5 Life Cycle

With respect to the Life cycle envisioned in [PP9911], seven different phases may be sorted out.

The life cycle of the composite TOE may be depicted as follows:

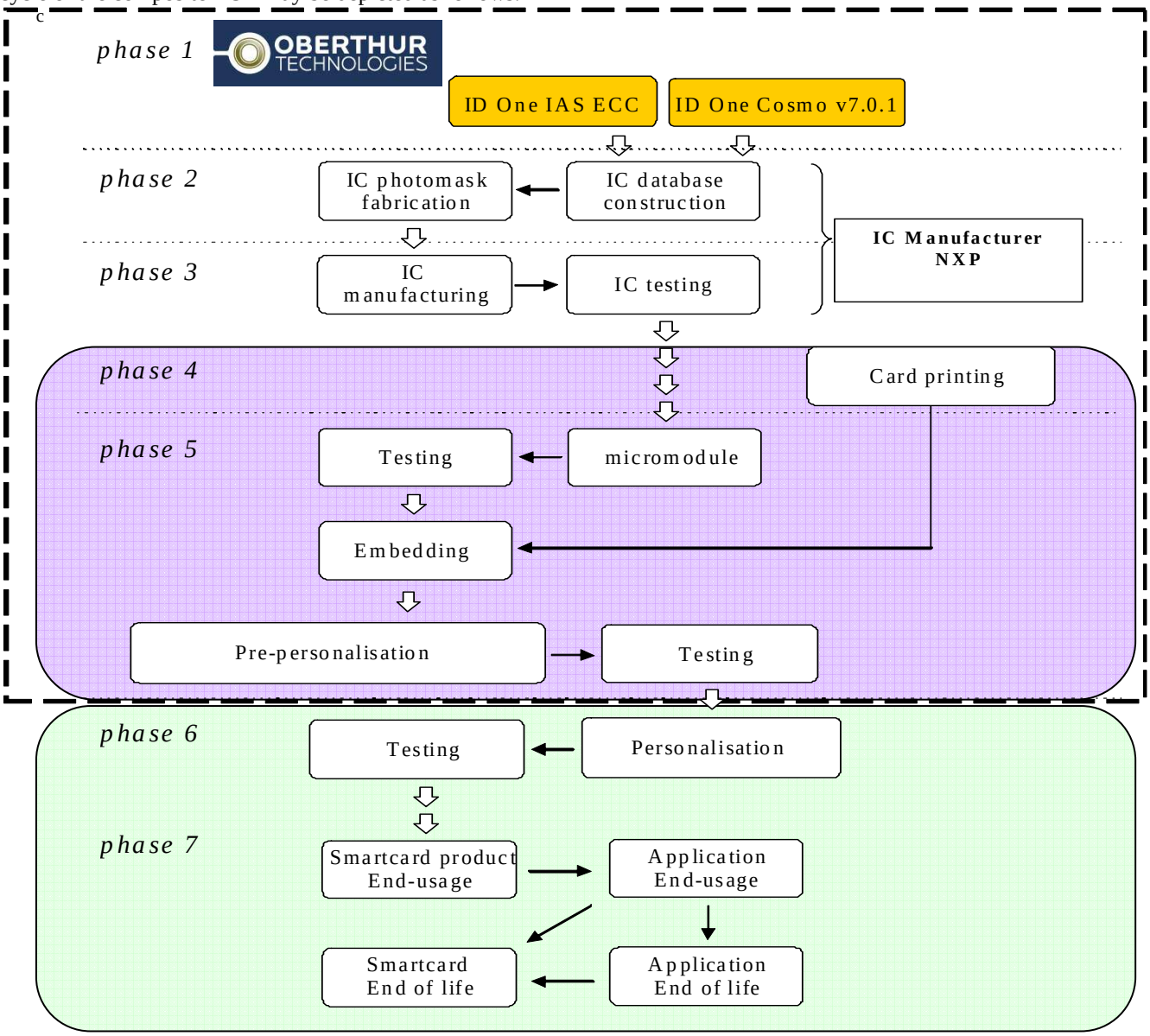


Figure 1 : life cycle state of the composite TOE

2.5.1 Description of the TOE Environment

The TOE environment may be spitted into two different parts:

- The **Development environment**, in which the parts of TOE are designed, tested and manufactured.
- The **Production environment**, in which the TOE is under construction. The security requirements of the javacard platform (JOP) are fulfilled and assurance levels are met.
- The **Operational environment**, in which the TOE is self protected and can be used as stated (personalized and used). Once personalized according to [**AGD_PRE**], the TOE is constructed: the security requirements of the TOE are fulfilled and the assurance levels are met.

2.5.2 Development environment

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

- the javacard platform components;
- the javacard packages (applet and interface);

2.5.2.1 Software development (phase 1)

This development environment of the Javacard Applet and javacard platform (JOP) is enforced by **OBERTHUR TECHNOLOGIES**.

The confidentiality and integrity of the cap files and of the javacard platform is covered by the evaluation of the development premises of **OBERTHUR TECHNOLOGIES**.

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

- Access control to OBERTHUR TECHNOLOGIES offices and sensitive areas.
- Access to development data through the use of a secure computer system to design, implement and test software

At the end of this phase, the javacard packages together with the javacard platform are transferred to the chip manufacturer in order to be masked on silicium.

At the end of this phase 1, the javacard packages are protected in integrity and confidentiality.

This phase takes place in **OBERTHUR TECHNOLOGIES** premises and is covered by [ALC]

2.5.2.2 Hardware development (Phase 2)

In this phase, the javacard platform (JOP) is being built.

The javacard packages are stored in the ROM code of the javacard platform (JOP).

This phase takes place at the manufacturing site of the silicium provider and is covered by [ALC].

The confidentiality and integrity of the javacard packages and javacard platform is covered by the evaluation of the development premises of the silicium manufacturer (see [**PLATFORM**])

2.5.3 Production environment

The production environment encompasses the environments in which the TOE is prepared.

It corresponds to the following steps:

- Software is engraved in the silicium to get the javacard platform (JOP).
- The chip is mounted on a physical layout (card, USB token...)
- The javacard platform is prepersonalized
- The javacard platform is personalized
- The application is instantiated

2.5.3.1 Javacard platform manufacturing (phase 3)

In this phase, the javacard platform (JOP) is self protected. The javacard packages are self protected as they are present in the ROM code of the javacard platform (JOP)

This phase takes place at the manufacturing site of the silicium provider and is covered by [ALC].

At the end of phase 3, the javacard packages are self protected: their integrity and confidentiality is ensured as they are present in the ROM code of the javacard platform

2.5.3.2 Javacard platform (JOP) packaging and initialization (phase 4)

The Javacard platform (JOP) is under the control of the **Manufacturing Agent**. This subject is in charge of the Javacard platform (JOP) packaging.
This phase takes place in the manufacturing site of Vitré (France – 35) and is covered by [ALC].

2.5.3.3 Javacard platform (JOP) pre-personnnalization (phase 5)

The Javacard platform (JOP) is under the control of the **Manufacturing Agent**.

This phase is done in the manufacturing site of Vitré (France – 35) and is covered by [ALC].

During this phase, the javacard platform is pre-personnalized and personalized by the **Manufacturing Agent.** This subject shall be authenticated prior to any action on the javacard platform.
The main operations performed by the **Manufacturing Agent** during this phase are the following:

- Configuration of the javacard platform (ATR,..)
- Configuration and activation of the Card Manager
- Loading of the keys of the Card Manager
- Locking of the javacard platform (to ban any applet loading)

Moreover, the manufacturing site ensures a secure management of the keys used to prepare the TOE. The procedures, the security measures and the IT infrastructure ensure the integrity and authenticity of the keys.

At the end of this phase, the TOE is produced and self protected.

At the end of this phase, the TOE is delivered together with its personalisation keys (keys of the Card Manager).

The point of delivery is the end of phase 5

2.5.4 Operational environment

The operational environment encompasses the environments in which the TOE is constructed. It corresponds to the following steps:

- Personalization of the IAS ECC Application
- Use of the IAS ECC Application

2.5.4.1 TOE personalization (phase 6)

The TOE is under the control of the **Personalization Agent** in charge of personalizing the Applet. This subject shall be authenticated prior to any action on the Javacard platform.

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

During this phase, the applet is personalized according to [**AGD_PRE**]: 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

2.5.4.2 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**.
During this phase, the TOE may be used both in contact and/or contactless mode.

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

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

Life cycle phase	Environment	Covered by
Phase 1	**Development**	**ALC**
Phase 2	**Development**	**ALC**
Phase 3	**Development**	**ALC**
Phase 4	**Production of TOE**	**ALC**
Phase 5	**Production of TOE**	**ALC**
Point of delivery of the TOE		
TOE is self protected		
Phase 6	**Operational**	**AGD_OPE [PLATFORM] AGD_PRE**
TOE is constructed		
Phase 7	**Operational**	**AGD_OPE [PLATFORM] AGD_OPE**

The point of delivery of the TOE is the end of phase 5. The TOE is delivered with its personalisation key (keys of the Card Manager), required to use it in phase 6 and 7.

2.5.6 State of the TOE depending on the phase

This chapter describes when the TOE is self protected

Life cycle phase	State of the TOE at the end of the phase
Phase 1	In construction
Phase 2	In construction
Phase 3	In construction
Phase 4	In construction
Phase 5	In construction and self protected
Point of delivery of the TOE	
Phase 6	Constructed and self protected
Phase 7	Constructed and self protected

2.5.7 Mapping with the life cycle and Subjects described in [SSCD2] and [SSCD3]

The life cycle of the TOE is based on the one described in [PP9911]. This chapter focuses on mapping it to the one described in [SSCD2] and [SSCD3].

Life cycle phase of the TOE	Life cycle phase with respect to [SSCD2] and [SSCD3]
Phase 1	Design
Phase 2	Fabrication
Phase 3	Fabrication
Phase 4	N/A
Phase 5	Loading of application data
Point of delivery of the TOE	
TOE is self protected	
Phase 6	Personalization
TOE is constructed	
Phase 7	Usage Destruction

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

Life cycle phase of the TOE	Subject interacting with the TOE
Phase 1	OBERTHUR TECHNOLOGIES
Phase 2	OBERTHUR TECHNOLOGIES
Phase 3	OBERTHUR TECHNOLOGIES
Phase 4	Manufacturing Agent (OBERTHUR TECHNOLOGIES) Offcard
Phase 5	Manufacturing Agent (OBERTHUR TECHNOLOGIES) Offcard
Point of delivery of the TOE	
TOE is self protected	
Phase 6	Personalization Agent Offcard
TOE is constructed	
Phase 7	User (Signatory or Administrator) TOE_Administrator Offcard

2.5.8 Presentation of the different subjects interacting with the TOE

In phase 1 up to 3, the TOE is under the control of **OBERTHUR TECHNOLOGIES.** It is in charge of designing and manufacturing the TOE.

In phase 4, the TOE is under the control of **OBERTHUR TECHNOLOGIES** which acts as the **Manufacturing Agent**. It is in charge of loading data within the TOE to make it operational. During this phase, the **Manufacturing Agent** ensures a sufficient level of security.

In phase 5, the TOE is under the control of **OBERTHUR TECHNOLOGIES** which acts as the **Manufacturing Agent**. Once the phase 5 is successfully completed, the TOE is delivered together with its personalisation key.

In phase 6, the TOE is under the control of the **Personalization Agent**. It is in charge of loading data within the TOE to make it operational. During these phase, the Personalization agent ensures a sufficient level of security.
In particular, in phase 6, the **Personalization Agent** may:

- Create and load the **RAD**
- Create and load the **SCD/SVD**
- Create and generate the **SCD/SVD**
- Export the **SVD**
- Create the security policies to be applied to files and objects

The **Personalization Agent** behaves as the **Administrator** and **Signatory** for the key management features for this phase

In phase 7, the TOE is under the control of the **Signatory** and **Administrator**.
In particular, the **Administrator** may:

- Create the **RAD**
- Create the **SCD/SVD**
- Create the **SCD/SVD**

The **Signatory** or the **Administrator** may:

- Load the **RAD**
- Load the **SCD/SVD**
- Generate the **SCD/SVD**
- Export the **SVD**

and **Signatory** may

- sign **DTBS/DTBS-representation**
- change its **RAD**

During phase 7, another entity may manage the TOE: **TOE_Administrator.** It is in charge of managing some features of the TOE such as:

- Allowing signing DTBS representation computed off card
- Allowing the authentication of remote IT or administrator by means of symmetric and/or asymmetric scheme
- Allowing to restrict the contact and/or contactless interface for communication

3 Target Of Evaluation Security Environment

3.1 Remote IT entity

The following remote IT entity may interact with the TOE

Remote IT	Description
SCA	This remote IT is in charge of sending the **DTBS/DTBS** representation to the **TOE** This remote IT is present in phase 7 of the life cycle of the TOE
CGA	This remote IT is in charge of issuing a (qualified) certificate as well as a link enabling to find the (qualified) certificate matching the **SCD**. This remote IT is present in phase 6 and 7 of the life cycle of the TOE
SSCD type 1	This remote IT is in charge of importing a **SCD/SVD** pair on the TOE as well as a link enabling to find the (qualified) certificate matching the **SCD**. This remote IT is present in phase 6 and 7 of the life cycle of the TOE
IFD	In case the contactless is used to establish communication with the TOE, the communication shall be established with an **IFD**, ensuring the communications are protected by a secure channel. The IFD is in charge as well the remote entity interacting with the TOE in case eServices are used This entity shall be recognized by the TOE issuer. The **IFD** is considered as being part of the remote IT (**CGA**, **SSCD type 1** and **SCA**) with which the TOE wants to communicate in a secure manner. This remote IT is present in phase 7 of the life cycle of the TOE
HI	Human interface used by local users to enter **RAD** or **VAD**. The data entered are transmitted to the TOE via a trusted path

It is very important to stress to these Remote IT are just an abstract point of view. Depending on the use case, the following situation may arise

- Several Remote IT are realized by a single entity (e.g. SCA, CGA and SSCD type 1)

- A remote IT is as well a subject (e.g. the SCA is the Administrator, the CGA is the TOE_Administrator...)

Moreover, in phase 6, the SSCD type 1 remote IT is tightly linked to the subject operating during this phase (i.e. **S.Personnalizer**). The SSCD securely transmits the SCD to the TOE by mean of an encryption key. The encryption key is deduced from diversifying data agreed during the authentication of the "**Personalizer**" with the TOE. Therefore, in phase 6, the import of SCD from a SSCD type 1 requires **S.Personnalizer** to be authenticated in a first step.

The Human interface (**HI**) used to enter the PIN is considered as being part of the **SCA**, **CGA** or **SSCD**, depending on the case. It benefits from the trusted channel between the TOE and the **SCA**, or the **SSCD type 1** or the **CGA** to transmit the **RAD** or **VAD** to the TOE.

3.2 Subjects

The following Subject interact with the TOE

Subject	Description
S.User	End User of the TOE that can be identified as **S.Admin** or **S.Signatory** It is named **User**
S.Admin	User(s) who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions This User may operate during phase 7. Depending on the use case envisioned, the subject(s) **S.SCA**, **S.CGA**, **S.SSCD** or **S.IFD** may be the subject **S.Admin**. It is named **Administrator**
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents It is named **Signatory**
S.TOE_Admin	User who is in charge to perform the configuration management of the TOE It is named **TOE_Administrator**
S.Personalizer	User who operates in Phase 6 of the life cycle. It is in charge to perform the TOE initialization and TOE personalization It is named **Personalizer**
S.DAP_Admin	User who operates as soon as the DAP feature is activated on the javacard platform: in phase 6 (optionally) & 7 of the life cycle. It holds the DAP signature key and is in charge of controling the applet to be loaded on the javacard platform. It is named **DAP_Admin**

S.Manufacturer	User who operates in Phase 5. It is in charge of physically building the javacard platform, e.g. mounting the chip on the antenna physically building the card performing the graphical personalization and performing some basic prepersonalisation operation it is only entitled to perform The action of this subject is covered by [PLATFORM] It is named **Manufacturer**
S.SCA	It is the **SCA** seen as a subject interacting with the TOE. As such, depending on the use case, it might belong to the category S.Admin. It is named **SCA**
S.CGA	It is the **CGA** seen as a subject interacting with the TOE. As such, depending on the use case, it might belong to the category S.Admin. It is named **CGA**
S.SSCD	It is the **SSCD** seen as a subject interacting with the TOE. As such, depending on the use case, it might belong to the category S.Admin. It is named **SSCD**
S.IFD	It is the **IFD** seen as a subject interacting with the TOE. As such, depending on the use case, it might belong to the category S.Admin. It is named **IFD**
S.Offcard	Attacker as being a human or process acting on his behalf being located outside the TOE. The main goal of the attacker is to access the **SCD** or to false the electronic signature. The attacker has a high attack potential and knows no secret

3.3 User data

The following user data are managed by the TOE

User Data	Description
D.DTBS	**DTBS** and **DTBS representation** ; set of data or its representation which is intended to be signed
D.VAD	**VAD** : **PIN** code data entered by the End User (**S.Signatory**

	or **S.Admin**) to authenticate itself or to perform a signature operation
D.AUTH_CRYPTOGRAM	Authentication data used to authenticate subjects such as **S.Admin** **S.TOE_Admin.** **S.Personalizer** **S.SCA** **S.CGA** **S.SSCD** **S.IFD** It is a cryptogram sent by the outside the TOE checks with **D.AUTH_KEYS**
D.SIGNATURE	Electronic signature (Unforgeabilty of electronic signatures must be assured)
D.DTBS	**DTBS** and **DTBS representation** stored within the TOE; set of data or its representation which is intended to be signed
D.RAD	**RAD** : Reference PIN code authentication data used to authenticate the End User (S.Signatory or S.Admin) There might be several RAD within the TOE
D.SCD	**SCD :** private key used to perform an electronic signature operation There might be several SCD within the TOE
D.SVD	**SVD :**public key linked to the SCD and used to perform an electronic signature verification There might be several SVD within the TOE
D.TOE_SerialNumber	Serial number of the TOE. This data is required to perform device and external authentication. It is an **IDENTIFICATION_DATA**
D.AUTH_KEYS	Group of keys stored on the TOE used to perform a mutual authentication with subjects such as : **S.Admin** **S.TOE_Admin**. **S.Personalizer** **S.SCA** **S.CGA** **S.SSCD** **S.IFD** Or used to authenticate external entities such as SSCD type 1 used to import a SCD SCA for signature creation CGA for certificate generation. IFD in case of contactless communication **These keys are secret data shared by the TOE and the**

	other entity (symmetric keys)
D.ESERVICES_KEYS	Group of keys/Parameters stored on the TOE used to perform eServices such as Certificate verification – first key stored in the TOE Key Agreement Domain parameters Key Decryption keys Some are public : Certificate verification – first key stored in the TOE Key Agreement Domain parameters Public portion of key decryption key Some shall remain secret Private key of key decryption key
D.TOE_AUTH_PUBLIC_KEYS	Group of public key matching the private authentication key of the TOE
D.TOE_AUTH_PRIVATE_KEYS	Group of authentication private key(s) of the TOE. The authentication mechanism involved are C/S authentication DAPP Internal authentication
D.IDENTIFICATION_DATA	Data or group of data stored in the TOE, which may be used to uniquely identify the TOE and therefore the TOE holder.
User Data	**Description**
D.DTBS	**DTBS** and **DTBS representation** ; set of data or its representation which is intended to be signed

3.4 TSF data

The following TSF data are managed by the TOE

TSF Data	Description
D.APPLI	The quality of the signature creation application (IAS ECC) must be maintained so that it can participate to the legal validity of electronic signature
D.SCD_ID	Identifier of the **SCD**. In order to identify the matching certificate, each **SCD** shall be associated with an identifier
D.EPHEMERAL_KEYS	The ephemeral key extracted from a certificate (**CVC**). It may be used to Verify another certificate Authenticate a subject or a remote IT entity The ephemeral key is a public portion of a RSA key pair. It can only be extracted with a trusted key, i.e. a key whose issuer is trusted (the public key is either stored in the TOE or extracted from another certificate).

	This category key is said to be ephemeral as it is not stored in the TOE but has to be directly used to verify another certificate or authenticate a subject or a remote IT In case of authentication protocol relying on asymmetric scheme, it is used to authenticate entities such as **a certificate issuer** **S.Admin** **S.SCA** **S.CGA** **S.SSCD** **S.IFD** Or used to authenticate external entities such as **SSCD type 1** used to import a **SCD** **SCA** for signature creation **CGA** for certificate generation. **IFD** in case of contactless communication
D.STATE	Life Cycle state of the TOE. Its value is either "**SELECTABLE**" (in phase 6) or "**PERSONALIZED**". (in phase 7)
D.Medium	Attribute of the TOE indicating which communication medium can be used (contact and/or contactless)
D.HashOffCard	Attribute of the TOE indicating if qualified signature can be performed on a hash computed off card
D.SymAuthMechanisms	Attribute of the TOE indicating if authentication mechanisms based on symmetric scheme can be used
D.AsymAuthMechanisms	Attribute of the TOE indicating if authentication mechanisms based on asymmetric scheme can be used
D.SM_DATA	Keys and data used by the TOE to establish and manage a trusted channel in phase 7. These data ensure identification of both parties (TOE and the entity) and the protection in integrity and confidentiality of data exchanged.

3.5 Assumption

3.5.1 Standard Assumption

A.CGA	**Trustworthy certification-generation application**

The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced 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.SCD_Generate	Trustworthy SCD/SVD generation

If a party other than the signatory generates the SCD/SVD-pair of a signatory, then

(a) this party will use a SSCD for SCD/SVD-generation,

(b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and

(c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory.

(d) The generation of the SCD/SVD is invoked by authorised users only

(e) The SSCD Type1 ensures the authenticity of the SVD it has created and exported

3.5.2 Complementary Assumption

N/A

3.6 Threats

3.6.1 Standard threats

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 addresses all the assets.

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 release 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.Sig_Forgery	Forgery of the electronic signature

An attacker forges the signed data object maybe together with its electronic signature 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.

T.Sig_Repud	Repudiation of signatures

If an attacker can successfully threaten any of the assets, then the non repudiation of the electronic signature is compromised. The signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.

T.SVD_Forgery	Forgery of the signature-verification data

An attacker forges the SVD presented by the TOE. This result in loss of SVD integrity in the certificate of the signatory.

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.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.

3.6.2 Complementary threats

T.TOE_ID_Contactless	Identification of the TOE

When the TOE is configured to be used in contactless mode, an attacker tries to trace the movement of the TOE by identifying it remotely by establishing or listening a communication through the contactless communication interface.

T.Skimming_Contactless	Skimming of the TOE in contactless

When the TOE is configured to be used in contactless mode, an attacker imitates the device to retrieve data from the TOE via the contact less communication channel of the TOE.

T.Eavesdropping_Contactless	Eavesdropping of the communication between TOE and device

When the TOE is configured to be used in contactless mode, an attacker listens to the communication between the TOE and a device in order to retrieve sensitive data.

T.Key_Divulg	Storing ,copying, and releasing of a key stored in the TOE

An attacker can store, copy an authentication or eService key stored in the TOE outside the TOE. An authentication key may be either used to authenticate an external entity or the TOE, and may be symmetric or asymmetric. An attacker can release an authentication or eService key during generation, storage and use in the TOE.

T.Key_Derive	Derive a key

An attacker derives an authentication key (of the TOE or an external entity) or eService key 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.

T.TOE_PublicAuthKey_Forgery	Forgery of the public key of a TOE authentication key

An attacker forges the public key of a TOE authentication key presented by the TOE. This results in loss of the public key integrity in the authentication certificate of the TOE.

T.Authentication_Replay	Replay of an authentication of an external entity

An attacker retrieves by observation authentication data used by a third party during an authentication sequence. The attacker tries to replay this authentication sequence to grant access to the TOE.

3.7 Organizational security policies

3.7.1 Standard organizational security policies

P.CSP_QCert	Qualified certificate

The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alia 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 qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate and is created by a SSCD.

P.Sigy_SSCD	TOE as secure signature-creation device

The TOE stores the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

3.7.2 Complementary organizational security policies

P.EMSEC_Design	The TOE is designed to reduce the E.M emanation

The cryptographic computation, memory access, and software execution are implemented in such a way that they are not susceptible to leakage attacks

P.SecurityPolicy_Contactless	Security policy definition.

All the data that may be accessed in contactless mode and that would lead to unambiguously identify and track the TOE shall not be accessible in free mode. They shall be accessed upon successful authentication of the entity willing to access it. Moreover, the TOE shall enforce these data to be accessed through a communication channel protected in confidentiality (for the sole recipient) and ensuring the authentication of the sender. The subject in charge of creating these data that might be accessed in contactless mode (Administrator, Signatory, Personalizer) shall enforce this security policy.

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

P.ControlOfAppletToBeLoaded_Contactless	Control of the other applet that may be loaded on the javacard open platform

When the TOE is configured to be used in contactless mode, the **Manufacturing Agent** (for phase 5), the **Personalization Agent** (for phase 6), and the **DAP_Administrator** (for phase 6 & 7) shall ensure that any applet that is loaded on the javacard open platform does not enable to track/identify the TOE.

P.TOE_PublicAuthKey_Cert	Certificate for asymmetric TOE authentication keys

The TOE contains certificate(s) issued by a known entity ensuring its public key corresponding to its private key used for authentication is genuine.

P.TOE_Construction	Construction of the TOE by the Personnalization Agent

The recommendations indicated in [**AGD_PRE**] required to construct the TOE are correctly applied.

3.8 Security Objectives for the TOE

3.8.1 Standard security objectives of the TOE

OT.EMSEC_Design	Provide physical emanations security

Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.

OT.Lifecycle_Security	Lifecycle security

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-import or re-generation.

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.SCD_SVD_Corresp	Correspondence between SVD and SCD

The TOE shall ensure the correspondence between the SVD and the SCD. The TOE shall verify on demand the correspondence between the SCD stored in the TOE and the SVD if it has been sent to the TOE.

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.Tamper_ID	Tamper detection

The TOE provides system features that detect physical tampering of a system component, and use those features to limit security breaches.

OT.Tamper_Resistance	Tamper resistance

The TOE prevents or resists physical tampering with specified system devices and components.

OT.Init	SCD/SVD generation

The TOE provides security features to ensure that the generation of the SCD and the SVD is invoked by authorized users only.

OT.SCD_Unique	Uniqueness of the signature-creation data

The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible low.

OT.SCD_Transfer	Secure transfer of SCD between SSCD

The TOE shall ensure the confidentiality of the SCD transferred between SSCDs.

OT.DTBS_Integrity_TOE	Verification of the DTBS-representation integrity

The TOE shall verify that the DTBS-representation received from the SCA has not been altered in transit between the SCA and the TOE. The TOE itself shall ensure that the DTBS representation is not altered by the TOE as well. Note, that this does not conflict with the signature-creation process where the DTBS itself could be hashed by the TOE.

OT.Sigy_SigF	Signature generation function for the legitimate signatory only

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

OT.Sig_Secure	Cryptographic security of the electronic signature

The TOE generates electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the electronic signatures. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.

3.8.2 Complementary security objectives of the TOE

OT.Authentication_Secure	Secure authentication mechanisms

The TOE enables to create/erase authentication keys used to provide authentication mechanisms enabling to

- authenticate remote entities in order to grant them some access rights
- authenticate the TOE towards external entities, ensuring it is not cloned

The TOE generates and uses from remote entities authentication cryptogram that cannot be forged without knowledge of the authentication key through robust encryption techniques. The authentication key cannot be reconstructed using the authentication cryptogram. The cryptogram shall be resistant against these attacks, even when executed with a high attack potential. Moreover, the TOE uses freshly generated random in authentication protocols in order to avoid replay attacks.

OT.Privacy_Contactless	Privacy of sensitive data exchanged in contactless

When used in contactless, the TOE protects the access to sensitive data (identification data,..). It enforces the data to be sent from an authenticated device in a manner protected from disclosure, ensuring it can not be retrieved by an attacker. Moreover, any identification data can only be returned to successfully authenticated entities, in a way ensuring they are protected from disclosure and are issued by the TOE.

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.Key_Lifecycle_Security	Lifecycle security of the key(s) stored in the TOE

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide safe destruction techniques for the authentication keys (of the TOE and/or the external entities) and eServices keys it stores in case of erasure, re-import or re-generation.

OT.Key_Secrecy	Secrecy of the key(s) stored in the TOE

The secrecy of the authentication keys (of the TOE and/or the external entities) and eServices keys stored in the TOE is reasonably assured against attacks with a high attack potential.

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

The TOE shall ensure the cryptographic quality of the asymmetric 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.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** may be created, generated, imported or erased
- The **ESERVICES_KEYS**,**AUTH_KEYS**, **TOE_AUTH_PUBLIC_KEYS** and **TOE_AUTH_PRIVATE_KEYS** may be created, imported, generated or erased
- The RAD (s) may be created and loaded
- **SVD** may be exported
- **TOE_AUTH_PUBLIC_KEYS** may be exported

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

OT.eServices	Provision of eServices

The TOE provides eServices Mechanisms enabling to create, import, generate, export the matching public key and erase eServices keys. These keys are used to

- decrypt encryption keys
- authenticate the TOE
- verify CVC certificates

3.9 Security objectives for the Environment

3.9.1 Standard security objectives of the Environment

OE.SCD_SVD_Corresp	Correspondence between SVD and SCD

The SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSCD Type1 shall verify the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.

OE.SCD_Transfer	Secure transfer of SCD between SSCD

The SSCD Type1 shall ensure the confidentiality of the SCD transferred to the TOE. The SSCD Type1 shall prevent the export of a SCD that already has been used for signature generation by the SSCD Type2. The SCD shall be deleted from the SSCD Type1 whenever it is exported into the TOE.

OE.SCD_Unique	Uniqueness of the signature-creation data

The SSCD Type1 shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible low.

OE.CGA_QCert	**Generation of qualified certificates**

The CGA generates qualified certificates which include inter alia

(a) the name of the signatory controlling the TOE,

(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,

(c) the advanced signature of the CSP.

OE.SVD_Auth_CGA	**CGA verifies the authenticity of the SVD**

The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

OE.HI_VAD	**Protection of the VAD**

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.

OE.SCA_Data_Intend	**Data intended to be signed**

The SCA

(a) generates the DTBS-representation 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,

(b) sends the DTBS-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE

(c) attaches the signature produced by the TOE to the data or provides it separately.

3.9.2 Complementary security objectives of the Environment

OE.SecurityPolicy_Contactless	**Security policy definition.**

All the data that may be accessed in contactless mode and that would lead to unambiguously identify and track the TOE shall not be accessible in free mode. They shall be assigned a relevant security policy ensuring they can only be accessed by a successfully authenticated entity. Moreover, they shall only be transferred in a manner ensuring protection in confidentiality (can only be retrieved by the entitled recipient) and proving the authenticity of the sender.

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

OE.ControlOfAppletToBeLoaded_Contactless	**Control of the other applet that may be loaded on the javacard open platform**

Prior to any applet loading, the entity in charge of administrating the javacard open platform shall make sure the applet does not disclose identification data that may be used by an attacker to track the TOE in contactless mode (e.g. a static identifier in free access,…)

OE.AuthKey_Transfer	**Secure transfer of Authentication key(s) to the TOE**

The entity in charge of generating the authentication keys to be loaded in the TOE shall ensure the confidentiality of the key(s) transferred to the TOE.

OE.AuthKey_Unique	**Uniqueness of the authentication key(s)**

The entity in charge of generating the authentication keys to be loaded in the TOE shall ensure the cryptographic quality of the authentication key(s). The authentication key used for authentication can practically occur only once and, in case of a TOE authentication key cannot be reconstructed from its public portion. In that context 'practically occur once' means that the probability of equal keys is negligible low.

OE.TOE_PublicAuthKey_Transfer	**Secure transfer of Public Authentication key(s) of the TOE**

The entity in charge of generating the authentication certificate from the TOE's authentication public key generated in the TOE shall ensure the authenticity of this data when transferred from the TOE. This may be achieved by the retrieval of the public key according to certain rules imposed to the TOE holders.

OE.TOE_Construction	**Construction of the TOE by the Personnalization 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 [**AGD_PRE**]. These recommendations are required to construct the TOE

3.10 TOE Security functional requirements

3.10.1 FCS: CRYPTOGRAPHIC SUPPORT

3.10.1.1 FCS_CKM.1 Cryptographic key generation

FCS CKM.1.1 / RSA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***RSA key generation***] and specified cryptographic key sizes [***1024 bits or 1536 bits or 2048 bits***] that meet the [***ANSI X9.31***]

FCS CKM.1.1 / DES session keys

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***DES key generation***] and specified cryptographic key sizes [***128 bits***] that meet the [***IASECC***]

Refinement Note:

The hashing algorithm used by the TOE to generate the session keys from the Seed is the SHA-1 and SHA-256.

3.10.1.2 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 / SCD/SVD

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***].

Refinement:
This SFR applies to all asymmetric keys, whether it is a qualified signature key (SCD or SVD), a TOE authentication key (TOE_AUTH_PUBLIC_KEYS and TOE_AUTH_PRIVATE_KEYS), an eServices key (ESERVICES_KEYS except the Diffie Hellman Domain parameters).

Application note:
The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD is re-imported into the TOE.

FCS_CKM.4.1 / Symmetric 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***].

Application note:
The Symmetric DES key includes the keys used for the device authentication and the External Role authentication based on the symmetric scheme (both belonging to AUTH_KEYS) as well as the secure messaging session keys.
The destruction of the previous keys is mandatory when they are updated

3.10.1.3 FCS_COP Cryptographic operation

FCS_COP.1 Cryptographic operation

FCS_COP.1.1/ CORRESP

The TSF shall perform [***SCD/SVD correspondence verification***] in accordance with a specified cryptographic algorithm [***PKCS #1 V1.5 Block Type 1 with Message Digest Info with RSA CRT***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***PKCS #1 v1.5***].

FCS_COP.1.1/ SIGNING

The TSF shall perform [***Digital signature-generation***] in accordance with a specified cryptographic algorithm [***PKCS #1 V1.5 Block Type 1 with Message Digest Info addition with RSA CRT key***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***PKCS #1 v1.5***].

FCS_COP.1.1/ Diffie Hellman computation

The TSF shall perform [***Key Agreement***] in accordance with a specified cryptographic algorithm [***Diffie Hellmann***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***PKCS#3***].

FCS_COP.1.1/ Secure Messaging in Confidentiality

The TSF shall perform [***Secure Messaging in confidentiality***] in accordance with a specified cryptographic algorithm [***Retail MAC***] and cryptographic key sizes [***128 bits***] that meet the following: [***IASECC***].

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

FCS_COP.1.1/ Secure Messaging in Integrity

The TSF shall perform [***Secure Messaging in integrity***] in accordance with a specified cryptographic algorithm [***Triple DES CBC encryption/decryption***] and cryptographic key sizes [***128 bits***] that meet the following: [***IASECC***].

Application Note: This algorithm is used during secure Messaging: in integrity of incoming and outgoing data

FCS_COP.1.1/ Data hashing

The TSF shall perform [***data hashing***] in accordance with a specified cryptographic algorithm [***SHA-1 and SHA-256***] and cryptographic key sizes [***none***] that meet the following: [***FIPS 140-2***].

Application Note: This SFR corresponds to the data hashing used by the TOE.

FCS_COP.1.1/ C/S Authentication

The TSF shall perform [***C/S Authentication***] in accordance with a specified cryptographic algorithm [***PKCS #1 V1.5 Block Type 1 without Message Digest Info addition with RSA CRT key***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***PKCS#1 v1.5***].

FCS_COP.1.1/ Encryption key decipherment

The TSF shall perform [***Encryption key decipherment***] in accordance with a specified cryptographic algorithm [***PKCS #1 V1.5 Block Type 2 without Message Digest Info addition with RSA CRT key***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***PKCS#1 v1.5***].

FCS_COP.1.1/ Symmetric Role Authentication

The TSF shall perform [***Symmetric Role Authentication***] in accordance with a specified cryptographic algorithm [***based on Triple DES***] and cryptographic key sizes [***128 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Symmetric Device Authentication

The TSF shall perform [***Symmetric Device Authentication***] in accordance with a specified cryptographic algorithm [***based on Triple DES***] and cryptographic key sizes [***128 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Certificate Verification

The TSF shall perform [***Certificate verification***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric Role Authentication

The TSF shall perform [***Asymmetric Role Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric Internal DAPP Authentication

The TSF shall perform [***Asymmetric Internal DAPP Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric External DAPP Authentication

The TSF shall perform [***Asymmetric External DAPP Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ GP Authentication

The TSF shall perform [***GP Authentication***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***128 bits***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	*list of standards*
Triple DES	***SCP1 and SCP02 as defined in [GP]***

Application Note: The type of algorithm used by the TOE depends on the configuration set during the platform personalisation (For more details see [AGD_PRE_PLATFORM]. The algorithm selection is performed by the subject R.Prepersonalizer and is covered by FMT_MTD.1/JCRE

FCS_COP.1.1/ GP secret data encryption

The TSF shall perform [***GP secret data encryption***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***128 bits***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	*list of standards*
Triple DES	***SCP1 and SCP02 as defined in [GP]***

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 [AGD_PRE_PLATFORM]). The algorithm selection is performed by the subject R.Prepersonalizer and is covered by FMT_MTD.1/JCRE

3.10.1.4 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 [***khi 2 test***].

3.10.2 FDP : USER DATA PROTECTION

3.10.2.1 FDP_ACC Access Control Policy

FDP_ACC.1.1/SVD transfer SFP

The TSF shall enforce the [***SVD transfer SFP***] on [***import and export of SVD by User or Personalizer***].

FDP_ACC.1.1/Initialisation SFP

The TSF shall enforce the [***Initialisation SFP***] on [***Generation of SCD/SVD pair by User or Personalizer***].

FDP_ACC.1.1/ Personalisation SFP

The TSF shall enforce the [***Personalisation SFP***] on [***Creation of PIN RAD by Administrator or Personalizer***].

FDP_ACC.1.1/Signature-creation SFP
The TSF shall enforce the [***Signature-creation SFP***] on
[***Sending of DTBS representation by SCA***]
[***Signing of DTBS-representation by Signatory***].

FDP_ACC.1.1/SCD Import SFP

The TSF shall enforce the [***SCD Import SFP***] on [***Import of SCD by User or Personalizer***].

FDP_ACC.1.1/IAS ECC Administration SFP

The TSF shall enforce the [***IAS ECC Administration SFP***] on [***Management of Medium, HashOffCard, SymAuthMechanisms and AsymAuthMechanisms by the TOE Administrator or Personalizer***].

FDP_ACC.1.1/Key Management SFP

The TSF shall enforce the [***Key Management SFP***] on [***import of AUTH_KEYS, TOE_AUTH_PRIVATE_KEYS, TOE_AUTH_PUBLIC_KEYS and ESERVICES_KEYS, generation of TOE_AUTH_PRIVATE_KEYS/TOE_AUTH_PUBLIC_KEYS and ESERVICES_KEYS (except Diffie Hellman***

Domain parameters), export of TOE_AUTH_PUBLIC_KEYS, public portion of ESERVICES_KEYS (including Diffie Hellman Domain parameters) by the User or Personalizer].

FDP_ACC.1.1/Protection against eavesdropping SFP

The TSF shall enforce the [***Protection against eavesdropping SFP***] on [***receiving RAD, VAD, SVD, DTBS, ESERVICES_KEYS, AUTH_KEYS, TOE_AUTH_PUBLIC_KEYS , TOE_AUTH_PRIVATE_KEYS and exporting IDENTIFICATION_DATA, SVD, TOE_AUTH_PUBLIC_KEYS, public portion of ESERVICES_KEYS (except Diffie Hellman Domain parameters) and SIGNATURE]***.

Application note:
It is very important to stress the following point. When used in contactless, the TOE will have to apply this policy to receive the VAD, RAD, DTBS, AUTH_KEYS, ESERVICES KEYS, TOE_AUTH_PRIVATE_KEYS and TOE_AUTH_PUBLIC_KEYS and return the signature, the SVD, the eServices keys (except the Diffie Hellman Domain parameters), the TOE_AUTH_PUBLIC_KEYS, the identification data. It does not conflict with the existing security policies set for SCD import, signature creation, SVD export. It only enhances the security policies. In such case, the IFD will be considered as a unique entity acting as a SCA, CGA and SSCD. However, the IFD may afterwards dispatch the data to the true SCA, CGA and SSCD, provided it does ensures a trusted channel between the IFD and the SCA, CGA and SSCD.

3.10.2.2 FDP_ACF Security attribute based access control

Here is a mapping between the user, subject, objet, attribute and attached status as defined in [SSCD2] & [SSCD3].

General Attribute

Subject	Attribute	Status	Remark
User, **Personalizer**	**Role**	**S.Admin**	Several User with the status **S.Admin** may be distinguished by the TOE The Role **S.Admin** may be granted upon successful authentication based on a cryptographic mean or on a **RAD** (PIN) verification This subject can only interact in **phase 7** of the life cycle
		S.Signatory	The Role **S.Signatory** may be granted upon successful authentication based on a **RAD** verification This subject can only interact in **phase 7** of the life cycle
		S.Personalizer	The Role **S.Personalizer** may be granted upon successful GP authentication based on a cryptographic mean This subject can only interact in **phase 6** of the life cycle

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 **S.Personalizer** and in phase 7 by **S.TOE_Admin**
		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 **S.Personalizer** and in phase 7 by **S.TOE_Admin**
		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 **S.Personalizer** and in phase 7 by **S.TOE_Admin**
		Not authorized	
AsymAuthMechanisms	Authentication mechanisms based on asymmetric scheme allowed	**Authorized**	The TOE may be configured to enable/disable the authentication mechanism based on asymmetric scheme. It may be changed in phase 6 by **S.Personalizer** and in phase 7 by
		Not authorized	

			S.TOE_Admin

Initialisation attribute group

Subject	Security Attribute	Status	Remark
User, **Personalizer**	**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 subject with the role **S.Personalizer** has the attribute **SCD/SVD Management** set to Authorized. In Phase 7, two access mode may be distinguished by the TOE **SCD/SVD generation** (type 3) **SCD/SVD import** (type 2) The access condition is granted to a User if the following conditions are fulfilled: The User is successfully authenticated The User was given the right to manage the **SCD** & **SVD** (import and/or generation) by the TOE issuer. If theses two conditions are fulfilled, the attribute **SCD/SVD management** is set to **authorized**, otherwise it is set to **not authorized** This subject can only interact in phase 7 of the life cycle
		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**. The **SSCD** securely transmits the **SCD** to the TOE by mean of an encryption key. The encryption key is deduced from diversifying data agreed during the authentication of **S.Personnalizer** with the TOE. Therefore, the security attribute **Secure SCD import** is set to **Yes** when the Subject has the role **S.Personalizer** 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 data exchanged 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	

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 **S.Signatory**
		Yes	
DTBS	**Sent by an authorized SCA**	**No**	The TOE imposes the **DTBS** to be sent just before the signature computation request. As the TOE controls the access on every object it possess, in particular the **SCD** and the **SVD**, requesting the **SCD** to be sent by an authorized SCA will ensure the attribute **Sent by an authorized SCA** for the DTBS is controlled.
		Yes	

Key Management group

Subject	Security Attribute	Status	Remark
User **SCA** **CGA** **SSCD type 1** **IFD** **Personalizer**	**Key import Management**	**Authorized**	In phase 6, the subject with the role **S.Personalizer** has the attribute Key import Management set to Authorized In phase 7, the TOE controls the access on every object it possess, in particular a key belonging to the **AUTH_KEYS**, **ESERVICES_KEYS**, **TOE_AUTH_PRIVATE_KEYS** or **TOE_AUTH_PUBLIC_KEYS**. 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) If theses two conditions are fulfilled, the attribute Key import management is set to authorized, otherwise it is set to not authorized This subject can only interact in phase 7 of the life cycle
		Not authorized	

	Key generation Management	**Authorized**	In phase 6, the subject with the role **S.Personalizer** has the attribute Key generation Management set to Authorized In phase 7, the TOE controls the access on every object it possess, in particular a key belonging to the **ESERVICES_KEYS** (including Diffie Hellmann Domain parameters) **TOE_AUTH_PRIVATE_KEYS** or **TOE_AUTH_PUBLIC_KEYS**. 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 theses two conditions are fulfilled, the attribute Key generation management is set to authorized, otherwise it is set to not authorized This subject can only interact in phase 7 of the life cycle
		Not authorized	
	Key export Management	**Authorized**	In phase 6, the subject with the role **S.Personalizer** has the attribute Key export Management set to Authorized In phase 7, the TOE controls the access on every object it possess, in particular a key belonging to the public portions of **ESERVICES_KEYS** (including Diffie Hellmann Domain parameters, and **TOE_AUTH_PUBLIC_KEYS**. The access condition is granted to **User**, **SCA**, **CGA**, **SSCD type 1** or **IFD** if the following conditions are
		Not authorized	

			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 This subject can only interact in phase 7 of the life cycle

Protection against eavesdropping group

User	Security Attribute	Status	Remark
IFD	**Data exchange in contactless**	**Not authorized**	The TOE controls the access on every object it possesses, in particular the **DTBS**, **VAD**, **SIGNATURE**, **RAD**, **SVD**, **AUTH_KEYS**, **ESERVICES_KEYS**, **TOE_AUTH_PRIVATE_KEYS** or **TOE_AUTH_PUBLIC_KEYS**. The access condition is granted to IFD if the following conditions are fulfilled: The Subject is successfully authenticated The Subject was given the right to import/export the data A secure channel exists in order to protect the data exchange If theses three conditions are fulfilled, the attribute "Data exchange in contactless " is set to authorized, otherwise it is set to not authorized
		authorized	

3.10.2.2.1 SVD transfer SFP

FDP_ACF.1.1/ SVD transfer SFP
The TSF shall enforce the [***SVD transfer SFP***] to objects based on [***General attribute***]

FDP_ACF.1.2/ SVD transfer SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
(a) ***[In phase 7, the User with the security attribute "role" set to "Administrator" or "Signatory" is allowed to export SVD]***
(b) ***[In phase 6, the subject with the security attribute "role" set to "Personalizer" is allowed to export SVD in phase 6.]***

Refinement note:
Depending on the use case, the "role" allowed to export the SVD may be restricted to "Administrator" (or one of its sub-subjects: SCA, CGA, SSCD, IFD) or to "Signatory"

FDP_ACF.1.3/ SVD transfer SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]

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

Application note:
The SVD may be exported in phase 6 & 7 of the life cycle

3.10.2.2.2 Initialisation SFP

FDP_ACF.1.1/ Initialisation SFP
The TSF shall enforce the [***Initialisation SFP***] to objects based on [***General attribute***] and [***Initialisation attribute group***].

FDP_ACF.1.2/ Initialisation 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 "Administrator" or set to "Signatory" and with the security attribute "SCD/SVD management" set to "authorised" is allowed to generate SCD/SVD pair.***]
(b) [***In phase 6, the subject with the security attribute "role" set to "Personalizer" is allowed to generate SCD/SVD pair.***]

Refinement note:
Depending on the use case, the "role" allowed to generate the SCD/SVD may be restricted to "Administrator" (or one of its sub-subjects : SCA, CGA, SSCD, IFD) or to "Signatory"

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

FDP_ACF.1.4/ Initialisation SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
(a) [***In phase 7, the user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.***]
(b) [***In phase 6, the subject without the security attribute "role" set to " Personalizer " is not allowed to generate SCD/SVD pair.***]

Application note:
The Initialization SFP applies in phase 6 & 7 of the life cycle

3.10.2.2.3 SCD Import SFP

FDP_ACF.1.1/ SCD Import SFP
The TSF shall enforce the [***SCD Import SFP***] to objects based on [***General attribute***] and [***Initialisation attribute group***].

FDP_ACF.1.2/ SCD Import 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 "Administrator" or set to "Signatory" and with the security attribute "SCD/SVD management" set to "authorised" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".]***
(b) ***[In phase 6, the subject with the security attribute "role" set to "Personalizer" is allowed to import SCD]***

Refinement note:

Depending on the use case, the “role” allowed to import the SCD may be restricted to “Administrator” (or one of its sub-subjects: SCA, CGA, SSCD, IFD) or to “Signatory”
The role “Personalizer” implies that the security attribute “SCD/SVD Management” is set to “authorized” and “secure SCD import allowed” is set to Yes.

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

FDP_ACF.1.4/ SCD Import SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
(a) [***In phase 7, the user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".***]
(b) [***In phase 7, the user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD/SVD management" set to "authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no".***]
(c) [***In phase 6, the user without the security attribute "role" set to " Personalizer " is not allowed to import SCD.***]

Application note:
The SCD Import SFP applies in phase 6 & 7 of the life cycle
The SCD import SFP enables as well to erase the SCD

3.10.2.2.4 Personalisation SFP

FDP_ACF.1.1/ Personalisation SFP
The TSF shall enforce the [***Personalisation SFP***] to objects based on Personalisation SFP [***General attribute group***]

FDP_ACF.1.2/ Personalisation 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 "Administrator" is allowed to create the RAD***]
(b) [***In phase 6, the subject with the security attribute "role" set to "Personalizer" is allowed to create the RAD***]

Refinement note:
Depending on the use case, the “role Administrator” allowed to create the PIN may be restricted to a sub-subjects or Administrator (SCA, CGA, SSCD, IFD)

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

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

Application note:
The Personalization SFP applies in phase 6 & 7 of the life cycle

3.10.2.2.5 Signature Creation SFP

FDP_ACF.1.1/ Signature-creation SFP
The TSF shall enforce the [***Signature-creation SFP***] to objects based on [***General attribute group***] and [***Signature-creation attribute group***].

FDP_ACF.1.2/ Signature-creation SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[***In phase 7, the User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes"***]

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

FDP_ACF.1.4/ Signature-creation SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
(a) [***In phase 6 and 7, User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS which is not sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".]***
(b) [***In phase 6 and 7, User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no".]***
(c) [***In phase 6, User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".]***

Application note:
The Signature creation SFP applies in phase 6 and 7 of the life cycle

3.10.2.2.6 IAS ECC Administration SFP

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

FDP_ACF.1.2/ IAS 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 7, Subject with the security attribute "role" set to "TOE_Administrator" is allowed to modify the TOE attributes***]
(b) [***In phase 6, Subject with the security attribute "role" set to "Personalizer" is allowed to modify the TOE attributes***]

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

FDP_ACF.1.4/ IAS ECC Administration SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(a) [***In phase 7, Subject without the security attribute "role" set to "TOE_Administrator" is allowed to modify the TOE attributes***]
(b) [***In phase 6, Subject without the security attribute "role" set to "Personalizer" is allowed to modify the TOE attributes***]

Application note:
The IAS ECC Administration SFP applies in phase 6 & 7 of the life cycle

3.10.2.2.7 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 subject with the security attribute "role" set to "Administrator", "Signatory", "SCA", CGA", "IFD" or "SSCD type 1" and with the security attribute "Key import Management" set to "authorised".***]
(b) [***In phase 6, the subject with the security attribute "role" set to "Personalizer" is allowed to import a AUTH_KEYS, ESERVICES_KEYS, TOE_AUTH_PRIVATE_KEYS, and TOE_AUTH_PUBLIC_KEYS.***]
(c) [***In phase 7, the subject with the security attribute "role" set to "Administrator", "Signatory", "SCA", CGA", "IFD" or "SSCD type 1" and with the security attribute "Key generation Management" set to "authorised".***]
(d) [***In phase 6, the subject with the security attribute "role" set to "Personalizer" is allowed to generate a ESERVICES_KEYS (except Diffie Hellman Domain parameters), TOE_AUTH_PRIVATE_KEYS/TOE_AUTH_PUBLIC_KEYS.***]
(e) [***In phase 7, the subject with the security attribute "role" set to "Administrator", "Signatory", "SCA", CGA", "IFD" or "SSCD type 1" and with the security attribute "Key export Management" set to "authorised".***]
(f) [***In phase 6, the subject with the security attribute "role" set to "Personalizer" is allowed to export a public portion of an ESERVICES_KEYS (including Diffie Hellman Domain parameters), and TOE_AUTH_PUBLIC_KEYS.***]

Refinement note:
Depending on the use case considered, the list of subjects allowed to import, generate or export the keys may be reduced to several of them (Some may be excluded)
The role "Personalizer" implies that the security attributes are set to "authorized".

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***]

Application note:
The Key Management SFP applies in phase 6 & 7 of the life cycle
The Key Management SFP enables as well to erase the RSA keys (public and private portion)

3.10.2.2.8 Protection against eavesdropping SFP

FDP_ACF.1.1/ Protection against eavesdropping SFP
The TSF shall enforce the [***Protection against eavesdropping SFP***] to objects based on [***Protection against eavesdropping group***].

FDP_ACF.1.2/ Protection against eavesdropping SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[In phase 7, the user with the security attribute "role" set to "IFD" and with the security attribute " data exchange in contactless allowed " set to "authorised" is allowed to import and export data]

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

FDP_ACF.1.4/ Protection against eavesdropping SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
(a) ***[In phase 7, the user without the security attribute "role" set to "IFD" and with the security attribute "data exchange in contactless" set to "authorised" is not allowed to import and export data]***
(b) ***[In phase 7, the user with the security attribute "role" set to "IFD" and without the security attribute "data exchange in contactless" set to "not authorised" is not allowed to import and export data]***

Application note:
The Protection against eavesdropping SFP applies in phase 7 of the life cycle

3.10.2.3 FDP_ETC : Export to outside TSF control

3.10.2.3.1 SVD Transfer

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

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

Application note:
The Export of user data applies in phase 6 & 7 of the life cycle

3.10.2.3.2 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.

Application note:
The Export of user data applies in phase 6 & 7 of the life cycle

3.10.2.3.3 Transfer protected against eavesdropping

FDP_ETC.1.1/ Transfer protected against eavesdropping The TSF shall enforce the [***Protection against eavesdropping SFP***] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/ Transfer protected against eavesdropping The TSF shall export the user data without the user data's associated security attributes.

Application note:
The Export of user data applies in phase 7 of the life cycle

3.10.2.4 FDP_ITC Import from outside TSF control

3.10.2.4.1.1 SCD Import

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 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: [***SCD shall be sent by an Authorised SSCD***].

Application note:
A SSCD of Type 1 is authorized to send SCD to a SSCD of Type 2, if it is designated to generate the SCD for this SSCD of Type 2 and to export the SCD for import into this SSCD of Type 2. Authorized SSCD of Type 1 is able to establish a trusted channel to the SSCD of Type 2 for SCD transfer as required by FTP_ITC.1.3/SCD export.
In phase 6, an authorized SSCD is the one that received from **S.Personnalizer** the correct diversification data to correctly encrypt the SCD to transmit to the TOE.

3.10.2.4.1.2 DTBS import

FDP_ITC.1.1/ DTBS The TSF shall enforce the [***Signature-creation SFP***] when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/ DTBS The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [***DTBS-representation shall be sent by an Authorised SCA***].

Application note:
A SCA is authorized to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature and able to establish a trusted channel to the SSCD as required by FTP_ITC.1.3/SCA DTBS.

3.10.2.4.1.3 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 belonging to AUTH_KEYS or ESERVICES_KEYS groups shall be sent by the administrator, the Personalizer, the SCA, the CGA, the IFD or the SSCD type 1***].

Application note:
These SFRs only applies for the import of user data envisioned by the Key Management SFP
Depending on the use case considered, a choice may be done between the administrator, the Personalizer, the SCA, the CGA, the IFD or the SSCD type 1...

3.10.2.5 FDP_RIP Residual information protection

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: [***SM_DATA, AUTH_CRYPTOGRAM, AUTH_KEYS, ESERVICES_KEYS, EPHEMERAL_KEYS, TOE_AUTH_PUBLIC_KEYS, TOE_AUTH_PRIVATE_KEYS, SCD, VAD, and RAD***].

3.10.2.6 FDP_SDI Stored data integrity

3.10.2.6.1 Persistent data

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

- SCD
- RAD
- SVD
- AUTH_KEYS
- ESERVICES_KEYS

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 persistent 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 Signatory about integrity error.***]

3.10.2.6.2 DTBS-representation

The Protection Profiles [SSCD2] and [SSCD3] specify that the DTBS representation temporarily stored by TOE have the user data attribute "integrity checked stored data".

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 data***].

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 Signatory about integrity error.]

3.10.2.7 FDP_UCT Inter-TSF user data confidentiality transfer protection

3.10.2.7.1 SCD Import

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

Application note:
The TSF ensures protection of the SCD against unauthorized disclosure in phase 6 & 7 of the life cycle

3.10.2.7.2 Protection against eavesdropping in contactless

FDP_UCT.1.1/ TOE Contactless
The TSF shall enforce the [***Protection against eavesdropping SFP***] to [***receive and transmit***] user data in a manner protected from unauthorised disclosure.

Application Note:
This SFRs only applies in phase 7, when the SSCD features are used in contactless.

3.10.2.8 FDP_UIT Inter-TSF user data integrity transfer protection

3.10.2.8.1 SVD transfer

FDP_UIT.1.1/ SVD transfer
The TSF shall enforce the [***SVD transfer SFP***] to [***transmit***] user data in a manner protected from [***modification and insertion***] errors.

Refinement
This SFR only applies in phase 7

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

3.10.2.8.2 DTBS transfer

FDP_UIT.1.1/ TOE DTBS
The TSF shall enforce the [***Signature-creation SFP***] to [***receive***] user data in a manner protected from [***modification, deletion and insertion***] errors.

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

3.10.2.8.3 Protection against eavesdropping in contactless

FDP_UIT.1.1/ TOE Contactless The TSF shall enforce the [***Protection against eavesdropping SFP***] to [***receive and transmit***] user data in a manner protected from [***modification, deletion and insertion***] errors.

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

Application Note:
These SFRs only applies in phase 7, when the SSCD features are used in contactless

3.10.3 FIA: IDENTIFICATION AND AUTHENTICATION

3.10.3.1 FIA_AFL Authentication failure

FIA_AFL is specific to the RAD and the Authentication keys.

- RAD used by the Signatory
- RAD used by the Administrator.
- The Symmetric key(s) used by the Personalization Agent
- The Symmetric key(s) used by the TOE Administrator
- Symmetric external authentication keys used by the Administrator
- Symmetric device authentication keys used by the Administrator or a remote IT
- Asymmetric external authentication keys used by the Administrator
- Asymmetric device authentication keys used by the Administrator or a remote IT

FIA AFL.1.1/RAD The TSF shall detect when [***an administrative configurable positive integer within 1 and 15***] unsuccessful authentication attempts occur related to [***consecutive failed authentication attempts***].

FIA AFL.1.2/RAD When the defined number of unsuccessful authentication attempts has been [***met or surpassed***], the TSF shall [***block RAD***].

Application Note:
The Authentication Try Limit N, defined during personalisation, must verify $1 \leq N \leq 15$.

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:
The Authentication or external entities (subjects or remote IT entities) may be performed with the D.AUTH_KEYS or with D.EPHEMERAL_KEYS. Depending on the cases, several cases may occur:

Type of TSF data	Entity to be authenticated	Selection for FIA_AFL.1.1 /Authentication keys	List of action
D.AUTH_KEYS	S.Personalizer	*Positive integer number* '1'	*Time of next authentication increases*
D.AUTH_KEYS	S.TOE_Admin	*Positive integer number* '1'	*Time of next authentication increases*
D.AUTH_KEYS	S.Admin (when using symmetric role authentication)	*Administrator configurable positive integer* 'N' $0 \leq N \leq 15$	*If N= '0', no actions are taken. If N != '0', the key is blocked*
D.AUTH_KEYS	S.Admin or Remote IT entity (when using symmetric device authentication)	*Administrator configurable positive integer* 'N' $0 \leq N \leq 15$	*If N= '0', no actions are taken. If N != '0', the key is blocked*
D.EPHEMERAL_KEYS	S.Admin (when using asymmetric role authentication)	*Positive integer number* '1'	*The key is deallocated with respect to FDP_RIP.1.1*
D.EPHEMERAL_KEYS	Administrator or Remote IT entity (when using asymmetric device authentication)	*Positive integer number* '1'	*The key is deallocated with respect to FDP_RIP.1.1*

It is important to note that the subject S.Admin may be the SCA, CGA, SSCD or IFD if they act as a subject.

3.10.3.2 FIA_ATD User attribute definition

FIA ATD.1.1 / S.Signatory
The TSF shall maintain the following list of security attributes belonging to individual users [***RAD***]

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

Application Note:
This is mandated if the User "Administrator" is authenticated by mean of a RAD.

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 [***AUTH_KEYS and EPHEMERAL_KEYS***]

Application Note:
Each subject is authenticated thanks to a dedicated authentication key and a dedicated authentication scheme. The key to use is a TSF data that is either permanently stored in the TOE (**AUTH_KEYS**), or an ephemeral key extracted from a certificate (**EPHEMERAL_KEYS**).

3.10.3.3 FIA_UAU User authentication

FIA UAU.1.1
The TSF shall allow
[***Identification of the user by means of TSF required by FIA_UID.1***]
[***Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP_ITC.1/SCD import***]
[***Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE to transmit the VAD if the TOE is used in contact in phase 7***]
[***Establishing a trusted channel between an IFD and the TOE by means of TSF required by FTP_ITC.1/ TOE Contactless to transmit the VAD if the TOE is used in contactless in phase 7***]
[***Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import in phase 7***]
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.

Application note:
"Local user" mentioned in component FIA_UAU.1.1 is the user using the trusted path provided between the SCA in the TOE environment and the TOE as indicated by FTP_TRP.1/SCA and FTP TRP.1/TOE.
This trusted path enables to authenticate the role Signatory and Administrator (if it is authenticated with a RAD).

3.10.3.4 FIA_UID User Identification

FIA UID.1.1
The TSF shall allow
[***Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP_ITC.1/SCD import***]
[***Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE to transmit the VAD if the TOE is used in contact in phase 7***]
[***Establishing a trusted channel between an IFD and the TOE by means of TSF required by FTP_ITC.1/ TOE Contactless to transmit the VAD if the TOE is used in contactless in phase 7***]
[***Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import in phase 7***]
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.

3.10.4 FMT: SECURITY MANAGEMENT

3.10.4.1 FMT_MOF Management of functions in TSF

FMT_MOF.1.1
The TSF shall restrict the ability to [***enable***] the functions [***signature-creation function***] to [***Signatory***].

3.10.4.2 FMT_MSA Management of security attributes

FMT_MSA.1.1/ Administrator - Initialisation
The TSF shall enforce the [***Initialisation SFP***] to restrict the ability to [***modify***] the security attributes [***SCD/SVD management***] to [***Administrator and Personalizer***].

FMT_MSA.1.1/ Administrator - Import
The TSF shall enforce the [***SCD Import SFP***] to restrict the ability to [***modify***] the security attributes [***SCD/SVD management and secure SCD import allowed***] to [***Administrator and Personalizer***].

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 [***Signatory***].

FMT_MSA.1.1/ Management of TOE
The TSF shall enforce the [***IAS ECC Administration SFP***] to restrict the ability to [***modify***] the security attributes [***Medium, HashOffCard, SymAuthMechanism and AsymAuthMechanism***] to [***TOE_Administrator or Personalizer***].

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 [***User, SCA, CGA, SSCD, IFD***].

FMT_MSA.1.1/ Protection against eavesdropping
The TSF shall enforce the [***Protection against eavesdropping SFP***] to restrict the ability to [***modify***] the security attributes [***data exchange in contactless***] to [***IFD***].

FMT_MSA.2.1
The TSF shall ensure that only secure values are accepted for [***SCD/SVD management, SCD operational, Medium, HashOffCard, SymAuthMechanism, AsymAuthMechanism, Key import management, Key generation management and Key export Management, data exchange in contactless]***.

FMT_MSA.3.1
The TSF shall enforce the [***Initialisation SFP, Signature-creation SFP, SCD Import SFP, IAS ECC Administration SFP and Key Management SFP, Protection against eavesdropping SFP***] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

Refinement:
The security attribute of the SCD "SCD operational" is set to "no" after generation or import of the SCD.

FMT_MSA.3.2 The TSF shall allow the [***assignment : the authorised identified role***] to specify alternative initial values to override the default values when an object or information is created.

Refinement:
The following refinement applies:

Security attributes	Authorized identified role
SCD/SVD Management	Administrator Personalizer
SCD Operational	Administrator
Medium HashOffCard SymAuthMechanism AsymAuthMechanism	Personalizer TOE_Administrator
data exchange in contactless	IFD
Key import Management Key generation Management Key export Management	User, SCA, CGA, SSCD, IFD
Secure SCD import Allowed	SSCD
Sent by an authorized SCA	SCA
Role	User Personalizer

3.10.4.3 FMT_MTD Management of TSF data

3.10.4.3.1 Signatory

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

Refinement:
This requirement applies only if the RAD is the one used for the Authentication of the Role Signatory

3.10.4.3.2 Association between SCD and SCD_ID

FMT_MTD.1.1/ Association between SCD and SCD_ID The TSF shall restrict the ability to [***associate***] the [***SCD and a SCD_ID***] to [***Administrator and Personalizer***].

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

3.10.4.3.3 Protection against traceability

FMT_MTD.1.1/ Disabling identification data retrieval

The TSF shall restrict the ability to [***to disable read access for users to***] the [**IDENTIFICATION_DATA**] to [***Manufacturer***].

Application note:
The requirement is only needed in case the TOE is used in contactless mode. It ensures it is not possible to retrieve identification data such as CPLC data, TOE identifier, FCI of the Card Manager,
Rely on the SFRs provided by [ST_PLATFORM] :

- FMT_MOF.1/PP_TOE enable to disable identification data retrieval
- FDP_ACC.2/PP restricts the access to this feature to the Manufacturer

3.10.4.3.4 TOE Serial number

FMT_MTD.1.1/ TOE Serial number The TSF shall restrict the ability to [***set***] the [***TOE_SerialNumber***] to [***Personalizer in phase 6***].

Application note:
The **Personalizer** only interacts with the TOE in phase 6

3.10.4.3.5 TOE State

FMT_MTD.1.1/ TOE State The TSF shall restrict the ability to [***modify***] the [***STATE***] to [***Personalizer in phase 6***].

Application note:
The **Personalizer** shall set D.STATE to “PERSONALIZED” at the end of phase 6 to switch the life cycle to phase 7.

3.10.4.3.6 RAD Unblocking

FMT_MTD.1.1/ Unblock The TSF shall restrict the ability to [***unblock***] the [***RAD***] to [***the Administrator in phase 7***].

Application note:
This SFR only applies to the RAD when it is a PIN.

3.10.4.4 FMT_SMF Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [***SCD/SVD Generation, SCD import, RAD personalization, Signature creation, Management of the TOE, Key Management, Protection against eavesdropping, RAD unblocking***].

3.10.4.5 FMT_SMR Security management roles

FMT_SMR.1.1 The TSF shall maintain the roles [***Administrator***, ***TOE_Administrator***, ***SCA***, ***CGA***, ***SSCD***, ***IFD***, ***Personalizer and Signatory***].

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

Application note:
The **SCA, CGA, SSCD,** and **IFD** may be seen as subjects. As such, the TOE maintains their Role.

3.10.5 FPT: PROTECTION OF THE TSF

3.10.5.1 FPT_EMSEC TOE Emanation

FPT_EMSEC.1.1
The TOE shall not emit [***Side channel emission***] in excess of [***limits specified by the state-of-the-art attacks on smart card IC***] enabling access to [***ESERVICES_KEY, AUTH_KEY,RAD and SCD***] and [***none***].

FPT_EMSEC.1.2
The TSF shall ensure [***all users***] are unable to use the following interface [***external contacts emanations***] to gain access to [***ESERVICES_KEY, AUTH_KEY,RAD and SCD***] and [***none***].

3.10.5.2 FPT_FLS Failure secure

FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [
those associated to the potential security violations described in FAU_ARP.1 of the underlying javacard open platform,
the applet deletion manager fails to delete a package/applet,
the object deletion functions fail to delete all the unreferenced objects owned by the applet that requested the execution of the method,
1. Invalid reference exception; 2. Code or data integrity failure; 3. Power loss while processing. 4. worm on or dead EEPROM, full security area, false CRC
For each problem the TOE sends a specific exception status or doesn't start,].

3.10.5.3 FPT_PHP TSF physical Protection

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.3.1
The TSF shall resist [***changing operational conditions every times: the frequency of the external clock, power supply, and temperature***] to the [***chip elements***] by responding automatically such that the SFRs are always enforced

3.10.5.4 FPT_TST TSF self test

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

FPT_TST.1.2
The TSF shall provide authorised users with the capability to verify the integrity of [***TSF data***].

FPT_TST.1.3
The TSF shall provide authorised users with the capability to verify the integrity of [***TSF executable code***].

3.10.6 FTP: TRUSTED PATH/CHANNELS

3.10.6.1 FTP_ITC Inter-TSF trusted channel

3.10.6.1.1 SCD Import

FTP_ITC.1.1/ SCD import
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 import
The TSF shall permit [***another trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SCD import
The TSF shall initiate communication via the trusted channel for [***SCD import***]

Refinement:
This requirement applies in phase 6 & 7.

3.10.6.1.2 SVD Transfer

FTP_ITC.1.1/ SVD transfer
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/ SVD transfer
The TSF shall permit [***another trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SVD transfer
The TSF shall initiate communication via the trusted channel for [***SVD transfer***]

Refinement:
The mentioned remote trusted IT product is a CGA in phase 7

Application note:
FTP_ITC.1/SVD Transfer will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

3.10.6.1.3 DTBS Import

FTP_ITC.1.1/ DTBS import 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/ DTBS import The TSF shall permit [***another trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3 DTBS import The TSF shall initiate communication via the trusted channel for [***signing DTBS-representation***]

Refinement:
The mentioned remote trusted IT product is a SCA.
This requirement applies in phase 7 only.

3.10.6.1.4 Protection against traceability in contactless

FTP_ITC.1.1/ TOE Contactless 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/ TOE Contactless The TSF shall permit [***another trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3 TOE Contactless The TSF shall initiate communication via the trusted channel for [***performing any operation that may disclose any information about the holder, such as identification or traceability***]

Refinement:
The mentioned remote trusted IT product is an interface device (IFD)

3.10.6.2 FTP_TRP Trusted path

FTP_TRP.1.1/ TOE The TSF shall provide a communication path between itself and [***local***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification or disclosure***].

FTP_TRP.1.2/ TOE The TSF shall permit [***local users***] to initiate communication via the trusted path.

FTP_TRP.1.3/ TOE The TSF shall require the use of the trusted path for [***initial user authentication***].

Application note:
The Trusted path is required to send the VAD to the TOE in order to identify & authenticate the **Signatory**, and the **Administrator (if it was authenticated with a RAD)**,
During phase 7, if the TOE is used in contactless mode, in order to protect the VAD against eavesdropping and prevent the traceability risks, the trusted path is removed and replaced by the trusted channel defined by:

- FTP_ITC.1.1/ TOE Contactless (against traceability)
- FTP_ITC.1.2/ TOE Contactless (against traceability)
- FTP_ITC.1.3/ TOE Contactless (against traceability)
- FDP_UCT.1.1/ TOE Contactless (against disclosure)
- FDP_UIT.1.1/ TOE Contactless (against eavesdropping)
- FDP_UIT.1.2/ TOE Contactless (against eavesdropping)

3.11 Security requirements for the IT environment

This section describes the IT security requirements that are to be met by the IT environment of the TOE. The IT environment of the TOE is composed of the Certification Generation Application (**CGA**) and the Signature Creation Application (**SCA**).
These requirements are as stated in [**SSCD2**] & [**SSCD3**].

3.11.1 Signature key generation (SSCD Type1)

3.11.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***RSA key generation***] and specified cryptographic key sizes [***1024 bits or 1536 bits or 2048 bits***] that meet the [***ANSI X9.31***]

FCS_CKM.1.1 / DES session keys
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***DES key generation***] and specified cryptographic key sizes [***128 bits***] that meet the [***IASECC***]

3.11.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 / Type1
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: [***assignment: list of standards***].

Application notes:
The cryptographic key SCD will be destroyed automatically after export.

FCS_CKM.4.1 / DES 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: [***assignment: list of standards***].

3.11.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP

The TSF shall perform [***SCD/SVD correspondence verification***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***assignment: list of standards***].

FCS_COP.1.1/ Diffie Hellman computation

The TSF shall perform [***Key Agreement***] in accordance with a specified cryptographic algorithm [***Diffie Hellmann***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***PKCS#3***].

FCS_COP.1.1/ Secure Messaging in Confidentiality

The TSF shall perform [***Secure Messaging in confidentiality***] in accordance with a specified cryptographic algorithm [***Retail MAC***] and cryptographic key sizes [***128 bits***] that meet the following: [***IASECC***].

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

FCS_COP.1.1/ Secure Messaging in Integrity

The TSF shall perform [***Secure Messaging in integrity***] in accordance with a specified cryptographic algorithm [***Triple DES CBC encryption/decryption***] and cryptographic key sizes [***128 bits***] that meet the following: [***IASECC***].

Application Note: This algorithm is used during secure Messaging: in integrity of incoming and outgoing data

FCS_COP.1.1/ Data hashing

The TSF shall perform [***data hashing***] in accordance with a specified cryptographic algorithm [***SHA-1 and SHA-256***] and cryptographic key sizes [***none***] that meet the following: [***FIPS 140-2***].

FCS_COP.1.1/ Certificate computation

The TSF shall perform [***Certificate computation***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric Internal DAPP Authentication

The TSF shall perform [***Asymmetric Internal DAPP Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric External DAPP Authentication

The TSF shall perform [***Asymmetric External DAPP Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ GP secret data encryption

The TSF shall perform [***GP secret data encryption***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***128 bits***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	*list of standards*
Triple DES	***SCP1 and SCP02 as defined in [GP]***

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 [AGD_PRE_PLATFORM]). The algorithm selection is performed by the subject R.Prepersonalizer and is covered by FMT_MTD.1/JCRE

3.11.1.4 Random Number Generation (FCS_RNG)

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

3.11.1.5 Subset access control (FDP_ACC.1)

FDP_ACC.1.1/ SCD Export SFP

The TSF shall enforce the [***SCD Export SFP***] on [***export of SCD by Administrator***].

3.11.1.6 Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1.1/ Sender
The TSF shall enforce the [***SCD Export SFP***] to [***transmit***] user data in a manner protected from unauthorised disclosure.

3.11.1.7 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SCD Export

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 Export
The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SCD Export
The TSF shall initiate communication via the trusted channel for [***SCD export***]

Refinement:
The mentioned remote trusted IT product is a SSCD Type2

Application note:
If the TOE exports the SVD to a SSCD Type2 and the SSCD Type 2 holds the SVD then the trusted channel between the TOE and the SSCD type 2 will be required.

3.11.2 Certification generation application (CGA)

3.11.2.1 Cryptographic key generation (FCS_CKM.1)

FCS CKM.1.1 / DES session keys

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***DES key generation***] and specified cryptographic key sizes [***128 bits***] that meet the [***IASECC***]

3.11.2.2 Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1/ CGA

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [***qualified certificates***] that meets the following: [***assignment: list of standards***].

3.11.2.3 Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/ CGA

The TSF shall perform [***import the SVD***] in accordance with a specified cryptographic key access method [***import through a secure channel***] that meets the following: [***IASECC***].

3.11.2.4 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 / DES 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: [***assignment: list of standards***].

3.11.2.5 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ Diffie Hellman computation

The TSF shall perform [***Key Agreement***] in accordance with a specified cryptographic algorithm [***Diffie Hellmann***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***PKCS#3***].

FCS_COP.1.1/ Secure Messaging in Confidentiality

The TSF shall perform [***Secure Messaging in confidentiality***] in accordance with a specified cryptographic algorithm [***Retail MAC***] and cryptographic key sizes [***128 bits***] that meet the following: [***IASECC***].

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

FCS_COP.1.1/ Secure Messaging in Integrity

The TSF shall perform [***Secure Messaging in integrity***] in accordance with a specified cryptographic algorithm [***Triple DES CBC encryption/decryption***] and cryptographic key sizes [***128 bits***] that meet the following: [***IASECC***].

Application Note: This algorithm is used during secure Messaging: in integrity of incoming and outgoing data

FCS_COP.1.1/ Data hashing

The TSF shall perform [***data hashing***] in accordance with a specified cryptographic algorithm [***SHA-1 and SHA-256***] and cryptographic key sizes [***none***] that meet the following: [***FIPS 140-2***].

FCS_COP.1.1/ Certificate computation

The TSF shall perform [***Certificate computation***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric Internal DAPP Authentication

The TSF shall perform [***Asymmetric Internal DAPP Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric External DAPP Authentication

The TSF shall perform [***Asymmetric External DAPP Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

3.11.2.6 Random Number Generation (FCS_RNG)

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

3.11.2.7 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ SVD Import The TSF shall enforce the [***SVD import SFP***] to [***receive***] user data in a manner protected from [***modification and insertion***] errors.

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

3.11.2.8 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SVD Import 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/ SVD Import The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SVD Import The TSF shall initiate communication via the trusted channel for [***SVD import***]

3.11.3 Signature creation application (SCA)

3.11.3.1 Cryptographic key generation (FCS_CKM.1)

FCS CKM.1.1 / DES session keys The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***DES key generation***] and specified cryptographic key sizes [***128 bits***] that meet the [***IASECC***]

3.11.3.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 / DES 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: [***assignment: list of standards***].

3.11.3.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ SCA Hash

The TSF shall perform [***hashing the DTBS***] in accordance with a specified cryptographic algorithm [***SHA-1 and SHA-256***] and cryptographic key sizes [***none***] that meet the following: [***FIPS 140-2***].

FCS_COP.1.1/ Diffie Hellman computation

The TSF shall perform [***Key Agreement***] in accordance with a specified cryptographic algorithm [***Diffie Hellmann***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***PKCS#3***].

FCS_COP.1.1/ Secure Messaging in Confidentiality

The TSF shall perform [***Secure Messaging in confidentiality***] in accordance with a specified cryptographic algorithm [***Retail MAC***] and cryptographic key sizes [***128 bits***] that meet the following: [***IASECC***].

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

FCS_COP.1.1/ Secure Messaging in Integrity

The TSF shall perform [***Secure Messaging in integrity***] in accordance with a specified cryptographic algorithm [***Triple DES CBC encryption/decryption***] and cryptographic key sizes [***128 bits***] that meet the following: [***IASECC***].

Application Note: This algorithm is used during secure Messaging: in integrity of incoming and outgoing data

FCS_COP.1.1/ Certificate computation

The TSF shall perform [***Certificate computation***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric Internal DAPP Authentication

The TSF shall perform [***Asymmetric Internal DAPP Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric External DAPP Authentication

The TSF shall perform [***Asymmetric External DAPP Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

3.11.3.4 Random Number Generation (FCS_RNG)

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

3.11.3.5 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ SCA DTBS
The TSF shall enforce the [***Signature-creation SFP***] to [***transmit***] user data in a manner protected from [***modification, deletion and insertion***] errors.

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

3.11.3.6 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SCA DTBS
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/ SCA DTBS
The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SCA DTBS
The TSF shall initiate communication via the trusted channel for [***signing DTBS-representation by means of the SSCD***]

3.11.3.7 Trusted path (FTP_TRP.1)

The trusted path between the TOE and the SCA will be required only if the human interface for user authentication is not provided by the TOE itself but by the SCA.

FTP_TRP.1.1/ SCA
The TSF shall provide a communication path between itself and [***local***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification or disclosure***].

FTP_TRP.1.2/ SCA
The TSF shall permit [***the TSF or local users***] to initiate communication via the trusted path.

FTP_TRP.1.3/ SCA

The TSF shall require the use of the trusted path for [***initial user authentication***].

3.11.4 Interface Device (IFD)

3.11.4.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 / Authentication keys The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***RSA key generation***] and specified cryptographic key sizes [***1024 bits or 1536 bits or 2048 bits***] that meet the [***ANSI X9.31***]

3.12 Security requirements for the Administrator

This section describes the Administrator security requirements that are to be met when they use cryptographic mean to authenticate themselves.

3.12.1.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ Data hashing The TSF shall perform [***data hashing***] in accordance with a specified cryptographic algorithm [***SHA-1 and SHA-256***] and cryptographic key sizes [***none***] that meet the following: [***FIPS 140-2***].

FCS_COP.1.1/ Symmetric Role Authentication The TSF shall perform [***Symmetric Role Authentication***] in accordance with a specified cryptographic algorithm [***based on Triple DES***] and cryptographic key sizes [***128 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Certificate computation The TSF shall perform [***Certificate computation***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric Role Authentication The TSF shall perform [***Asymmetric Role Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

3.13 Security requirements for the Personalizer and TOE_Administrator

This section describes the Personalizer and TOE_Administrator security requirements that are to be met as they use cryptographic mean to authenticate themselves.

3.13.1.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ GP Authentication

The TSF shall perform [***GP Authentication***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***128 bits***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	*list of standards*
Triple DES	***SCP1 and SCP02 as defined in [GP]***

Application Note: The type of algorithm used by the TOE depends on the configuration set during the platform personalisation (For more details see [AGD_PRE_PLATFORM]. The algorithm selection is performed by the subject R.Prepersonalizer and is covered by FMT_MTD.1/JCRE

3.14 Security requirements for the non-IT environment

3.14.1 Standard security requirements

R.Administrator_Guide *Application of Administrator Guidance*

The implementation of the requirements of the Directive, ANNEX II "Requirements for certification service-providers issuing qualified certificates", literal (e), stipulates employees of the CSP or other relevant entities to follow the administrator guidance provided for the TOE. Appropriate supervision of the CSP or other relevant entities shall ensure the ongoing compliance.

R.Sigy_Guide *Application of User Guidance*

The SCP implementation of the requirements of the Directive, ANNEX II "Requirements for certification service-providers issuing qualified certificates", literal (k), stipulates the signatory to follow the user guidance provided for the TOE.

R.Sigy_Name *Signatory's name in the Qualified Certificate*

The CSP shall verify the identity of the person to which a qualified certificate is issued according to the Directive [1], ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (d). The CSP shall verify that this person holds the SSCD, which implements the SCD corresponding to the SVD to be included

3.14.2 Complementary security requirements

R.Keys_Protection *Protection of the authentication keys and TOE's public authentication keys during transfer*

The environment shall ensure the protection of authentication keys when transferred to the TOE in order to protect it from disclosure and ensure they are not modified nor altered. The TOE's public authentication key shall be protected against modification when exported from the TOE to the outside when an authentication certificate request is made.

R.Contactless_Personalization *Specific rules when used in contactless*

When the TOE is used in contactless, the entity in charge of issuing the TOE (the Personalizer) shall ensure the security policy applied to protect the identification data (stored in the TOE) is restrictive. The TOE shall either refuse the access, or mandate the authentication of the outside. When exchanged, the data shall be protected in confidentiality and authenticate the sender.
Furthermore, if another applet is loaded on the javacard open platform, the entity in charge of issuing the TOE shall make sure the applet does not endanger the privacy of the TOE by enabling it to be tracked. It shall either control the applet behaviour, either ban it.

This requirement applies to

- The manufacturer, if the applet is loaded in phase 5
- The personaliser, if the applet is loaded in phase 6 while DAP is not activated
- The DAP_Admin, if the applet is loaded while DAP control is activated

R.LinkBetweenSCDandCertificate	*Link between the SCD(s) stored in the TOE and qualified certificates*

The environment shall ensure at any time a valid link between the SCD(s) stored in the TOE and the matching (qualified) certificates. Each time the SCD is modified (by import or generation), an unambiguous link between the SCD(s) and the matching (qualified) certificate(s) shall be maintained. This link might be figured out by a PKCS#15 structures, an XML structure, an identifier .linking a SCD to the file containing the qualified certificate or the URL hosting them. In particular, it implies it is updated, each time the SCD is created, imported, erased or generated.

R.TOE_Construction	*Construction of the TOE*

The Construction of the TOE shall be done by the Personalization Agent who acts in phase 6 of the TOE life Cycle. The Personalization Agent shall be a trusted person and shall apply the recommendations indicated in [**AGD_PRE**].

4 TOE summary specification

4.1 Security function of the TOE

4.1.1 Security functions provided by the javacard open platform

All the security functions provided by the javacard open platform are described in [**ST_PLATFORM**].
They are listed in the following table.

Security function	Description
SF_Firewall	Firewall Security policy
SF_Card_Content_Management	Control of loading, deletion and installation of applet and packages
SF_Card_Management_Environment	Initialization and management of internal data structure of the Card Manager
SF_Signature	Generation/Verification of signature
SF_Encryption_and_Decryption	Encryption/Decryption of Data
SF_Message_Digest_Generation	Message Digest computation
SF_Random_Number_Generation	Random number generation
SF_Key_Destruction	Destruction of keys
SF_data_integrity	Integrity of keys, PIN, packages, …
SF_Clearing_of_Sensitive_Information	Clearing of sensitive data when not used anymore
SF_Atomic_Transactions	Execution of atomic operations
SF_Key_Generation	Generation of Asymmetric keys
SF_Key_Distribution	Distribution of keys
SF_Cardholder_Verification	Authentication of the cardholder with PIN
SF_Hardware_Operating	Hardware self tests at start up or before first use

SF_Memory_failure	Management of non volatile memory
SF_Data_Coherency	Transaction mechanism
SF_Exception	Management of abnormal execution
SF_DAP_Verification	DAP verification for applet loading
SF_TOKEN	Validity of card content management
SF_Manufacturer_Authentication	Authentication of the manufacturer agent
SF_Resident_Application_Dispatcher	Control of security level when communicating with resident application
SF_Entity_Authentication/Secure_Channel	GP Secure Channel management
SF_GP_Dispatcher	Control of security level when communicating with the Card manager
SF_KEY_MANAGEMENT	Management of the keys of the Card Manager
SF_Security_Functions_of_the IC	Security function of the IC
SF_Unobservability	Unobservability of secure element processing
SF_Prepersonalization	Prepersonalization of the TOE
SF_Key_Access	Secure Access to keys and PINs
SF_Key_Agreement	Key agreement

4.1.2 Security functions added by the composite TOE

The TOE provides the following security functions on top of the one provided by the underlying javacard open platform.

Security function	Description
SF.PIN_MGT	PIN Management
SF.SIG	Signature Computation
SF.DEV_AUTH	Device Authentication
SF.ADM_AUTH	Administrator Authentication
SF.SM	Secure messaging
SF.KEY_MGT	Key Management
SF.CONF	Configuration of TOE
SF.ESERVICE	Execution of eServices
SF.EAVESDROPPING_PROTECTION	Protection of communication against eavesdropping (when the TOE is used in contactless)
SF.SAFESTATE_MGT	Safe State Management
SF.PHYS	Physical protection

SF.PIN_MGT

This security function is involved in the PIN (RAD) management. In particular, it provides access control over the creation, update, reset and verification of the PIN, depending on the subject and the life cycle state.

In phase 6, this security function only allows the RAD(s) to be created and its value to be loaded in an encrypted way by the Personalizer Agent. It can not be checked.

In phase 7, this security function enables to create the RAD, to verify, unblock, and change the RAD according to the security policies set at RAD creation

This security function enables to authenticate the subject Signatory and Administrator (if it is authenticated with a RAD). It manages as well an error counter for each RAD, ensuring protection against brute force attacks.

This security function ensures the deallocation of the RAD when it is updated and of the VAD when it is sent to the TOE for checking

This security function enables the RAD management either directly through the IAS ECC applet with APDU command, or through shared interfaces. The shared interfaces enable, other applets loaded on the javacard open platform to use the services provided by the security function.

However, in any case, whether shared interfaces or APDU commands are used, the same security policy is applied to access RAD management features.

SF.SIG

This security function manages the signature computation.

In phase 6, it ensures the Personalizer Agent can not sign on behalf of the Signatory

In phase 7, it enforces the correct security policy for the DTBS import and for the signature computation, depending on the subjects

It performs the signature computation and ensures the SCD and SVD correspond.

SF.DEV_AUTH

This security function manage the (mutual) device authentication between the TOE and a remote IT. It is only active in phase 7.

It enables the TOE to establish a trusted channel with remote IT entities such as the SCA, the CGA, the SSCD type 1 and the IFD. The device authentication may be either realized with symmetric or asymmetric scheme.

This security function ensures the mutual authentication of both entities (TOE and remote IT entity). Upon successful authentication, it computes a shared secret (called the seed) used by SF.SM to generate the session key to ensure the protection in integrity and confidentiality of the data exchanged. This seed is computed from random numbers partly generated by the TOE, partly generated by the remote IT.

This security function manages as well an error counter for each key used for the authentication of the remote IT entity.

This security function ensures the deallocation of

- the authentication cryptogram received once processed

- in case the asymmetric scheme is used, it ensures as well the deallocation of the ephemeral public keys extracted form the certificates processed by the TOE after use

SF.ADM_AUTH

This security function enables the TOE to authenticate external entities. It is active in phase 6 and 7.

In phase 6, it enables the TOE to authenticate the Personalization Agent and in phase 7, it enables to authenticate the TOE_Administrator, and the Administrator.

The authentication of the Administrator may be either realized with symmetric or asymmetric scheme.

This security function manages as well an error counter for each key used for the authentication of the external entity.

This security function ensures the deallocation of

- the authentication cryptogram received once processed
- in case the asymmetric scheme is used, it ensures as well the deallocation of the ephemeral public keys extracted form the certificates processed by the TOE after use

SF.SM

This security function applies only in phase 7. It ensures the protection of communication between the TOE and Remote IT entities.

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

This security function ensures the following properties:

- The TOE can detect any **modification or deletion** when receiving data
- The incoming data are protected against **disclosure**
- The TOE can return data in a manner protected from **modification and deletion**
- The TOE can return data in a manner protected against **disclosure**
- Upon reception of the data, the recipient can check the **data were issued by the expected sender** (authenticated by SF.DEV_AUTH).

The integrity and confidentiality of data exchanged are ensured by cryptographic means: data are encrypted and their integrity is ensured by a MAC computed with session keys.

This security function builds 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. In order to ensure a protection against replay attacks, the MAC is computed from an ICV which is generated randomly by the TOE and by the external entity once the device authentication is successful.

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

SF.KEY_MGT

This security function applies in phase 6 & 7. It provides the mean to

- Create any kind of keys and the DH parameters
- generate asymmetric key pairs (used for signature computation or TOE authentication)
- update the keys (symmetric key used for authentication of external entity, SCD/SVD, eServices keys, asymmetric keys for TOE's authentication) and the DH Domain parameters
- export the SVD and the TOE's authentication public key

It provides access control over these operations and means to set at creation the relevant security policy to apply for the key use.

In particular, in case of SCD/SVD key pair update (by import or generation), this security function ensures the "SCD operational" state is reset.

When a key value is updated (by import or generation), the former key value is destroyed.

SF.CONF

This security function applies in phase 6 & 7. It manages the initialization of TSF data and administration features of the TOE.

It provides access control on the modification of the following TOE attributes:

- Communication medium : contact and/or contactless
- Type of cryptography to be used for the remote IT entities and remote subject authentication (symmetric or asymmetric)
- Type of DTBS to be used: the DTBS representation fully computed outside the TOE may be used.

Only the Personalization Agent can modify them in phase 6, and the TOE_Administrator in phase 7.

It restricts the initialization of the following TSF data to the Personalization Agent/Manufacturing Agent only:

- TOE serial number – shall be initialized in phase 6 by the **Personalization Agent**
- identification data of the TOE – Retrieval can be locked in phase 5 by the **Manufacturing or Personalization Agent**
- TOE State – it shall be set at the end of phase 6 to PERSONNALIZED by the **Personalization Agent**

SF.ESERVICE

This security function applies in phase 7. It enables to perform eservices such as

- C/S authentication
- Decryption key decipherment
- Certificate verification

SF.EAVESDROPPING_PROTECTION

This security function applies in phase 7. It enables to ensure protection of sensitive data against eavesdropping when the TOE is used in contactless.
This security function requires **P.SecurityPolicy_Contactless** to be applied.

It enforces the keys, the PIN (RAD and VAD) as well as the identification data to be transferred through a trusted channel established with an interface device.

SF.SAFESTATE_MGT

This security function applies in phase 6 & 7. It performs the following operations:

- Monitoring the integrity of the TOE and the TSF data by performing selftests
- Ensuring the TOE returns in a safe state when an unexpected event occurs (loss of power, tearing,…): all sensitive data are erased and the TOE returns in a restrictive and secure state.

In case a major error is detected, the security function destroys the TOE.

SF.PHYS

This security function applies in phase 6 & 7. It ensures

- the TOE detects physical manipulation (I/O manipulation, EM perturbation, temperature perturbation,…) and takes countermeasures.
- The TOE is protected against probing and that there is no information leakage that my be used to reconstruct sensitive data

In case a major error is detected, the security function destroys the TOE.

4.1.3 Composition with the Security functions provided of the javacard Open platform

The .following table shows how the security functions of the Composite TOE are supported by the security functions of the underlying javacard open platform:

Security function	Depends on
SF.PIN_MGT	SF_Cardholder_Verification SF_Clearing_of_Sensitive_Information
SF.SIG	SF_Key_Access SF_Clearing_of_Sensitive_Information SF_Message_Digest_Generation SF_Encryption_and_Decryption
SF.DEV_AUTH	SF_Key_Access SF_Clearing_of_Sensitive_Information SF_Key_Destruction SF_Random_Number_Generation SF_Message_Digest_Generation SF_Encryption_and_Decryption SF_Signature
SF.ADM_AUTH	SF_Key_Access SF_KEY_MANAGEMENT SF_Entity_Authentication/Secure_Channel SF_Clearing_of_Sensitive_Information SF_Key_Destruction SF_Random_Number_Generation SF_Message_Digest_Generation SF_Encryption_and_Decryption SF_Signature

SF.SM	SF_Key_Access SF_Clearing_of_Sensitive_Information SF_Key_Destruction SF_Random_Number_Generation SF_Encryption_and_Decryption SF_Signature
SF.KEY_MGT	SF_Key_Access SF_Key_Generation SF_Clearing_of_Sensitive_Information SF_Key_Destruction
SF.CONF	N/A
SF.ESERVICE	SF_Key_Access SF_Message_Digest_Generation SF_Encryption_and_Decryption SF_Signature
SF.EAVESDROPPING_PROTECTION	SF_Prepersonalization SF_Resident_Application_Dispatcher SF_Manufacturer_Authentication
SF.SAFESTATE_MGT	SF_Exception SF_Data_Coherency SF_Memory_failure SF_Hardware_Operating SF_Atomic_Transactions SF_data_integrity SF_Random_Number_Generation SF_Signature
SF.PHYS	SF_Unobservability SF_Security_Functions_of_the IC

4.1.4 Dependencies of the Security functions

This section shows that the security functions are complete and internally consistent by showing that they are mutually supportive and provide an 'integrated effective whole' also with the javacard open platform, on which it is built

ID	Security function	Supported by	
1	SF.PIN_MGT	SF_Cardholder_Verification SF_Clearing_of_Sensitive_Information SF.PHYS SF.SAFESTATE_MGT SF.EAVESDROPPING_PROTECTION	#25 #21 #11 #10 #9
2	SF.SIG	SF_Key_Access SF_Clearing_of_Sensitive_Information SF_Message_Digest_Generation SF_Encryption_and_Decryption SF.PHYS SF.SAFESTATE_MGT SF.EAVESDROPPING_PROTECTION SF.CONF SF.KEY_MGT SF.SM	#40 #21 #17 #16 #11 #10 #9 #7 #6 #5

3	SF.DEV_AUTH	SF_Key_Access SF_Clearing_of_Sensitive_Information SF_Key_Destruction SF_Random_Number_Generation SF_Message_Digest_Generation SF_Encryption_and_Decryption SF_Signature SF.SAFESTATE_MGT SF.PHYS SF.CONF SF.KEY_MGT	#40 #21 #19 #18 #17 #16 #15 #11 #10 #7 #6
4	SF.ADM_AUTH	SF_Key_Access SF_KEY_MANAGEMENT SF_Entity_Authentication/Secure_Channel SF_Clearing_of_Sensitive_Information SF_Key_Destruction SF_Random_Number_Generation SF_Message_Digest_Generation SF_Encryption_and_Decryption SF_Signature SF.PHYS SF.SAFESTATE_MGT SF.CONF SF.KEY_MGT	#40 #36 #34 #21 #19 #18 #17 #16 #15 #11 #10 #7 #6
5	SF.SM	SF_Key_Access SF_Clearing_of_Sensitive_Information SF_Key_Destruction SF_Random_Number_Generation SF_Encryption_and_Decryption SF_Signature SF.PHYS SF.SAFESTATE_MGT SF.DEV_AUTH	#40 #21 #19 #18 #16 #15 #11 #10 #3
6	SF.KEY_MGT	SF_Key_Access SF_Key_Generation SF_Clearing_of_Sensitive_Information SF_Key_Destruction SF.PHYS SF.SAFESTATE_MGT SF.EAVESDROPPING_PROTECTION SF.SM	#40 #23 #21 #19 #11 #10 #9 #5
7	SF.CONF	SF.PHYS SF.SAFESTATE_MGT	#11 #10
8	SF.ESERVICE	SF_Key_Access SF_Message_Digest_Generation SF_Encryption_and_Decryption SF_Signature SF.PHYS SF.SAFESTATE_MGT SF.EAVESDROPPING_PROTECTION	#40 #17 #16 #15 #11 #10 #9
9	SF.EAVESDROPPING_PROTECTION	SF_Prepersonalization SF_Resident_Application_Dispatcher	#39 #33

		SF_Manufacturer_Authentication SF.PHYS SF.SAFESTATE_MGT SF.CONF SF.SM	#32 #11 #10 #7 #5
10	SF.SAFESTATE_MGT	SF_Exception SF_Data_Coherency SF_Memory_failure SF_Hardware_Operating SF_Atomic_Transactions SF_data_integrity SF_Random_Number_Generation SF_Signature SF.PHYS	#29 #28 #27 #26 #22 #20 #18 #15 #11
11	SF.PHYS	SF_Unobservability SF_Security_Functions_of_the IC	#38 #37
12	SF_Firewall		N/A
13	SF_Card_Content_Management		N/A
14	SF_Card_Management_Environment		N/A
15	SF_Signature		N/A
16	SF_Encryption_and_Decryption		N/A
17	SF_Message_Digest_Generation		N/A
18	SF_Random_Number_Generation		N/A
19	SF_Key_Destruction		N/A
20	SF_data_integrity		N/A
21	SF_Clearing_of_Sensitive_Information		N/A
22	SF_Atomic_Transactions		N/A
23	SF_Key_Generation		N/A
24	SF_Key_Distribution		N/A
25	SF_Cardholder_Verification		N/A
26	SF_Hardware_Operating		N/A
27	SF_Memory_failure		N/A
28	SF_Data_Coherency		N/A
29	SF_Exception		N/A
30	SF_DAP_Verification		N/A
31	SF_TOKEN		N/A
32	SF_Manufacturer_Authentication		N/A
33	SF_Resident_Application_Dispatcher		N/A
34	SF_Entity_Authentication/Secure_Channel		N/A
35	SF_GP_Dispatcher		N/A
36	SF_KEY_MANAGEMENT		N/A
37	SF_Security_Functions_of_the IC		N/A
38	SF_Unobservability		N/A
39	SF_Prepersonalization		N/A
40	SF_Key_Access		N/A
41	SF_Key_Agreement		N/A

4.2 Security assurance requirements

This chapter defines the list of the assurance measures required for the TOE security assurance requirements. The EAL4+ is claimed.

4.2.1 Evaluation Assurance Level rationale

The following assurance packages are required:

Measure	Name
AM_ADV	Development
AM_AGD	Guidance
AM_ALC	Life Cycle
AM_ASE	Security target
AM_ATE	Tests
AM_VAN	Vulnerability

4.2.2 ADV : Development

The following components are included:

Component	Level
ADV_ARC	1
ADV_FSP	4
ADV_IMP	1
ADV_INT	N/A
ADV_SPM	N/A
ADV_TDS	3

4.2.3 AGD : Guidance

The following components are included:

Component	Level
AGD_OPE	1
AGD_PRE	1

4.2.4 ALC : Life Cycle

The following components are included:

Component	Level
ALC_CMC	4
ALC_CMS	4
ALC_DEL	1
ALC_DVS	2 – enhanced component
ALC_FLR	N/A
ALC_LCD	1
ALC_TAT	1

Note : ALC_DVS is enhanced

4.2.5 ASE : Security target

The following components are included:

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

4.2.6 ATE : Tests

The following components are included:

Component	Level
ATE_COV	2
ATE_DPT	2 – enhanced component
ATE_FUN	1
ATE_IND	2

Note : ATE_DPT is enhanced

4.2.7 AVA : Vulnerability Analysis

The following component is included:

Component	Level
AVA_VAN	5 –enhanced component

Note : AVA_VAN is enhanced

4.3 EAL augmentations rationale

4.3.1 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.

AVA_VAN.5 has dependencies:

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

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

All these dependencies are fulfilled.

4.3.2 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.

4.3.3 ATE_DPT.2 Testing: security enforcing modules

The selection of the component ATE_DPT.2 provides a higher assurance than the predefined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

ATE_DPT.2 has dependencies:

- ADV_ARC.1
- ADV_TDS.3
- ATE_FUN.1

All these dependencies are fulfilled.

5 Conformance Claims

5.1 Conformance Claim to CC

This Security Target claims conformance to CC version 3.1 with the following documents:

- "Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", September 2012, Version 3.1 revision 4
- "Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements", September 2012, Version 3.1 revision 4
- "Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance requirements", September 2012, Version 3.1 revision 4

Conformance is claimed as follows:

- . Part 1: conformant
- . Part 2: extended with the FCS_RNG.1 and FPT_EMSEC.1. All the other Security requirements have been drawn from the catalogue of requirements in Part 2
- . Part 3: conformant EAL4 augmented with ALC_DVS.2, ATE_DPT.2, and AVA_VAN.5.

5.2 Protection Profile reference

This Security Target claims conformance with the following protection profiles

- Protection Profile «Secure Signature Creation Device Type 2, version 1.04», reference BSI-PP-0005-2002.
- Protection Profile «Secure Signature Creation Device Type 3, version 1.05», reference BSI-PP-0006-2002.

5.3 Conformance Claim rationale

The TOE described in this Security target is conformant with the TOE type described in [SSCD2] and [SSCD3]. The security problem definition of this Security Target is consistent with the one defined in [SSCD2] and [SSCD3] as it was extracted from them.

The TOE claims a demonstrable conformance

However the security problem definition was extended to consider the following behaviour of the TOE

- the various authentication features
- the management of keys
- the life cycle management which separates the phase 6 (under the personalization Agent control) and the phase 7

5.3.1 Rationale for TOE objectives

All the TOE objectives described in [SSCD2] and [SSCD3] are included. The following ones are added:

- **OT.Authentication_Secure** : The TOE enable secure authentication of itself and external entities
- **OT.Privacy_Contactless** : When used in contactless, the TOE ensures privacy of data
- **OT.SCD/SVD_Management** : The TOE does not consider only one couple SCD/SVD but considers several that may be created, erased and loaded all along the TOE life cycle
- **OT.Key_Lifecycle_Security** ; The Toe protects the authentication and eServices keys all over its life cycle
- **OT.Key_Secrecy** : The TOE ensures the secrecy of the authentication and eServices keys
- **OT.TOE_AuthKey_Unique** : When the TOE generates an asymmetric key pair used to authenticate itself, it ensures it will be unique
- **OT.LifeCycle_Management** : The Life cycle of the TOE is splitted in two phases : the first one in which the TOE is under the Personalization Agent control and during which data are loaded in the TOE and during which the TOE can not sign, and the second one in which the TOE can be used by the Signatory to sign
- **OT.eServices** : The TOE realize eServices

None of these new objectives interfere with the security problem definition stated by [SSCD2] and [SSCD3].

5.3.2 Rationale for threats

All the threats present in [SSCD2] and [SSCD3] are included. The following ones are added:

- **T.TOE_ID_Contactless** : Identification of the TOE when used in contactless
- **T.Skimming_Contactless** : Skimming of the TOE when used in contactless
- **T.Eavesdropping_Contactless** : Eavesdropping of the communication when used in contactless
- **T.Key_Divulg** : Divulgation of an authentication of eService key
- **T.Key_Derive** : Derivation of an authentication of eServices key
- **T.TOE_PublicAuthKey_Forgery** : Forgery of the authentication public key of the TOE
- **T.Authentication_Replay** : replay of an authentication protocol

Moreover, **T.Hack_Phys** is extended to address all the threats over the keys stored in the TOE (SCD, SVD, authentication keys and eServices keys)

None of these new threats interfere with the security problem definition stated by [SSCD2] and [SSCD3].

5.3.3 Rationale for Assumptions

No assumptions were added

5.3.4 Rationale for Organisational Security Policies

All the OSPs present in [SSCD2] and [SSCD3] are included. The following ones are added:

- **P.EMSEC_Design** : The development of the TOE was made in order to avoid any exploitable information leakage
- **P.SecurityPolicy_Contactless** :If the TOE is to be used in contactless, a relevant security policy shall be set to protect TOE against traceability and to protect it from skimming.
- **P.LinkSCD_QualifiedCertificate** : there shall exist a link between the SCD used to create the signature and the matching qualified certificate
- **P.ControlOfAppletToBeLoaded_Contactless** : the other applets that might be present shall not enable to trace the TOE when used in contactless
- **P.TOE_PublicAuthKey_Cert** : the TOE contains certificate enabling to use the authentication features of the TOE.
- **P.TOE_Construction** : the recommendations indicated in [**AGD_PRE**] shall be applied to ensure the correct construction of the TOE. This OSP is just added for conformance reasons and does not modify the SPD

None of these new OSPs interfere with the security problem definition stated by [SSCD2] and [SSCD3].

5.3.5 Rationale for Environment objectives

All the Environment objectives present in [SSCD2] and [SSCD3] are included. The following ones are added:

- **OE.AuthKey_Transfer** : the environment ensures the confidentiality and integrity of the authentication keys when transferred in the TOE
- **OE.AuthKey_Unique** : the environment ensures the uniqueness of each TOE authentication keys loaded in the TOE
- **OE.TOE_PublicAuthKey_Transfer** : the environment ensures the authenticity of the authentication public keys when transferred from the TOE
- **OE.SecurityPolicy_Contactless :** The security policy applied by the environment on sensitive data that may be accessed in contactless is correctly defined
- **OE.LinkSCD_QualifiedCertificate :** The environment ensures that when the SCD is updated, the link with the qualified certificate is maintained
- **OE.ControlOfAppletToBeLoaded_Contactless :** When an applet is loaded on the javacard open platform, the applet shall ensure the privacy of the TOE (no tracking)
- **OE.TOE_Construction** : the Personalization Agent shall be a trusted person and be skilled enough to apply the recommendations indicated in [**AGD_PRE**]. This OE is just added for conformance reasons and does not modify the SPD.

None of these new environment objectives interfere with the security problem definition stated by [SSCD2] and [SSCD3].

5.3.6 Rationale for Security requirements

Security requirement of the {SSCD2] and {SSCD3] are defined in this Security target. However, as they are based on previous Common Criteria version (v2.1), some requirements are adapted to CC v3.1 (mainly wording) as well as some dependencies that were modified. In particular, FPT_AMT is replaced by FPT_TEE in CC v3.1.

In the case of the TOE, FPT_TEE is non applicable. With respect to the definition of this SFR, it implies the TOE to perform test on external entities. However, as the TOE does not rely on any external mechanisms to realize the security services and as all the security features are present in the TOE scope, this SFR is non applicable and is withdrawn from the current security target.

Moreover, due to compliance with the CC v3.1, FMT_SMF.1 is added in this current security target

5.4 Security Objectives rationale

5.4.1 Security Objectives coverage

	OT.EMSEC_Design	OT.Lifecycle_Security	OT_SCD_Secrecy	OT_SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.Init	OT.SCD_Unique	OT.SCD_Transfer	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.Authentication_Secure	OT.Privacy_Contactless	OT.SCD/SVD_Management	OT.Key_LifeCycle_Security	OT.Key_Secrecy	OT.TOE_AuthKey_Unique	OT.LifeCycle_Management	OT.eServices	OE.SCD_SVD_Corresp	OE.SCD_Transfer	OE.SCD_Unique	OE.CGA_QCert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend	OE.AuthKey_Transfer	OE.AuthKey_Unique	OE.TOE_PublicAuthKey_Transfer	OE.SecurityPolicy_Contactless	OE.LinkSCD_QualifiedCertificate	E.ControlOfAppletToBeLoaded_ Contactless	OE.TOE_Construction
T.Hack_Phys	X		X			X	X											X																	
T.SCD_Divulg			X							X													X												
T.SCD_Derive									X				X											X											
T.Sig_Forgery	X	X	X	X	X	X	X			X			X									X	X		X	X		X							
T.Sig_Repud	X	X	X	X	X	X	X		X	X	X	X	X							X		X	X	X	X	X		X							
T.SVD_Forgery					X																					X									
T.DTBS_Forgery											X																	X							
T.SigF_Misuse											X	X								X							X	X								
T.TOE_ID_Contactless													X													X							X		
T.Skimming_Contactless													X	X												X									
T.Eavesdropping_Contactless													X																						
T.Key_Divulg														X	X																				
T.Key_Derive													X							X															
T.TOE_PublicAuthKey_Forgery																																X			
T.Authentication_Replay													X																						
A.CGA																																			
A.SCA																																			

A.SCD_Generate								X	X	X							
P.CSP_QCert		X						X			X						
P.QSign					X	X					X	X					
P.Sigy_SSCD			X	X	X					X							
P.EMSEC_Design	X																
P.SecurityPolicy_Contactless							X							X			
P.LinkSCD_QualifiedCertificate															X		
P.ControlOfAppletToBeLoaded_Contactless																X	
P.TOE_PublicAuthKey_Cert													X				
P.TOE_Construction																	X

5.4.2 Security objectives sufficiency

In the following chapter, all refinements to the OSP, Threats and Assumptions of the [SSCD2] and [SSCD3] are indicated in *blue italic letters*.

5.4.2.1 Policies and Security Objective Sufficiency

P.CSP_QCert (CSP generates qualified certificates)

establishes the qualified certificate for the signatory and provides that the SVD matches the SCD that is implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by the TOE by **OT.SCD_SVD_Corresp** and **OE.SCD_SVD_Corresp** concerning the correspondence between the SVD and the SCD, in the TOE IT environment, by **OE.CGA_QCert** for generation of qualified certificates by the CGA, respectively.

P.QSign (Qualified electronic signatures)

provides that the TOE and the SCA may be employed to sign data with qualified electronic signatures, as defined by the Directive [1], article 5, paragraph 1. Directive [1], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The requirement of qualified electronic signatures being based on qualified certificates is addressed by **OE.CGA_QCert**. **OE.SCA_Data_Intend** provides that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. **OT.Sig_Secure** and **OT.Sigy_SigF** address the generation of advanced signatures by the TOE.

P.Sigy_SSCD (TOE as secure signature-creation device)

establishes the TOE as secure signature-creation device of the signatory with practically unique SCD. This is addressed by **OT.Sigy_SigF** ensuring that the SCD is under sole control of the signatory and **OE.SCD_Unique** and **OT.SCD_Unique** ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. **OT.Init** provides that generation of the SCD/SVD pair is restricted to authorised users

P.EMSEC_Design (TOE designed to reduce the E.M. emanations)

ensures that all the sensitive operations that may disclose information through electromagnetic signal are protected. In particular it ensures the memory access, the cryptographic computation, the software execution do not emit any usable data that may be used to find any assets. It addresses **OT.EMSEC_Design**

P.SecurityPolicy_Contactless (Security policy definition)

ensures that the TOE identification data, the access to the RAD, the sending of the VAD is protected against disclosure and eavesdropping. It requires these data to be exchanged through a communication channel ensuring identification of both entity (sender and the TOE) and ensuring protection against disclosure. It is addressed by **OE.SecurityPolicy_Contactless** that guarantees the correct security policy is set to objects/files and by **OT.Privacy_Contactless** that ensures the TOE does apply this security policy.

P.LinkSCD_QualifiedCertificate (Link between a SCD and its qualified certificate)

ensures that the SCA can unambiguously find the qualified certificate matching a SCD chosen to perform a SDO. It is addressed by **OE.LinkSCD_QualifiedCertificate** that ensures a link between the SCD and a unique identifier within the TOE file structure

P.ControlOfAppletToBeLoaded_Contactless (Control of the other applet that may be used on the javacard open platform)

ensures that there is no malicious applet loaded in the TOE that may be used to trace it (by emitting a unique identifier for instance) in case it is used in contactless mode. This is the responsibility of the SSCD Service provider to control the applet loaded in the TOE. It is addressed by **OE.ControlOfAppletToBeLoaded_Contactless** .

P.TOE_PublicAuthKey_Cert (Certificate for asymmetric TOE authentication keys)

ensures that each private key(s) of the TOE for authentication matches the public key stored within the relevant certificate issued by an entitled entity. The authentication public key is exported thanks to **OE.TOE_PublicAuthKey_Transfer**.

P.TOE_Construction (TOE construction)

ensures that all the recommendations indicated in [**AGD_PRE**] are applied. It is addressed by **OE.TOE_Construction**.

5.4.2.2 Threats and Security Objective Sufficiency

T.Hack_Phys (Exploitation of physical vulnerabilities)

deals with physical attacks exploiting physical vulnerabilities of the TOE. **OT.SCD_Secrecy** preserves the secrecy of the SCD, ***OT.Key_Secrecy*** *preserves the secrecy of all the authentication and eServices keys stored in the TOE*. Physical attacks through the TOE interfaces or observation of TOE emanations are countered by **OT.EMSEC_Design**. **OT.Tamper_ID** and **OT.Tamper_Resistance** counter the threat **T.Hack_Phys** by detecting and by resisting tamper attacks.

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

addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [1], recital (18). This threat is countered by **OT.SCD_Secrecy** which assures the secrecy of the SCD used for signature generation. **OT.SCD_Transfer** and **OE.SCD_Transfer** ensures the confidentiality of the SCD transferred between SSCDs.

T.SCD_Derive (Derive the signature-creation data)

deals with attacks on the SCD via public known data produced by the TOE. This threat is countered by **OE.SCD_Unique** (in case of SCD import) and **OT.SCD_Unique** (in case of key generation) that provides cryptographic secure generation of the SCD/SVD-pair. **OT.Sig_Secure** ensures cryptographic secure electronic signatures.

T.Sig_Forgery (Forgery of the electronic signature)

deals with non-detectable forgery of the electronic signature. This threat is in general addressed by **OT.Sig_Secure** (Cryptographic security of the electronic signature), **OE.SCA_Data_Intend** (SCA sends representation of data intended to be signed), **OE.CGA_QCert** (Generation of qualified certificates), **OT.SCD_SVD_Corresp** and **OE.SCD_SVD_Corresp** (Correspondence between SVD and SCD), **OT.SVD_Auth_TOE** (TOE ensures authenticity of the SVD), **OE.SVD_Auth_CGA** (CGA proves the authenticity of the SVD), **OT.SCD_Secrecy** and **OT.SCD_Transfer** (Secrecy of the signature-creation data), **OT.SCD_Transfer** (Secure transfer of SCD between SSCD), **OT.EMSEC_Design** (Provide physical emanations security), **OT.Tamper_ID** (Tamper detection), **OT.Tamper_Resistance** (Tamper resistance) and **OT.Lifecycle_Security** (Lifecycle security), as follows: **OT.Sig_Secure** ensures by means of robust encryption techniques that the signed data and the electronic signature are securely linked together. **OE.SCA_Data_Intend** provides that the methods

used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation is appropriate for the cryptographic methods employed to generate the electronic signature. The combination of **OE.CGA_QCert**, **OT.SCD_SVD_Corresp**, **OT.SVD_Auth_TOE**, and **OE.SVD_Auth_CGA** provides the integrity and authenticity of the SVD that is used by the signature verification process. **OT.Sig_Secure**, **OT.SCD_Secrecy**, **OT.SCD_Transfer**, **OT.EMSEC_Design**, **OT.Tamper_ID**, **OT.Tamper_Resistance**, and **OT.Lifecycle_Security** ensure the confidentiality of the SCD implemented in the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

T.Sig_Repud (Repudiation of electronic signatures)

deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by **OE.CGA_QCert** (Generation of qualified certificates), **OT.SVD_Auth_TOE** (TOE ensures authenticity of the SVD), **OE.SVD_Auth_CGA** (CGA proves the authenticity of the SVD), **OT.SCD_SVD_Corresp** and **OE.SCD_SVD_Corresp** (Correspondence between SVD and SCD), **OT.SCD_Unique** and **OE.SCD_Unique**(Uniqueness of the signature-creation data), **OT.SCD_Transfer** and **OE.SCD_Transfer** (Secure transfer of SCD between SSCD), **OT.SCD_Secrecy** (Secrecy of the signature-creation data), **OT.EMSEC_Design** (Provide physical emanations security), **OT.Tamper_ID** (Tamper detection), **OT.Tamper_Resistance** (Tamper resistance), **OT.Lifecycle_Security** (Lifecycle security), **OT.Sigy_SigF** (Signature generation function for the legitimate signatory only), **OT.Sig_Secure** (Cryptographic security of the electronic signature), **OE.SCA_Data_Intend** (SCA sends representation of data intended to be signed) and **OT.DTBS_Integrity_TOE** (Verification of the DTBS-representation integrity). **OE.CGA_QCert** ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. **OE.CGA_QCert**, **OT.SVD_Auth_TOE** and **OE.SVD_Auth_CGA** ensure the integrity of the SVD. **OE.CGA_QCert** and **OT.SCD_SVD_Corresp** ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. **OT.SCD_Unique** provides that the signatory's SCD can practically occur just once. **OT.Sig_Secure**, **OT.SCD_Transfer**, **OT.SCD_Secrecy**, **OT.Tamper_ID**, **OT.Tamper_Resistance**, **OT.EMSEC_Design**, and **OT.Lifecycle_Security** ensure the confidentiality of the SCD implemented in the signatory's SSCD. **OT.Sigy_SigF** provides that only the signatory may use the TOE for signature generation. **OT.Sig_Secure** ensures by means of robust cryptographic techniques that valid electronic signatures may only be generated by employing the SCD corresponding to the SVD that is used for signature verification and only for the signed data. **OE.SCA_Data_Intend** and **OT.DTBS_Integrity_TOE** ensure that the TOE generates electronic signatures only for DTBS-representations which the signatory has decided to sign as DTBS.
OT.LifeCycle_Management *ensures that when the TOE is under the Personalizer control, it can not be misused to sign on behalf of the legitimate Signatory.*

T.SVD_Forgery (Forgery of the signature-verification data)

deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. **T.SVD_Forgery** is addressed by **OT.SVD_Auth_TOE** which ensures that the TOE sends the SVD in a verifiable form to the CGA, as well as by **OE.SVD_Auth_CGA** which provides verification of SVD authenticity by the CGA.

T.DTBS_Forgery (Forgery of the DTBS-representation)

addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which then does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The TOE counters this threat by the means of **OT.DTBS_Integrity_TOE** by verifying the integrity of the DTBS-representation. The TOE IT environment addresses **T.DTBS_Forgery** by the means of **OE.SCA_Data_Indent**.

T.SigF_Misuse (Misuse of the signature-creation function of the TOE)

addresses the threat of misuse of the TOE signature-creation function to create Signed Data Object by others than the signatory to create SDO for data the signatory has not decided to sign, as required by the Directive [1],Annex III, paragraph 1, literal (c). This threat is addressed by the **OT.Sigy_SigF** (Signature generation function for the legitimate signatory only), **OE.SCA_Data_Intend** (Data intended to be signed), **OT.DTBS_Integrity_TOE** (Verification of the DTBS-representation integrity), and **OE.HI_VAD** (Protection of the VAD) as follows: **OT.Sigy_SigF** ensures that the TOE provides the signature-generation function for the legitimate signatory only. **OE.SCA_Data_Intend** ensures that the SCA sends the DTBS-representation only for data the signatory intends to sign. The combination of **OT.DTBS_Integrity_TOE** and **OE.SCA_Data_Intend** counters the misuse of the signature generation function by means of manipulation of the channel between the SCA and the TOE. If the SCA provides the human interface for the user authentication, **OE.HI_VAD** provides confidentiality and integrity of the VAD as needed by the authentication method employed.
OT.LifeCycle_Management *ensures that when the TOE is under the Personalizer control, it can not be misused to sign on behalf of the legitimate Signatory..*

T.TOE_ID_Contactless (Identification of the TOE)

deals with the threats for the TOE to be traced when used in contactless. This threat is addressed by **OE.SecurityPolicy_Contactless** that ensures that identification data stored by TOE can not be disclosed to an unauthenticated entity, and **OT.Privacy_Contactless** that ensures that this security policy is enforced: sensitive data (including the identification data) managed by the TOE are protected against retrieval by an unauthorized entity. **OE.ControlOfAppletToBeLoaded_Contactless** ensures that when an applet is loaded in the javacard open platform, it does not endanger the privacy of the TOE and of the holder.

T.Skimming_Contactless (skimming of the TOE)

deals with the threats of an attacker accessing the TOE by imitating an entitled device. **OT.Authentication_Secure** ensures it is very difficult for the attacker to imitate an entitled device as the cryptographic techniques are very resistant. **OE.SecurityPolicy_Contactless** ensures a suitable security policy is applied, so that authentication of the TOE and the external entity is applied prior to access data, and that exchanges are protected in confidentiality (for the sole recipient) and proves the authenticity of the sender. **OT.Privacy_Contactless** ensures this security policy is enforced.

T.Eavesdropping_Contactless (eavesdropping of the communication)

deals with the threats of an attacker listening to communication between the TOE and a device to get sensitive information. This is addressed by **OT.Privacy_Contactless** that ensures sensitive data are exchanged through an encrypted channel with an authenticated entity.

T.Key_Divulg (storing, copying and releasing a key)

addresses the threat against the (1) authentication key of the TOE, (2) the authentication keys of entities and (3) the eServices keys stored in the TOE due to storage and copying of key(s) outside the TOE. This threat is countered by **OT.Key_Secrecy** which assures the secrecy of the keys stored and used by the TOE. **OE.AuthKey_Transfer** ensures the confidentiality of the authentication keys transferred to the TOE.
OT.Key_Lifecycle_Security (Lifecycle security) ensures the secrecy of the keys stored in the TOE during the whole life of the TOE.

T.Key_Derive (Derive a key)

deals with attacks on authentication and eServices keys via public known data produced or received by the TOE (public key, authentication cryptogram,…). This threat is countered by **OE.AuthKey_Unique** (in case of import) and **OT.TOE_AuthKey_Unique** (in case of TOE's authentication key generation) that provides cryptographic secure generation of the keys. **OT.Authentication_Secure** ensures secure authentication cryptograms.

T.TOE_PublicAuthKey_Forgery (Forgery of the public key of a TOE authentication key)

deals with the forgery of the TOE's public key used for authentication exported by the TOE to an entitled entity for the generation of the certificate. This is addressed by **OE.TOE_PublicAuthKey_Transfer** which ensures the authenticity of the TOE's public key for authentication.

T.Authentication_Replay (Replay of an authentication of an external entity)

deals with the threats an attacker retrieves an authentication cryptogram presented to the TOE by an entity and present it again to the TOE is order to grant some rights in order to gain access to some data on the TOE. This is addressed by **OT.Authentication_Secure** that ensures the authentication cryptogram can not be replayed as they rely on random data internally generated by the TOE;

5.4.2.3 Assumption and Security Objective Sufficiency

A.CGA (Trustworthy certification-generation application)

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

A.SCA (Trustworthy signature-creation application)

establishes the trustworthiness of the SCA according to the generation of DTBS-representation. This is addressed by **OE.SCA_Data_Intend** (Data intended to be signed) which ensures that the SCA generates the DTBS-representation of the data that has been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE

A.SCD_Generate (Trustworthy SCD/SVD generation)

establishes a trustworthy SCD/SVD pair. This that the SCD must be unique, objective met by **OE.SCD_Unique**, that the SCD and the SVD must correspond, objective met by **OE.SCD_SVD_Corresp**. The secrecy of the SCD must be maintained while it is transferred to the TOE before being deleted, **OE.SCD_Transfer**.

6 Annex A : Extended Family

6.1 Definition of FPT_EMSEC

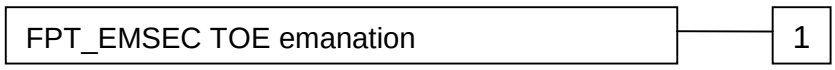
The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2.

The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6.2 Definition of FCS_RNG

See [**ST_PLATFORM**] for definition