

# SECURITY TARGET CPS2TER APPLICATION ON ID-ONE COSMO V8.2

ISSUE: 6

## Verification and approval

Function	Name	Visa
Certification Manager	D.BOULY	
Certification Project Manager	S.BOUKYOUD	

CIRCULATION LIST : SEE FQR 110 8971

DOCUMENT REVISION HISTORY			
Issue	Date	Author	Purpose
0.1	10/01/2019	IDEMIA	Initial version
0.2	27/01/2019	IDEMIA	Review and update
1.0	05/02/2019	IDEMIA	Review and update
2.0	23/05/2019	IDEMIA	Review and update
3.0	03/10/2019	IDEMIA	Review and update
4.0	05/09/2022	IDEMIA	Update IC, PTF certificates references and guides references, §1.2 and §1.3
5.0	10/10/2022	IDEMIA	Update following lab comments
6.0	07/04/2023	IDEMIA	Update AGD_OPE version

## Table of contents

<b>1</b>	<b>SECURITY TARGET INTRODUCTION .....</b>	<b>7</b>
1.1	ST IDENTIFICATION .....	7
1.2	TOE REFERENCE.....	7
1.3	TOE DOCUMENTATION .....	8
<b>2</b>	<b>TOE DESCRIPTION .....</b>	<b>9</b>
2.1	TOE OVERVIEW .....	9
2.1.1	<i>TOE type &amp; scope .....</i>	<i>9</i>
2.1.2	<i>Required non-TOE hardware/software/firmware .....</i>	<i>10</i>
2.2	TOE DESCRIPTION .....	11
2.2.1	<i>Global architecture.....</i>	<i>11</i>
2.2.2	<i>Platform functions.....</i>	<i>11</i>
2.2.3	<i>IAS ECC functions .....</i>	<i>12</i>
2.2.4	<i>CPS2ter functions.....</i>	<i>12</i>
2.2.5	<i>Out of scope features.....</i>	<i>13</i>
2.3	TOE PRODUCT LIFE CYCLE .....	14
2.3.1	<i>Card life cycle .....</i>	<i>14</i>
2.3.2	<i>Description of the TOE environment.....</i>	<i>15</i>
2.3.3	<i>Coverage of the different Life cycle state by the assurance components AGD &amp; ALC .....</i>	<i>17</i>
2.3.4	<i>Application life cycle.....</i>	<i>17</i>
<b>3</b>	<b>CONFORMANCE CLAIMS .....</b>	<b>19</b>
3.1	COMMON CRITERIA CONFORMANCE .....	19
3.2	PACKAGE CONFORMANCE .....	19
3.3	PROTECTION PROFILE CONFORMANCE .....	19
<b>4</b>	<b>SECURITY PROBLEM DEFINITION.....</b>	<b>20</b>
4.1	ASSETS.....	20
4.2	USERS / SUBJECTS.....	21
4.3	THREATS.....	21
4.4	ORGANISATIONAL SECURITY POLICIES .....	23
4.5	ASSUMPTIONS .....	23
<b>5</b>	<b>SECURITY OBJECTIVES .....</b>	<b>25</b>
5.1	SECURITY OBJECTIVES FOR THE TOE .....	25
5.2	SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT .....	26
<b>6</b>	<b>EXTENDED REQUIREMENTS.....</b>	<b>27</b>
6.1	EXTENDED FAMILY FCS_RNG - RANDOM NUMBER GENERATION .....	27
<b>7</b>	<b>SECURITY FUNCTIONAL REQUIREMENTS .....</b>	<b>28</b>
7.1	SECURITY FUNCTIONAL REQUIREMENTS .....	28
7.1.1	<i>Attributes .....</i>	<i>28</i>
7.1.2	<i>CHV .....</i>	<i>28</i>
7.1.3	<i>External authentication.....</i>	<i>30</i>
7.1.4	<i>Internal Authentication.....</i>	<i>32</i>
7.1.5	<i>Exchanges .....</i>	<i>32</i>
7.1.6	<i>File secure management.....</i>	<i>33</i>
7.1.7	<i>Transactions protection .....</i>	<i>37</i>
7.1.8	<i>Cryptography.....</i>	<i>38</i>
7.1.9	<i>TOE protection.....</i>	<i>39</i>

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>3/66</b>
-----------------------	-----------------	--------------------------	-------------

7.2	SECURITY ASSURANCE REQUIREMENTS.....	39
<b>8</b>	<b>TOE SUMMARY SPECIFICATION .....</b>	<b>40</b>
8.1	TOE SUMMARY SPECIFICATION.....	40
<b>9</b>	<b>RATIONALES .....</b>	<b>42</b>
9.1	SECURITY OBJECTIVES / SECURITY PROBLEM DEFINITION .....	42
9.1.1	<i>Threats .....</i>	<i>42</i>
9.1.2	<i>Organisational Security Policies .....</i>	<i>44</i>
9.1.3	<i>Assumptions .....</i>	<i>44</i>
9.1.4	<i>SPD and Security Objectives .....</i>	<i>44</i>
9.2	SECURITY REQUIREMENTS / SECURITY OBJECTIVES .....	47
9.2.1	<i>Objectives .....</i>	<i>47</i>
9.2.2	<i>Rationale tables of Security Objectives and SFRs.....</i>	<i>50</i>
9.3	DEPENDENCIES .....	52
9.3.1	<i>SFRs dependencies .....</i>	<i>52</i>
9.3.2	<i>SARs dependencies .....</i>	<i>53</i>
9.4	SFRs / TSS .....	55
9.5	EAL RATIONALE .....	56
9.6	EAL AUGMENTATIONS RATIONALE .....	56
9.6.1	<i>AVA_VAN.5 Advanced methodical vulnerability analysis .....</i>	<i>56</i>
9.6.2	<i>ALC_DVS.2 Sufficiency of security measures .....</i>	<i>57</i>
<b>10</b>	<b>STATEMENT OF COMPATIBILITY.....</b>	<b>58</b>
10.1	COMPATIBILITY BETWEEN SFRS .....	58
10.2	COMPATIBILITY BETWEEN OTs .....	59
10.3	COMPATIBILITY BETWEEN OEs.....	60
10.4	COMPATIBILITY BETWEEN AS.....	60
10.5	COMPATIBILITY BETWEEN OSPs.....	61
10.6	COMPATIBILITY BETWEEN Ts.....	61
10.7	COMPATIBILITY BETWEEN SFs .....	63
10.8	COMPATIBILITY OF ASSURANCE REQUIREMENTS .....	64
<b>11</b>	<b>GLOSSARY .....</b>	<b>65</b>
<b>12</b>	<b>REFERENCES.....</b>	<b>66</b>

**List of figures**

Figure 1 Smartcard architecture overview .....	10
Figure 2 TOE functional architecture .....	11
Figure 3 CPS2ter security features overview .....	13
Figure 4 CPS2ter applet lifecycle .....	18
Figure 5 ACs lattice .....	36

**List of tables**

Tableau 1 Threats and Security Objectives - Coverage.....	44
Tableau 2 Security Objectives and Threats - Coverage.....	45
Tableau 3 OSPs and Security Objectives - Coverage .....	45
Tableau 4 Security Objectives and OSPs - Coverage .....	46
Tableau 5 Assumptions and Security Objectives for the Operational Environment - Coverage.....	46
Tableau 6 Security Objectives for the Operational Environment and Assumptions - Coverage.....	46
Tableau 7 Security Objectives and SFRs - Coverage.....	50
Tableau 8 SFRs and Security Objectives .....	51
Tableau 9 SFRs dependencies .....	52
Tableau 10 SARs dependencies .....	54
Tableau 11 SFRs and TSS - Coverage.....	55
Tableau 12 TSS and SFRs - Coverage.....	56

## 1 Security Target introduction

### 1.1 ST Identification

<b>Title</b>	Security Target CPS2ter Application on ID-One Cosmo v8.2
<b>Reference</b>	FQR 110 9044
<b>Version</b>	6
<b>Date of Issue</b>	04/04/2023
<b>ITSEF</b>	CEA-LETI
<b>Certification Body</b>	ANSSI
<b>Author</b>	IDEMIA
<b>CC Version</b>	3.1 Revision 5
<b>Assurance Level</b>	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
<b>Protection Profiles</b>	n/a

### 1.2 TOE Reference

The TOE is made up with the following components:

CPS2ter technical identification:

Name	CPS2ter Java Applet
Software identification (code SAAAAR)	0708312
Patch code identification (code SAAAAR)	093072

IAS ECC technical identification:

Name	IAS ECC Applet
Software identification (code SAAAAR)	077234
Certificates	ANSSI-CC-2019/33, ANSSI-CC-2019/34, ANSSI-CC-2019/35, ANSSI-CC-2019/36

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>7/66</b>
-----------------------	-----------------	--------------------------	-------------

Platform technical identification:

Name	ID-One Cosmo v8.2
Software identification (code SAAAAR)	091121
Platform Certificate	[PLT]

IC identification:

Name:	NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software
IC Certificate	[IC-cert]

### 1.3 TOE Documentation

The TOE documentation is listed in the table below:

<b>[AGD_PRE]</b>	GIP-CPS on ID-One Cosmo v8.2 - AGD_PRE Pre-Personalization Guide, FQR 110 8975 Ed3. IDEMIA
<b>[AGD_OPE]</b>	GIP-CPS on ID-One Cosmo v8.2 - AGD_OPE Reference Guide, FQR 110 8976 Ed2. IDEMIA
<b>[AGD_Platform]</b>	ID-One Cosmo V8.2 Pre-Perso Guide, FQR 110 8875 Ed9. IDEMIA ID-One Cosmo v8.2 Reference Guide, FQR 110 8885 Ed8. IDEMIA ID-One Cosmo v8.2 Security Recommendations, FQR 110 8963 Ed4. IDEMIA

## 2 TOE DESCRIPTION

This part of the ST describes the TOE as an aid to the understanding of its security requirements and addresses the product type, the TOE scope, the intended usage and the general features of the TOE.

### 2.1 TOE OVERVIEW

#### 2.1.1 TOE type & scope

The TOE is composed of the ID-One Cosmo v8.2 Java Card platform including an IAS ECC applet and a loaded applet also called CPS2ter, for secure storage of medical data and access to sensitive distant services. Therefore, the TOE is a smartcard providing the services of both IAS and CPS2ter on the same device. This intends to allow a smooth migration from the current technology of the “Agence des Systèmes d’Information Partagés de Santé” (ASIP Santé) known as CPS2ter to the future one called “CPS3” based on the “Identification, Authentication et Signature” standard (IAS). The CPS2ter application is an emulation in Java Card of the old native card executed besides and behind IAS considered as a front-end; if old APDUs dedicated to CPS2ter are detected they are automatically forwarded to CPS2ter by IAS for processing.

The Target of Evaluation (TOE) is defined by:

- an underlying Integrated Circuit (IC);
- the ID-One Cosmo v8.2 Java Card platform including Global Platform support;
- IAS ECC Applet running in contact and contactless;
- the CPS2ter Applet (with its patch code) running in contact mode only,

The product is closed, so that it is not possible to load any other applet after the point of delivery.

The Figure below gives a description of the TOE and its boundaries.

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>9/66</b>
-----------------------	-----------------	--------------------------	-------------

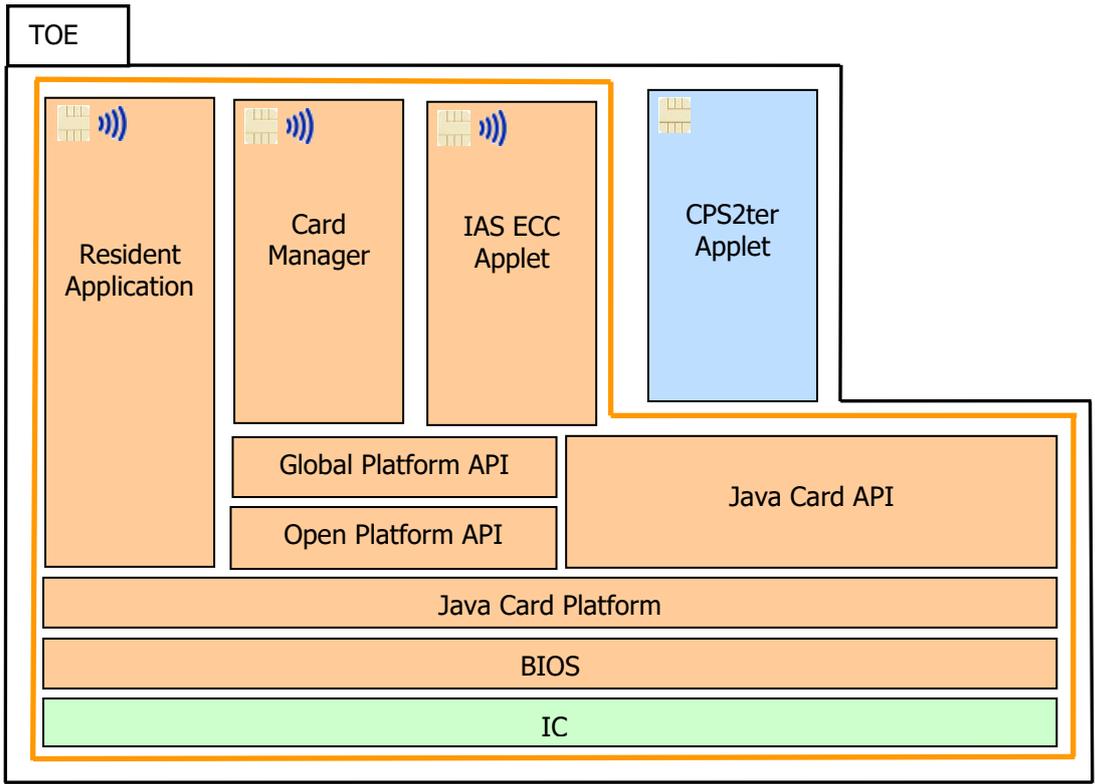


Figure 1 Smartcard architecture overview

2.1.2 Required non-TOE hardware/software/firmware

The TOE is an independent product and does not need any additional hardware/software/firmware to ensure its security.

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

All rights of IDEMIA are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

## 2.2 TOE DESCRIPTION

### 2.2.1 Global architecture

The purpose of the current Security Target is to specify and formalize security requirements of the CPS2ter application. Nevertheless, since it relies on both IAS and platform services, those entities are integrated in the current TOE.

For the enforcement of its security functionalities, CPS2ter relies on:

- the ID-One Cosmo v8.2 platform which provides a secure execution context and secures APIs, especially for key storage,
- the IAS shareable services for the management of PIN and the forwarding of APDUs.

The current CPS2ter application is considered as a bridge from old to new technology. Therefore one of the main objective is to migrate in a way users are unable to detect the evolution. That's why terminals will send all commands to IAS which will be responsible for forwarding if required to the correct application.

In the same way, managing PIN by IAS allows keeping PIN data when migrating to a full IAS infrastructure.

It is important to note that CPS2ter applet will be able to be addressed directly in “selectable mode” in order to ease the personalisation process.

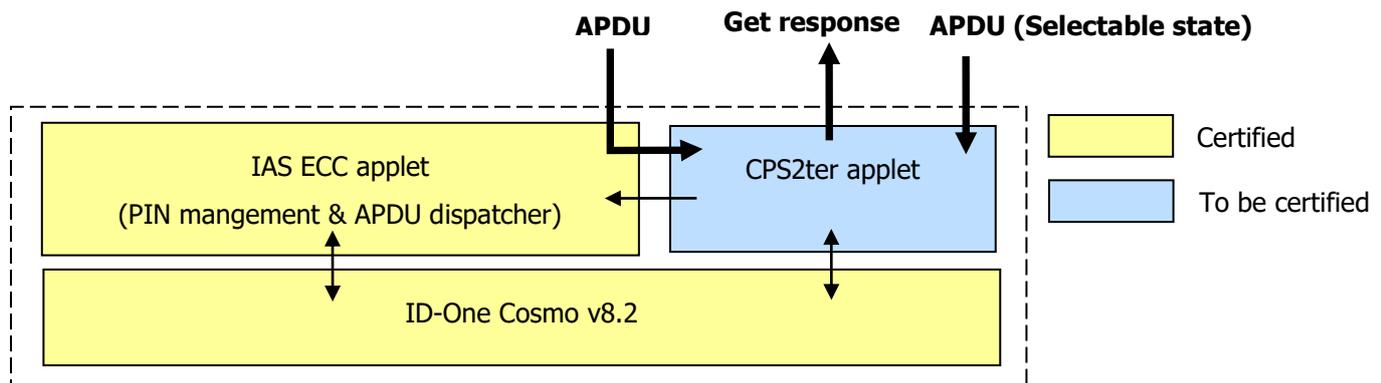


Figure 2 TOE functional architecture

### 2.2.2 Platform functions

The Operating System is based on Java Card technology [JCRE], [JCVM], [JCAPI] and Global Platform technology [GP]. His main responsibilities are:

- providing interface between the Integrated Circuit and the applet
- providing to the applet, basic services to access to memories and all needed cryptographic operations
- ensuring global management of the card (loading, installation and deletion of applets) and monitor the security of the card (data integrity and physical attacks counter-measures).

For details see [COSMO-ST].

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>11/66</b>
-----------------------	-----------------	--------------------------	--------------

### 2.2.3 IAS ECC functions

IAS ECC is conformant to [IAS] specifications and provides the following services via a shareable interface to other applets.

#### 2.2.3.1 PIN management

The IAS ECC applet may be used as a SSO (single sign on). The user may validate its PIN through IAS ECC application and any other applet may rely on this PIN to decide to grant access or not to the user.

This functionality enables to give access to the global PINs (located within the root) the IAS ECC applet manages to any other applet without endangering the PINs' values.

Still, the IAS ECC enforces its security policy prior to granting access to the global PINs: the PIN verification, the PIN change, the PIN reset, the PIN reset and change are still protected with the same security policy, even when these operations are performed through shared interfaces.

#### 2.2.3.2 APDU dispatcher feature

The IAS ECC applet may be used as an APDU dispatcher to another applet. When this feature is activated, the IAS ECC application behaves as if the two applets were selected at the same time:

- IAS ECC applet process all the APDU with the pair (CLA | INS) is known ,
- IAS ECC applet transfers the APDU to CPS2ter when the pair (CLA | INS) is unknown. The APDU is totally processed by the target applet.

The two applets are coupled together in phase 5 (see 2.3.1) during personalisation.

For details on IAS ECC see [IAS ECC-ST].

### 2.2.4 CPS2ter functions

The TOE implements a secure storage device allowing to access to sensitive data about the user when correctly authenticated and authorized using the following services:

- Import of PINs and keys (protected by 3DES),
- Pin Authentication of the user: the TOE holds the reference CHVs that is used to verify the CHVs provided by the user,
- Export of user data,
- Random number generation,
- External authentication of distant entities for user data access (3DES based protocol),
- Protection of incoming commands using the PRO mode (protected by 3DES),
- Implementation of a trusted channel for personalisation (GP channel).

The trusted channel which can be used in personalisation (i.e. "Selectable" state of the applet) is no longer available in "Personalised" state. Symmetrically, access rights checking are not activated in "Selectable" state and operational starting from the transition to "Personalised" state.

Note: PIN secure management is enforced by the IAS shareable service.

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>12/66</b>
-----------------------	-----------------	--------------------------	--------------

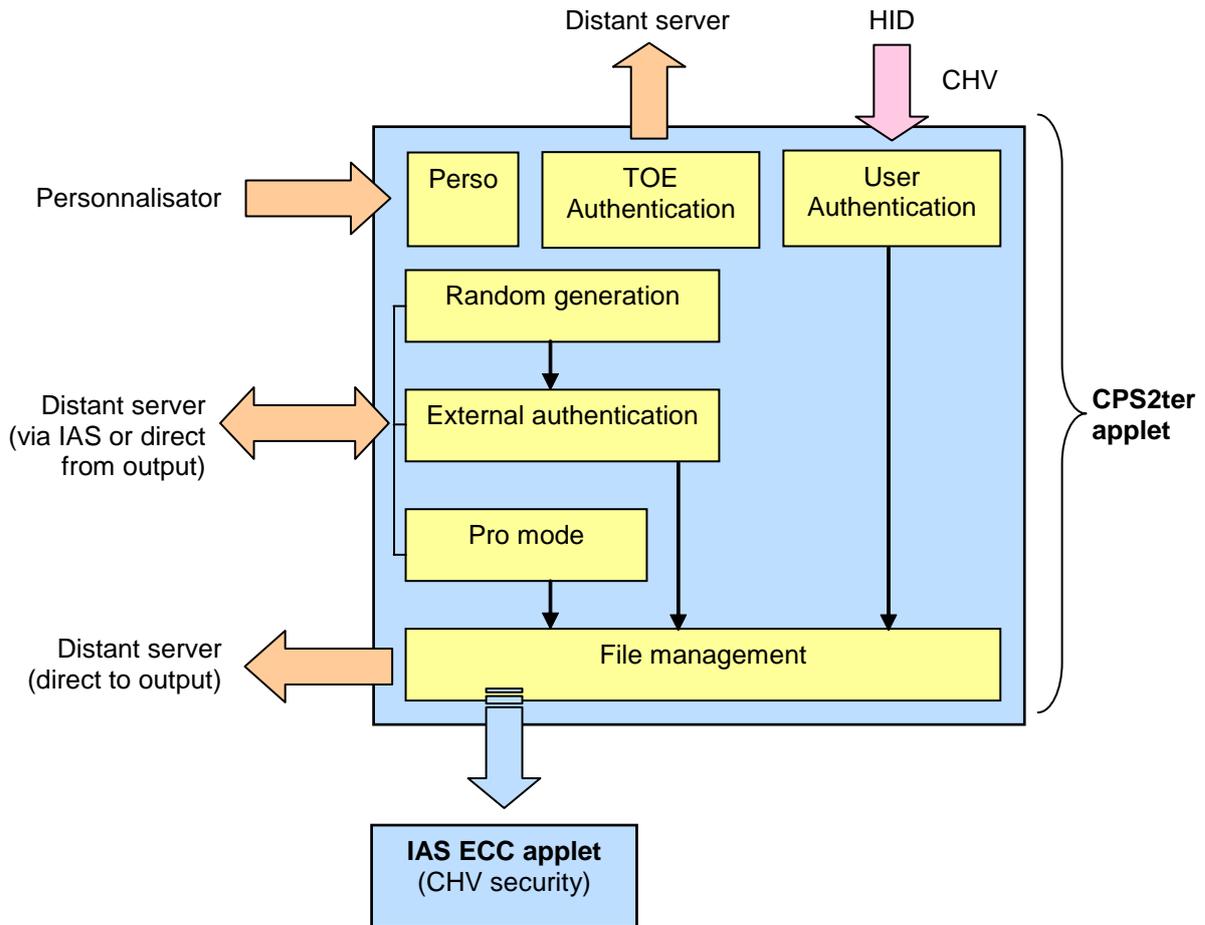


Figure 3 CPS2ter security features overview

For more information about CPS2ter security features see [SRS].

### 2.2.5 Out of scope features

Some features are put out of the evaluation scope and are therefore not part of the TSF. Here is the complete list of those functionalities:

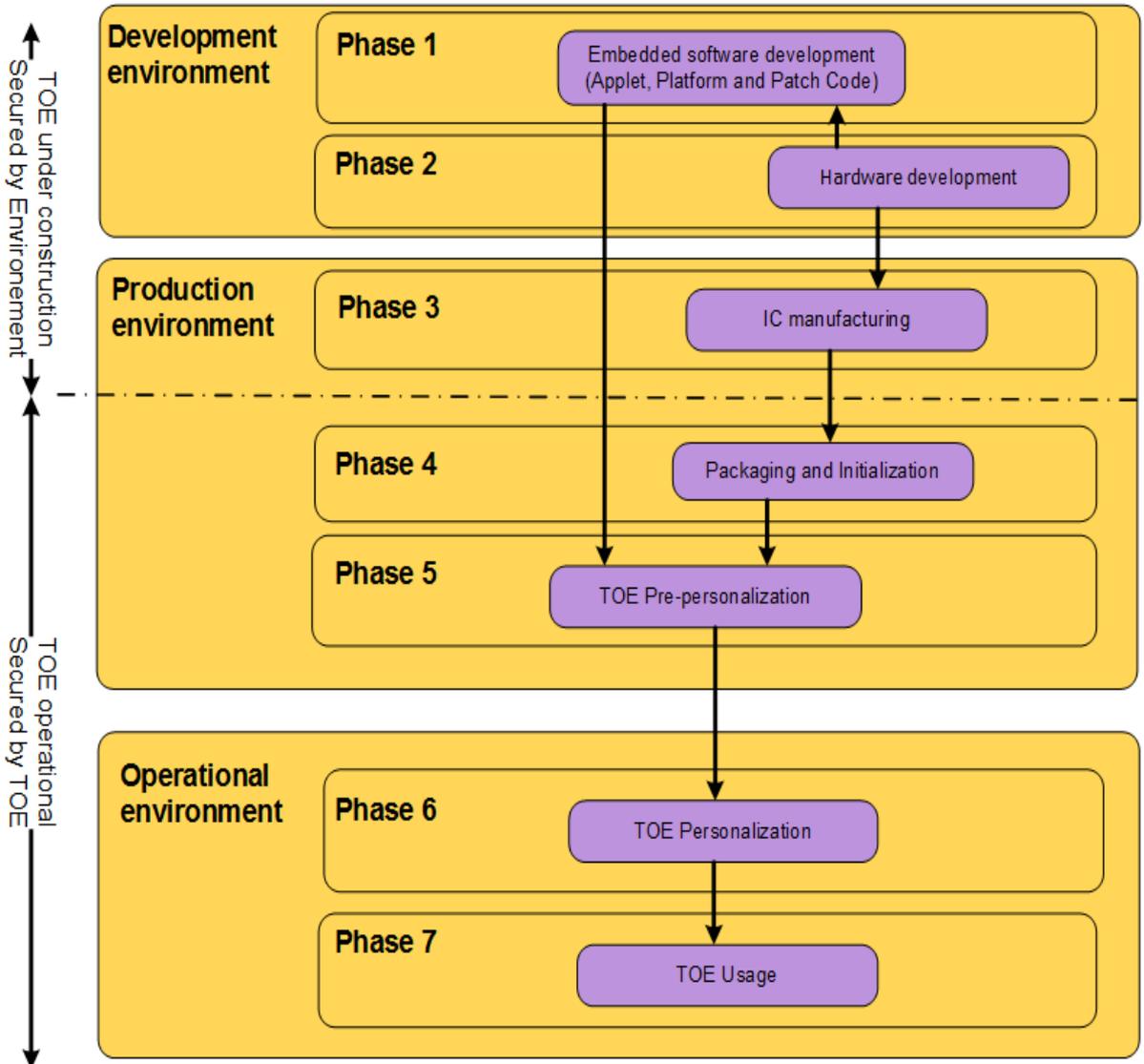
- Computation of signature using RSA (through command “Calcul Secret RSA”),
- Internal authentication using RSA (through command “Calcul Secret RSA”),
- Protection in integrity and proof of origin of exported Files data (through command “Read Binary Stamped”).

## 2.3 TOE product life cycle

### 2.3.1 Card life cycle

The Smart card product life cycle is split up into 7 phases<sup>1</sup> where evaluation scope (i.e. evaluation phases under the developer's responsibility) goes from phase 1 to phase 3.

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



<sup>1</sup> For details regarding phases see [COSMO-ST].

### 2.3.2 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 and tested.
- The **Production environment**, in which the TOE is under construction. The security requirements of the Java Card platform 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.

#### 2.3.2.1 Development environment

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

- the Java Card platform components;
- the Java Card applet and its patch code;
- the hardware.

##### 2.3.2.1.1 Software development (phase 1)

This development environment of the Java Card applet, its patch code and the Java Card platform is enforced by **IDEMIA**.

The confidentiality and integrity of the cap files, the patch code and the Java Card platform is covered by the evaluation of the development premises of **IDEMIA**.

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

- Access control to **IDEMIA** 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 Java Card applet together with the Java Card platform are transferred to the IC manufacturer in order to be masked on silicium. The patch code is transferred to the Manufacturing Agent in order to be loaded during the pre-personnalization of the Java Card platform (Phase 5).

**At the end of this phase 1, the Java Card applet is protected in integrity and confidentiality.**

This phase takes place in **IDEMIA** premises and is covered by ALC.

##### 2.3.2.1.2 Hardware development (Phase 2)

In this phase, the underlying integrated circuit is developed.

This phase takes place at the NXP manufacturing site and is covered by ALC.

The confidentiality and integrity of the Java Card applet and Java Card platform is covered by the evaluation of the development premises of the silicium manufacturer.

### 2.3.2.2 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 Java Card platform.
- The chip is mounted on a physical layout (card, USB token...)
- The Java Card platform is prepersonalized including patch code loading
- The Java Card platform is personalized
- The applet is instantiated

#### 2.3.2.2.1 IC manufacturing (phase 3)

In this phase, the code of the Java Card platform and the Java Card applet are masked on the IC. This phase takes place at the NXP manufacturing site.

The confidentiality and integrity of the Java Card applet and Java Card platform is covered by the evaluation of the development premises of the silicium manufacturer.

**At the end of phase 3, the Java Card platform and the TOE are self-protected: all its security functions are activated. The point of delivery of the TOE is the end of phase 3.**

#### 2.3.2.2.2 TOE packaging and initialization (phase 4)

This phase is performed by the Manufacturing Agent, which controls the TOE that is in charge of the packaging and initialization of the Java Card platform.

This phase spans the phase 4 of the Java Card platform life cycle and is covered by the platform preparative guidances [AGD\_Platform].

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

#### 2.3.2.2.3 TOE pre-personalization (phase 5)

The Java Card platform is under the control of the **Manufacturing Agent**.

During this phase, the Java Card platform is pre-personalized (including loading of the patch code) and personalized by the Manufacturing Agent. This subject shall be authenticated prior to any action on the Java Card platform.

The main operations performed by the **Manufacturing Agent** during this phase are the following:

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

This phase spans the phases 5, 6 and 7 of the Java Card platform and and is covered by the platform preparative and operational guidances [AGD\_Platform].

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

### 2.3.2.3 Operational environment

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

- Personalization of the TOE
- Use of the TOE

#### 2.3.2.3.1 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 Java Card 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 TOE is personalized as described in [AGD\_PRE]

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

#### 2.3.2.3.2 TOE Usage (phase 7)

The TOE can be used as described in [AGD\_OPE]

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

The following table indicates for each step of the life cycle, whether it is covered by ALC or AGD class:

Life cycle state	Covered by	Site
Phase 1	ALC (IDEMIA R&D)	Courbevoie and Pessac
Phase 2	ALC (IC)	IC certification [IC-cert]
Phase 3	ALC (IC)	IC certification [IC-cert]
<b>TOE delivery</b>		
Phase 4	AGD_PRE [PLT]	IDEMIA plant sites or another agent
Phase 5	AGD_PRE [PLT] AGD_OPE [PLT] [AGD_PRE]	IDEMIA plant sites or another agent
Phase 6	[AGD_PRE]	IDEMIA plant sites or another agent
Phase 7	[AGD_OPE]	N/A

#### 2.3.4 Application life cycle

The application is a Java Card applet instantiated in phase 6. The lifecycle follows the standard defined in [COSMO-ST] §3.5 which is depicted by the following figure:

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>17/66</b>
-----------------------	-----------------	--------------------------	--------------

- Phase 6**
- Phase 7**

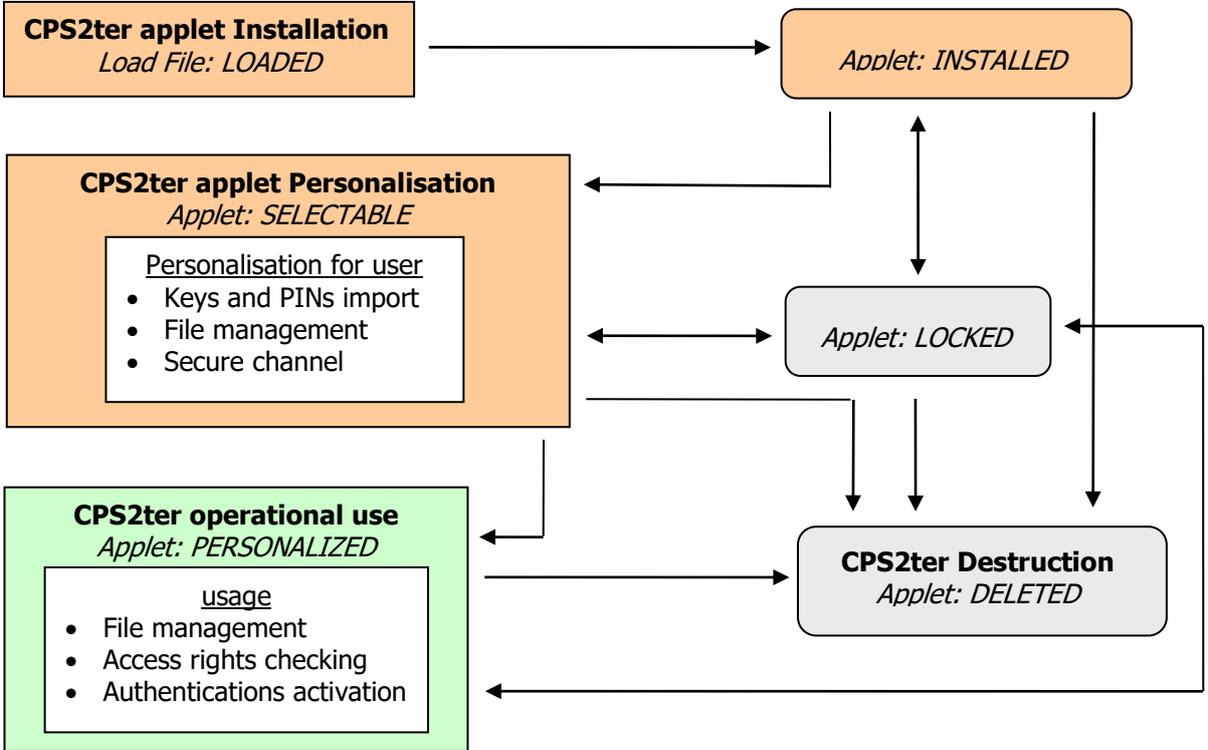


Figure 4 CPS2ter applet lifecycle

All rights of IDEMIA are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

### 3 Conformance claims

#### 3.1 Common Criteria conformance

This Security Target (ST) is CC Part 2 extended [CC-2], CC Part 3 conformant [CC-3] and written according to the Common Criteria version 3.1, revision 5, Part 1 [CC-1].

#### 3.2 Package conformance

This ST is conformant to the EAL4 package as defined in [CC-3].

The EAL4 have been augmented with the following requirement to fulfil the smartcard standard:

Requirement	Name	Type
ALC_DVS.2	Sufficiency of security measures	Higher hierarchical component
AVA_VAN.5	Advanced methodical vulnerability analysis	Higher hierarchical component

#### 3.3 Protection Profile conformance

No protection profile is claimed.

## 4 Security problem definition

### 4.1 Assets

#### PINs

Reference PINs used by the TOE to control access to sensitive data.

*Protection:* integrity and confidentiality.

*Application note:*

In the following PINs are also refer as CHVs.

#### Keys

3DES keys used to compute both MAC required in PRO mode and cryptogram in external authentication.

*Protection:* integrity and confidentiality.

#### Files data

File structures used to store sensitive user data.

*Protection:* integrity.

*Application note:*

PINs and keys are not included in this asset.

#### TryCounters

The PIN try counters manage the number of PIN wrong enters. When it reaches the defined maximum number (PIN Try Counter limit) of wrong enters, the PIN verification mechanism is blocked.

*Protection:* integrity.

#### ACs

Access conditions associated to a file specifying which security mechanisms have to be performed in order to grant access. There are 4 types of mechanisms available:

- o External authentication (see SF External Authentication),
- o Pro mode (see SF Pro mode),
- o CHV1 (see SF cardholder authentication),
- o CHV2 (see SF cardholder authentication).

All combinations can be used.

*Protection:* integrity.

#### TOE

The target of Evaluation is a smart card allowing to store sensitive data and access distant services. It provides security mechanisms to prevent illegal usage and access.

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>20/66</b>
-----------------------	-----------------	--------------------------	--------------

## 4.2 Users / Subjects

### S.User

S.User is the cardholder who wants to access to distant services. He authorizes access of its data to a distant server by providing the PIN associated to the file where those data are stored.

### S.DistantServer

S.DistantServer is an electronic device providing services based on data stored in the card of S.User. For accessing those data it can be required to perform:

- o an external authentication of the S.DistantServer,
- o communicating using protected commands,
- o a S.User authentication for getting user autorisation.

### S.Personnalisier

S.Personnalisier is in charge of writing initial user data, PINs and Keys during personnalisation phase. He uses a secure channel in order to communication with the card.

### S.APDU

S.APDU acts on behalf of the cardholder or the distant server by processing the APDUs they send.

## 4.3 Threats

### T.Keys\_Disclosure

Unauthorised knowledge of the secret keys.

*Assets threatened:* Keys.

*Application note:*

An attacker discloses the value of a key stored in the TOE in order, for instance, to illegitimately perform External authentication or commands in Pro mode and therefore executing unauthorised operations on file.

### T.Keys\_Corruption

Unauthorised modification of stored keys: an attacker modifies the value of a secret key and associated attributes stored in the TOE in order to input a known key.

*Assets threatened:* Keys.

### T.Files\_Corruption

Unauthorised modification of files data: an attacker modifies the content of a user file in the TOE in order to modify to write fake data in the card.

*Assets threatened:* Files data.

FQR : 110 9044	Issue: 6	Date : 07/04/2023	21/66
----------------	----------	-------------------	-------

*Application note:*

This can be, for instance, modifying the name and role of the cardholder which would be stored in the TOE. Therefore, distant server will retrieve afterward incorrect data from the TOE and would be able to decide to allow cardholder to access services which should not be available to him.

**T.ACs\_Corruption**

Unauthorised modification of Access conditions: an attacker modifies the AC of a file present in the TOE in order to set values that would allow him to access to the file.

*Assets threatened:* AC.

**T.PTC\_Corruption**

Unauthorised modification of stored PIN try counters: an attacker modifies the value of a PIN try counter stored in the TOE in order to change the limitation of the number of failing PIN required and finally to retrieve the associated PIN.

*Assets threatened:* TryCounters, PINs.

**T.CHV\_Disclosure**

Unauthorised knowledge of a PIN.

*Assets threatened:* PINs.

*Application note:*

An attacker discloses the value of a PIN stored in the TOE in order, for instance, to illegitimately authenticate himself subsequently as the cardholder in order to perform a file operation requiring a CHV authentication.

**T.CHV\_Corruption**

Unauthorised modification of PINs: an attacker modifies the value of a PIN stored in the TOE in order to input a known PIN.

*Assets threatened:* PINs.

**T.Replay**

Replay of commands.

Data are accessed without required authentications by replaying a correct sequence of operations leading to the intended operation.

*Assets threatened:* PINs, Keys, Files data, AC.

**T.User\_Usurpation**

An attacker is unduly granted the rights of the user to perform unauthorised operations on his/her behalf.

*Assets threatened:* Files data, Keys, AC, PINs.

*Application note:*

Operations that can be performed on behalf of the user are those that are specified to be protected by a CHV1 or CHV2 authentication in the AC of the file.

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>22/66</b>
-----------------------	-----------------	--------------------------	--------------

### T.DistantServer\_Usurpation

An attacker is unduly granted the rights of the distant server to perform unauthorised operations on his/her behalf.

*Assets threatened:* Files data, Keys, AC, PINs.

### T.TOE\_Usurpation

An attacker unduly authenticates itself to a third party as a genuine TOE in order to access restricted services.

*Assets threatened:* TOE.

### T.Tearing

The attacker may force the TOE into a non stable state by stopping or disrupting the execution of the commands.

*Assets threatened:* Files data, Keys, AC, TryCounters, PINs.

*Application note:*

An attack path is tearing the TOE out of the reader while a command is processed, breaking the execution flow and possibly switching the assets to uncorrect values.

## 4.4 Organisational Security Policies

### P.Crypto

Cryptographic (mathematical) functions used must be trusted to ensure integrity and confidentiality. Therefore, those cryptographic functions are expected to resist practical attacks. A practical attack is an attack that may occur during card lifespan or embedded key lifetime, and that can be led by an organisation with high expertise and computational resources. To that end:

- o Secure parameters: cryptographic functions shall use security parameters (key lengths, usage conditions...) strong enough to resist practical attacks,
- o Secure implementation: the implementation of cryptographic functions inside the TOE, including key storage, shall resist practical attacks.

### P.CHV\_management

CHV tranfers to the TOE are supposed be performed in an appropriate secure environment in usage phase.

This environment should be local and able to enforce integrity and confidentiality between the CHV device and the TOE.

*Application note:*

The CHV device is usually a PIN pad and its associated terminal but can also be a standard PC.

## 4.5 Assumptions

### A.Usage

The developper should communicate to the user the rules dealing with the use of the TOE. Especially it must inform the user that:

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>23/66</b>
-----------------------	-----------------	--------------------------	--------------

- o he must keep its TOE the same way he does for a highly valuable assets,
- o he must not divulgate his PINs to anyone.

The user should enforce these rules.

### **A.Perso**

The personaliser is a trusted entity enforcing rules and recommandations specified in the personalisation guide.

## 5 Security Objectives

### 5.1 Security Objectives for the TOE

#### O.CHV

The TSF shall ensure authentication of the user to the TOE for operations which require it.

#### O.Authentication

The TSF shall ensure authentication of the distant server before processing operations which require such an authentication.

#### O.TOE\_Usurpation

The TSF shall authenticate itself to be able to prove its own genuinity.

#### O.Export

Confidential data must not be exported.

#### O.Import

The TSF shall ensure that commands coming from the distant server are genuine.

#### O.Confidentiality\_Protection

The TSF shall provide the means to avoid unauthorised disclosure of data that must be protected in confidentiality: PINs and keys.

#### O.Integrity\_Protection

The TSF shall provide the means to avoid unauthorised modification of data that must be protected in integrity: PINs, keys, File data, TryCounters and AC.

#### O.replay\_Protection

The TSF shall ensure that replayed commands are detected and rejected.

*Application note:*

"replayed commands" referred to commands previously transmitted to the TOE and re-sended without any modification. This could allow to access sensitive data without any authorisation nor any knowledge of secrets contains in the TOE.

#### O.Access\_Control

The TOE security functionalities shall ensure that sensitive assets are only accessed by authorised users.

#### O.Crypto

Cryptographic functions of the TOE shall resist practical attacks led by organisations with high expertise and high computational resources.

FQR : 110 9044	Issue: 6	Date : 07/04/2023	25/66
----------------	----------	-------------------	-------

**O.Tamper**

The TSF shall prevent physical tampering of its security critical parts.

**O.Operate**

The TSF shall ensure the continued correct operation of its security functionalities especially in case of abnormal process of commands such as interruption during processing.

**5.2 Security objectives for the Operational Environment****OE.Usage**

It must be enforced that the developer must communicate to the user the rules dealing with the use of the TOE.

Especially it must inform the user that:

- o he must keep its TOE the same way he does for a highly valuable assets,
- o he must not divulgate his PINs to anyone.

The user shall enforce these rules.

**OE.Perso**

The personaliser must be a trusted entity enforcing rules and recommendations specified in the personalisation guide.

**OE.CHV\_Management**

CHV transfers to the TOE must be performed in an appropriate secure environment in usage phase.

This environment should be local and must enforce integrity and confidentiality between the CHV device and the TOE.

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>26/66</b>
-----------------------	-----------------	--------------------------	--------------

## 6 Extended requirements

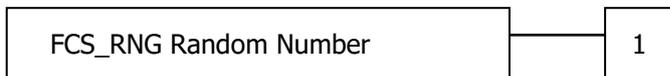
### 6.1 Extended family FCS\_RNG - Random Number Generation

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

**Family behavior:**

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

**Component leveling:**



FCS\_RNG.1 Random Number Generation has two constituents:

- FCS\_RNG.1.1 Random number generator type
- FCS\_RNG.1.2 Random number quality

**Management:**

There are no management activities foreseen

**Audit:**

There are no actions defined to be auditable

**FCS\_RNG.1 Random Number Generation**

Hierarchical to: No other components.  
 Dependencies: No dependencies. Definition

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

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

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>27/66</b>
-----------------------	-----------------	--------------------------	--------------

## 7 Security Functional Requirements

### 7.1 Security Functional Requirements

#### 7.1.1 Attributes

##### FIA\_ATD.1/Attributes User attribute definition

**FIA\_ATD.1/Attributes** The TSF shall maintain the following list of security attributes belonging to individual users:

- o **CHVx status which defines if the cardholder is authenticated with the PIN x,**
- o **ExternalAuth\_k which defines if the distant server is authenticated with an external authentication and the key k.**

#### 7.1.2 CHV

There can be several authentications of the cardholder to the TOE. they all use the mechanism of PIN verification referred in the following as Cardholder verification or CHV.

Actually, each DF can be associated to a different CHV but keys can only be associated to CHV1:

- if a key required CHV1 authentication, the cardholder must perform an authentication with CHV1 in order to use the key,
- if a file required a CHVx authentication in its AC for the received command, the cardholder must perform an authentication with CHVx in order to access the file (this opens the CHVx session).

*Remark:*

On the card, only one type of CHV can be used; either CHV1 or CHV2.

##### FIA\_UAU.1/CHV Timing of authentication

**FIA\_UAU.1/CHV** The TSF shall allow

- o **identifying the user by means of FIA\_UID.1/CHV (as CHVx for targeting the CHVx authentication),**
- o **unblocking CHVx,**
- o **any operation on file whose CHVx flag (in AC) is set to false,**
- o **any operation which uses a key whose CHV1 flag is set to false,**
- o **any operation requiring the CHVx authentication if the user is currently authenticated as CHVy**

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

**FIA\_UAU.1.2/CHV** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

*Refinement:*

This requirement considers the CHVx authentication of the cardholder.

CHVx authentication is performed using the adequate CHVx file defined as follow:

*Adequate* (CHVx,current\_DF)=

- o if a CHVx file F exist in current\_DF then return current\_DF
- o else return *Adequate* (CHVx,father\_DF)

*Application note:*

CHVx authentication is a PIN based authentication.

#### FIA\_UID.1/CHV Timing of identification

**FIA\_UID.1.1/CHV** The TSF shall allow

- o **unblocking CHVx,**
- o **any operation on file whose CHVx flag (in AC) is set to false,**
- o **any operation which uses a key whose CHV1 flag is set to false,**
- o **any operation requiring the CHVy authentication if the user is currently authenticated as CHVy**

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

**FIA\_UID.1.2/CHV** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

*Refinement:*

This requirement considers the CHVx identification of the cardholder.

#### FIA\_AFL.1/CHV Authentication failure handling

**FIA\_AFL.1.1/CHV** The TSF shall detect when **an administrator configurable positive integer within range [1,15]** unsuccessful authentication attempts occur related to **CHVx authentication**.

**FIA\_AFL.1.2/CHV** When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **block the PIN associated to the adequate CHVx file**.

*Refinement:*

blocking is a temporary operation that can be cancelled by the associated unblock PIN.

*Application note:*

The "associated unblock PIN" referred to the PUK linked to the specified CHVx. It is definitely blocked after a defined number of fail attempt.

**FIA\_USB.1/CHV User-subject binding**

**FIA\_USB.1.1/CHV** The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **CHVx status**.

**FIA\_USB.1.2/CHV** The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- o **CHVx status is set to true.**

**FIA\_USB.1.3/CHV** The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

- o **CHVx status cannot be modified except by the TOE during the authentication with another CHV,**
- o **CHVx status is reset to false**
  - **if an other file is selected with a different adequate file,**
  - **if the file related to CHVx is deactivated or deleted,**
  - **at each application startup.**

### 7.1.3 External authentication

**FIA\_UAU.1/ExtAuth Timing of authentication**

**FIA\_UAU.1.1/ExtAuth** The TSF shall allow

- o **identifying the distant server by means of FIA\_UID.1/ExtAuth,**
- o **any operation on file whose External Authentication flag (in AC) is set to false,**
- o **any operation requiring the ExternalAuth\_k authentication if the user is currently authenticated using an ExternalAuth\_k**

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

**FIA\_UAU.1.2/ExtAuth** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

*Refinement:*

This requirement considers the external authentication of the distant server.

External authentication is performed using the adequate file defined as follow:

*Adequate* (KeyFileType,current\_DF)=

- o if a KeyfileType F exist in current\_DF then return current\_DF
- o else return *Adequate* (KeyFileType,father\_DF)

with KeyFileType(File) = AppFile if File is transparent else GesFile

*Application note:*

ExternalAuth\_k referred to the external authentication using the key k. The only method to be used is the external authentication with 3DES. The other method by direct compare must not be activated in the key AC field.

The above requirement uses the following terms:

- "transparent file" which refers to an application file storing "files data" sensitive assets,
- "AppFile" which refers to the type of 3DES key files used for transparent files access,
- "GesFile" which refers to the type of 3DES key files used for management files access (i.e. operations on DF and key files).

**FIA\_UID.1/ExtAuth Timing of identification**

**FIA\_UID.1.1/ExtAuth** The TSF shall allow

- o **any operation on file whose External Authentication flag (in AC) is set to false,**

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

**FIA\_UID.1.2/ExtAuth** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

*Refinement:*

This requirement considers the identification of the distant server by means of the external authentication.

**FIA\_AFL.1/ExtAuth Authentication failure handling**

**FIA\_AFL.1.1/ExtAuth** The TSF shall detect when **an administrator configurable positive integer within range [0,15]** unsuccessful authentication attempts occur related to **external authentication or Pro mode verification with a defined key k.**

**FIA\_AFL.1.2/ExtAuth** When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **block the associated key k.**

*Refinement:*

The try counter is the one associated to the key.

*Application note:*

External authentication and Pro mode can use the same application key file. Therefore the try counter of a key can be decreased either by a failed External Authentication or a failed Pro mode verification.

**FIA\_USB.1/ExtAuth User-subject binding**

**FIA\_USB.1.1/ExtAuth** The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **ExternalAuth\_k status**.

**FIA\_USB.1.2/ExtAuth** The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- o **ExternalAuth\_k status is set to true.**

**FIA\_USB.1.3/ExtAuth** The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

- o **ExternalAuth\_k status cannot be modified except by the TOE during the external authentication with another key k',**
- o **ExternalAuth\_k status reset to false**
  - **if an other file is selected with a different adequate file,**
  - **if the file related to ExternalAuth\_k is deleted,**
  - **at each application startup.**

*7.1.4 Internal Authentication***FDP\_DAU.1/InitAuth Basic Data Authentication**

**FDP\_DAU.1.1/InitAuth** The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **the TOE**.

**FDP\_DAU.1.2/InitAuth** The TSF shall provide **any external entities** with the ability to verify evidence of the validity of the indicated information.

*7.1.5 Exchanges***FDP\_ETC.1/Export Export of user data without security attributes**

**FDP\_ETC.1.1/Export** The TSF shall enforce the **AC policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

**FDP\_ETC.1.2/Export** The TSF shall export the user data without the user data's associated security attributes

*Refinement:*

Only those data can be exported outside the TOE:

- o files AC using the SELECT APDU,
- o try counters using the SELECT APDU,
- o random values using ASK RANDOM APDU,

- o data contained in transparent files using READ BINARY APDU.

**FDP\_ITC.1/Import Import of user data without security attributes**

**FDP\_ITC.1.1/Import** The TSF shall enforce the **AC policy** when importing user data, controlled under the SFP, from outside of the TOE.

**FDP\_ITC.1.2/Import** The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

**FDP\_ITC.1.3/Import** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- o **the import of the first Load key file must be performed using the Key Exchange key (Kek) of the Card Manager to dechiper key data.**

**FMT\_SMF.1/Selectable Specification of Management Functions**

**FMT\_SMF.1.1/Selectable** The TSF shall be capable of performing the following management functions:

- o **switch the internal state of the applet from SELECTABLE to PERSONNALIZED and deactivate in the same time the possibility of going back to the SELECTABLE state when Set Data APDU is received.**

*7.1.6 File secure management***FDP\_SDI.2/IntegrityControl Stored data integrity monitoring and action**

**FDP\_SDI.2.1/IntegrityControl** The TSF shall monitor user data stored in containers controlled by the TSF for **corruption** on all objects, based on the following attributes:

- o **file header,**
- o **key secure container parameters,**
- o **PIN secure container parameters.**

**FDP\_SDI.2.2/IntegrityControl** Upon detection of a data integrity error, the TSF shall **kill the card.**

**FDP\_ACC.1/AccessControl Subset access control**

**FDP\_ACC.1.1/AccessControl** The TSF shall enforce the **AC policy** on

- o **Subject: S.APDU,**

- o **Objects:** Ob.File,
- o **Operations:** Op.Read, Op.Dir, Op.Update, Op.ChangeAC, Op.Delete, Op.Write, Op.Create, Op.LoadKeyFile.

*Application note:*

The object Ob.File refer to all files handled by the TOE: Master File (MF), Directory File (DF) and Elementary File (EF). All these files are organized within a File System compliant to [7816-4]. It represents the hierarchy between all the files. See [IAS ECC-ST] for more details. Operations (prefixed with "Op") are described in the following table.

Operation	Description
<b>Op.Read</b>	read data in the current EF.
<b>Op.Dir</b>	list all files and/or directories registered under the current directory (a DF or the MF).
<b>Op.Update</b>	update a part of the whole content of the current selected EF.
<b>Op.ChangeAC</b>	change the AC of the adequate file.
<b>Op.Delete</b>	delete a file (DF or EF) from the current directory (a DF or the MF).
<b>Op.Write</b>	write binary data into the content of the selected EF.
<b>Op.Create</b>	create a new file under the current directory (a DF or the MF).
<b>Op.LoadKeyFile</b>	Initialize or secure update of Key File.

**FDP\_ACF.1/AccessControl Security attribute based access control**

**FDP\_ACF.1.1/AccessControl** The TSF shall enforce the **AC policy** to objects based on the following:

- o **Subjects (attributes):** S.APDU (APDU.CHV1, APDU.CHV2, APDU.ExternalAuth\_k),
- o **Objects (attributes):** Ob.File (File.AC).

*Refinement:*

The attribute AC is divided into 4 sub-attributes defining the access rights for the a category of command.

**FDP\_ACF.1.2/AccessControl** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

<b>Subject</b>	<b>Operation(Object)</b>	<b>Rule*</b>
S.APDU	Op.Read(File)	<i>CheckAC(S.APDU,AC)</i> where AC = File.AC.groupe1
S.APDU	Op.Dir(File)	<i>CheckAC(S.APDU,AC)</i> where AC = File.AC.groupe1
S.APDU	Op.Update(File)	<i>CheckAC(S.APDU,AC)</i> where AC = File.AC.groupe2
S.APDU	Op.ChangeAC(File)	<i>CheckAC(S.APDU,AC)</i> where AC = File.AC.groupe3
S.APDU	Op.Delete(File)	<i>CheckAC(S.APDU,AC)</i> where AC = File.AC.groupe3
S.APDU	Op.Write(File)	<i>CheckAC(S.APDU,AC)</i> where AC = File.AC.groupe3
S.APDU	Op.Create(File)	<i>CheckAC(S.APDU,AC)</i> where AC = File.AC.groupe4
S.APDU	LoadKeyFile(File)	<i>CheckAC(S.APDU,AC)</i> where AC = File.AC.groupe4

\* *CheckAC* must be true to authorize operation.

Here is the definition as a boolean expression of *CheckAC(S.APDU,AC)* governing file access:

*CheckAC(S.APDU,AC): boolean =*

- o *AppletState=SELECTABLE* -> true, or
- o *AC.condition = "ALWAYS"* -> true, and
- o *AC.condition = "CHV1 or CHV1/AUTH or CHV1/PRO"* -> S.APDU.CHV1, and
- o *AC.condition = "CHV2 or CHV2/AUTH or CHV2/PRO"* -> S.APDU.CHV2, and
- o *AC.condition = "AUTH or CHV1/AUTH or CHV2/AUTH"* -> S.APDU.ExternalAuth\_k where k = AC.keyIndex, and
- o *AC.condition = "PRO or CHV1/PRO or CHV2/PRO"* -> S.APDU provides a correct certificate with k = AC.keyIndex, and
- o *AC.condition = "NEVER"* -> false

**FDP\_ACF.1.3/AccessControl** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

**FDP\_ACF.1.4/AccessControl** The TSF shall explicitly deny access of subjects to objects based on the

- o **Op.Read(Ob.File)** is forbidden if Ob.File is a key file or CHV file,
- o **Op.Update(Ob.File)** is forbidden if Ob.File is a key file,
- o **Op.Write(Ob.File)** is forbidden if Ob.File is a key file or CHV file,
- o **Op.ChangeAC(Ob.File,AC\_new)** is forbidden if AC\_new < File.AC.

See below the lattice corresponding to the set of ACs and the order relation "<":

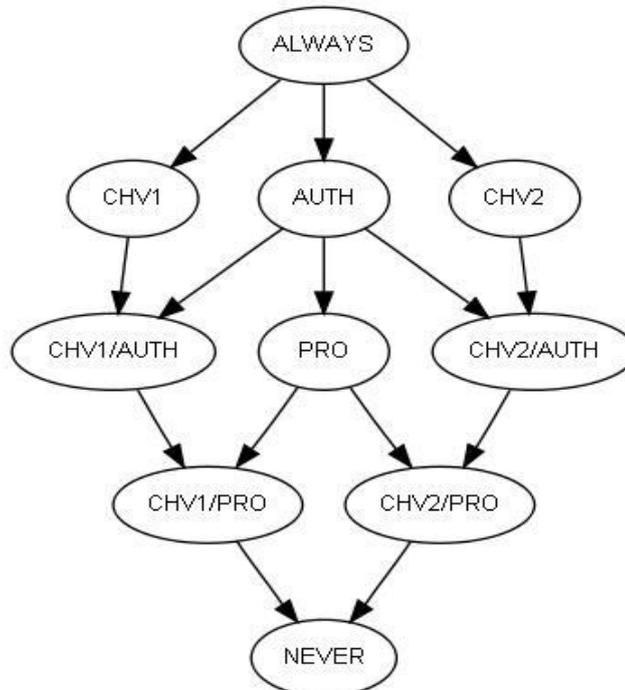


Figure 5 ACs lattice

*Application note:*

The subject S.APDU acts on behalf of the cardholder or the distant server by processing the APDUs they send. These are processed in a state defined by the previous CHV and External authentications performed and referred as the attributes APDU.CHVx and APDU.External\_Auth\_k.

FDP\_ACF.1.4 got the highest priority; requirements elements 3, 2 and 1 are applied in this order. Consequently, for instance, ACs cannot be changed to a lower security level even if current ACs are enforced.

Keys used are always contained in the Adequate file as specified in FIA\_UAU.1/ExtAuth.

A group is defined as the ACs of a set of operations (activated by related APDUs):

- groups 1 is composed of Op.Read and Op.Dir,
- groups 2 is composed of Op.Update,
- groups 3 is composed of Op.ChangeAC, Op.Delete and Op.Write,
- groups 4 is composed of Op.Create and Op.LoadKeyFile.

Details are provided in [SRS] §2.4, §3.1 and §4.3.4.

*7.1.7 Transactions protection***FDP\_UIT.1/Exchanges Data exchange integrity**

**FDP\_UIT.1.1/Exchanges** The TSF shall enforce the **AC policy** to be able to **receive** user data in a manner protected from **replay, modification, deletion and insertion** errors.

**FDP\_UIT.1.2/Exchanges** The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.

*Refinement:*

Replay and integrity protection is only enforced for:

- o external authentication,
- o all APDUs using Pro mode,
- o all APDUs sent in SELECTABLE state and embedding a sensitive asset.

*Application note:*

Key used is the one contained in the adequate file (see FIA\_UAU.1/ExtAuth).

**FDP\_UCT.1/LoadKey Basic data exchange confidentiality**

**FDP\_UCT.1.1/LoadKey** The TSF shall enforce the **AC policy** to **receive** user data in a manner protected from unauthorised disclosure.

*Refinement:*

Confidentiality is only to ensure for key loading.

*Application note:*

Key used is the one contained in the adequate file (see FIA\_UAU.1/ExtAuth).

**FTP\_ITC.1/Selectable Inter-TSF trusted channel**

**FTP\_ITC.1.1/Selectable** 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/Selectable** The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/Selectable** The TSF shall initiate communication via the trusted channel for **performing all operations specified in FDP\_ACF.1/AccessControl**.

*Application note:*

This secure channel is mandatory in SELECTABLE state for commands which support it.

### 7.1.8 Cryptography

**FCS\_COP.1/TDES Cryptographic operation**

**FCS\_COP.1.1/TDES** The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm

- o **3DES in CBC mode for Pro mode and data cipher,**
- and cryptographic key sizes **128 bits (only 112 bits are used)** that meet the following:
- o **[FIPS 46-3],**
  - o **[FIPS 81].**

*Application note:*

ANSI X3.92 is the international standard specifying 3DES. FIPS 46-3 is the equivalent standard issued by the USA.

ISO 10116 is the international standard specifying CBC mode of 3DES. FIPS 81 is the equivalent standard issued by the USA.

**FCS\_RNG.1/Random Random number generation**

**FCS\_RNG.1.1/Random** The TSF shall provide a **hybrid** random number generator that implements: **none**.

**FCS\_RNG.1.2/Random** The TSF shall provide random numbers that meet **[NIST SP 800-90]**.

**FCS\_CKM.4/Destruction Cryptographic key destruction**

**FCS\_CKM.4.1/Destruction** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **which ensures that any access to a cleared key throw an exception as specified by the method clearKey() of the underlying platform** that meets the following: **[JCAPI]**.

*7.1.9 TOE protection***FPT\_PHP.3 Resistance to physical attack**

**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.

*Application note:*

This requirement is connected to the FPT\_PHP.3 requirements of the platform. It detects physical attacks and reacts to these attacks by resetting the card or raising an exception. In these two cases, IC notifies the attack to the software.

**FPT\_FLS.1 Failure with preservation of secure state**

**FPT\_FLS.1.1** The TSF shall preserve a secure state when the following types of failures occur:

- o **tearing**.

**7.2 Security Assurance Requirements**

The security assurance requirement level is EAL4 augmented with AVA\_VAN.5 and ALC\_DVS.2. All these SARs are defined in [CC-3].

## 8 TOE Summary Specification

### 8.1 TOE Summary Specification

#### Cardholder authentication

This security feature allows the cardholder (or user) to authenticate himself to the card using a PIN based method.

For each file, Access Conditions can requires a user PIN authentication either with the CHV1 (first PIN) or CHV2 (second PIN). Depending on the directory in which this file is located those to CHV can differ. To grant access to the considered file, the TOE will check that CHV authenticationr required has been performed.

Each CHV is associated to a PUK which allows to unlock it when the maximum tries authorized has been met.

#### Pro mode

This security feature integrates a cryptogram to each incoming commands to check their authenticity. The following steps summarize it:

- o sending of a random value to the distant server,
- o Computing of a MAC in CBC mode with a key k on this random value and data bytes of the command,
- o checking of this MAC by the TOE with the key required by the file (see below),
- o Pro mode condition succeed.

For each file, Access Conditions can requires such a feature to grant access to the considered file. Depending on the directory in which this file is located and the key index specified in ACs, the key used to compute cryptogram will differ.

#### External Authentication

This security feature implements a protocol to ensure authentication of the distant server. The following steps summarize it:

- o sending of a random value to the distant server,
- o Computing of a MAC in CBC mode with a key k on this random value,
- o checking of this MAC by the TOE with the key required by the file (see below),
- o External Authentication succeed: all files requiring an External Authentication with this key k can be accessed.

For each file, Access Conditions can requires such a feature to grant access to the considered file. Depending on the directory in which this file is located and the key index specified in ACs, the key used to compute cryptogram will differ.

#### Internal Authentication

This security feature implements a protocol to ensure authentication of the TOE to adistant entity. The following steps summarize it:

- o sending of a random value from the distant server,
- o Computing of a MAC in CBC mode with a key k on this random value,

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>40/66</b>
-----------------------	-----------------	--------------------------	--------------

- o checking of the cryptogram by the distant server in order to validate the genuinity of the TOE.

### Random generation

This security feature allows to generate random based on both chip hardware random and software post-processing. Those randoms are exported by the TOE to the distant server in order to be included in the cryptograms it send. This feature provide protection against replay of previously send commands.

### Access Control

This security feature checks that access conditions specified in the AC of file are always enforced when accessing the file. Here are the main points checked for an incoming command of type T and ensured by the TOE:

- o what are the AC required by this file for T?,
- o If Cardholder verification is required (CHV1 or CHV2), has it been performed?,
- o If External Authentication is required, has it been performed? With the correct key?
- o If Pro Mode is required, is cryptogram presents in the command? With the correct key?
- o If an AC modification in required, does the new one more restrictive than the old one? Those checks are mandatory to grant access to the file.

Access control also checks that confidential data are not exported outside the TOE.

### Secure personnalisation

This secure feature allows to create a secure channel between the TOE and the personnalizer in order to perform operations on the TOE during phase 6 of the lifecycle. This secure channel is provided by card manager of the TOE an ensure authentication of the end-points, integrity, confidentiality and replay protection depending on the level requested during the initialisation of the channel.

In phase 6 (personnalisation) or Selectable state of the CPS2ter applet, this channel is the main feature protecting data transfers.

## 9 Rationales

### 9.1 Security objectives / Security Problem Definition

#### 9.1.1 Threats

**T.Keys\_Disclosure** To counter the threat, the TOE shall:

- o ensure the confidentiality of keys imported and stored (O.Confidentiality\_Protection),
- o control access to keys to the only authorized users (O.Access\_Control),
- o Forbid export of confidential data (O.Export),
- o enforce physical protection to avoid bypassing security mechanisms (O.Tamper).

**T.Keys\_Corruption** To counter the threat, the TOE shall:

- o ensure integrity of keys imported and stored (O.Integrity\_Protection),
- o control access to keys to the only authorized users (O.Access\_Control),
- o verify authenticity of imported data (O.Import),
- o enforce physical protection to avoid bypassing security mechanisms (O.Tamper).

**T.Files\_Corruption** To counter the threat, the TOE shall:

- o ensure integrity of files imported and stored (O.Integrity\_Protection),
- o control access to files to the only authorized users (O.Access\_Control),
- o verify authenticity of imported data (O.Import),
- o enforce physical protection to avoid bypassing security mechanisms (O.Tamper).

**T.ACs\_Corruption** To counter the threat, the TOE shall:

- o ensure integrity of ACs imported and stored (O.Integrity\_Protection),
- o control access to ACs to the only authorized users (O.Access\_Control),
- o verify authenticity of imported data (O.Import),
- o enforce physical protection to avoid bypassing security mechanisms (O.Tamper).

**T.PTC\_Corruption** To counter the threat, the TOE shall:

- o ensure integrity of PTC stored (O.Integrity\_Protection),
- o Forbid access to PTC; no entity but the TSF can manage this asset (O.Access\_Control),
- o enforce physical protection to avoid bypassing security mechanisms (O.Tamper).

**T.CHV\_Disclosure** To counter the threat, the TOE shall:

- o ensure the confidentiality of CHV stored (O.Confidentiality\_Protection),
- o control access to CHV to the only authorized users (O.Access\_Control),
- o Forbid export of confidential data (O.Export),
- o enforce physical protection to avoid bypassing security mechanisms (O.Tamper).

To counter the threat the environment must also:

- o ensure the confidentiality of CHV imported (OE.CHV\_Management).

**T.CHV\_Corruption** To counter the threat, the TOE shall:

- o ensure integrity of CHV stored (O.Integrity\_Protection),
- o control access to CHV to the only authorized users (O.Access\_Control),
- o verify authenticity of imported data (O.Import),
- o enforce physical protection to avoid bypassing security mechanisms (O.Tamper).

To counter the threat the environment must also:

- o ensure the confidentiality of CHV imported (OE.CHV\_Management).

**T.Replay** To counter the threat, the TOE shall:

- o ensure that all replayed commands are detected and rejected (O.replay\_Protection).

**T.User\_Usurpation** To counter the threat, the TOE shall:

- o enforce authentication of the user to the TOE before performing operations requiring it (O.CHV),
- o enforce physical protection to avoid bypassing security mechanisms (O.Tamper).

**T.DistantServer\_Usurpation** To counter the threat, the TOE shall:

- o enforce authentication of the distant server to the TOE before performing operations requiring it (O.Authentication),
- o enforce physical protection to avoid bypassing security mechanisms (O.Tamper).

**T.TOE\_Usurpation** To counter the threat, the TOE shall:

- o enforce authentication of the TOE to any third party in order to prove its own genuinity (O.TOE\_Usurpation),
- o enforce physical protection to avoid bypassing security mechanisms (O.Tamper).

**T.Tearing** To counter the threat, the TOE shall:

- o ensure the continued correct operation of its security functionalities especially in case of abnormal process of commands such as interruption during processing (O.Operate).

9.1.2 Organisational Security Policies

**P.Crypto** This OSP is directly enforced by the objectives O.Crypto.

**P.CHV\_management** This OSP is directly enforced by the objectives for the environment OE.CHV\_Management.

9.1.3 Assumptions

**A.Usage** This assumption is completely upheld by the objectives for the environment OE.Usage.

**A.Perso** This assumption is completely upheld by the objectives for the environment OE.Perso.

9.1.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
<a href="#">T.Keys Disclosure</a>	<a href="#">O.Access Control</a> , <a href="#">O.Confidentiality Protection</a> , <a href="#">O.Export</a> , <a href="#">O.Tamper</a>	<a href="#">Section 9.1.1</a>
<a href="#">T.Keys Corruption</a>	<a href="#">O.Access Control</a> , <a href="#">O.Integrity Protection</a> , <a href="#">O.Import</a> , <a href="#">O.Tamper</a>	<a href="#">Section 9.1.1</a>
<a href="#">T.Files Corruption</a>	<a href="#">O.Access Control</a> , <a href="#">O.Integrity Protection</a> , <a href="#">O.Import</a> , <a href="#">O.Tamper</a>	<a href="#">Section 9.1.1</a>
<a href="#">T.ACs Corruption</a>	<a href="#">O.Access Control</a> , <a href="#">O.Integrity Protection</a> , <a href="#">O.Import</a> , <a href="#">O.Tamper</a>	<a href="#">Section 9.1.1</a>
<a href="#">T.PTC Corruption</a>	<a href="#">O.Integrity Protection</a> , <a href="#">O.Tamper</a> , <a href="#">O.Access Control</a>	<a href="#">Section 9.1.1</a>
<a href="#">T.CHV Disclosure</a>	<a href="#">O.Access Control</a> , <a href="#">O.Confidentiality Protection</a> , <a href="#">O.Export</a> , <a href="#">O.Tamper</a> , <a href="#">OE.CHV Management</a>	<a href="#">Section 9.1.1</a>
<a href="#">T.CHV Corruption</a>	<a href="#">O.Access Control</a> , <a href="#">O.Integrity Protection</a> , <a href="#">O.Tamper</a> , <a href="#">O.Import</a> , <a href="#">OE.CHV Management</a>	<a href="#">Section 9.1.1</a>
<a href="#">T.Replay</a>	<a href="#">O.replay Protection</a>	<a href="#">Section 9.1.1</a>
<a href="#">T.User Usurpation</a>	<a href="#">O.CHV</a> , <a href="#">O.Tamper</a>	<a href="#">Section 9.1.1</a>
<a href="#">T.DistantServer Usurpation</a>	<a href="#">O.Authentication</a> , <a href="#">O.Tamper</a>	<a href="#">Section 9.1.1</a>
<a href="#">T.TOE Usurpation</a>	<a href="#">O.TOE Usurpation</a> , <a href="#">O.Tamper</a>	<a href="#">Section 6.1.1</a>
<a href="#">T.Tearing</a>	<a href="#">O.Operate</a>	<a href="#">Section 9.1.1</a>

**Tableau 1 Threats and Security Objectives - Coverage**

Security Objectives	Threats
<a href="#">O.CHV</a>	<a href="#">T.User Usurpation</a>
<a href="#">O.Authentication</a>	<a href="#">T.DistantServer Usurpation</a>
<a href="#">O.TOE Usurpation</a>	<a href="#">T.TOE Usurpation</a>
<a href="#">O.Export</a>	<a href="#">T.Keys Disclosure</a> , <a href="#">T.CHV Disclosure</a>
<a href="#">O.Import</a>	<a href="#">T.Keys Corruption</a> , <a href="#">T.Files Corruption</a> , <a href="#">T.ACs Corruption</a> , <a href="#">T.CHV Corruption</a>
<a href="#">O.Confidentiality Protection</a>	<a href="#">T.Keys Disclosure</a> , <a href="#">T.CHV Disclosure</a>
<a href="#">O.Integrity Protection</a>	<a href="#">T.Keys Corruption</a> , <a href="#">T.Files Corruption</a> , <a href="#">T.ACs Corruption</a> , <a href="#">T.PTC Corruption</a> , <a href="#">T.CHV Corruption</a>
<a href="#">O.replay Protection</a>	<a href="#">T.Replay</a>
<a href="#">O.Access Control</a>	<a href="#">T.Keys Disclosure</a> , <a href="#">T.Keys Corruption</a> , <a href="#">T.Files Corruption</a> , <a href="#">T.ACs Corruption</a> , <a href="#">T.PTC Corruption</a> , <a href="#">T.CHV Disclosure</a> , <a href="#">T.CHV Corruption</a>
<a href="#">O.Crypto</a>	
<a href="#">O.Tamper</a>	<a href="#">T.Keys Disclosure</a> , <a href="#">T.Keys Corruption</a> , <a href="#">T.Files Corruption</a> , <a href="#">T.ACs Corruption</a> , <a href="#">T.PTC Corruption</a> , <a href="#">T.CHV Disclosure</a> , <a href="#">T.CHV Corruption</a> , <a href="#">T.User Usurpation</a> , <a href="#">T.DistantServer Usurpation</a> , <a href="#">T.TOE Usurpation</a>
<a href="#">O.Operate</a>	<a href="#">T.Tearing</a>
<a href="#">OE.Usage</a>	
<a href="#">OE.Perso</a>	
<a href="#">OE.CHV Management</a>	<a href="#">T.CHV Disclosure</a> , <a href="#">T.CHV Corruption</a>

**Tableau 2 Security Objectives and Threats - Coverage**

Organisational Security Policies	Security Objectives	Rationale
<a href="#">P.Crypto</a>	<a href="#">O.Crypto</a>	<a href="#">Section 9.1.2</a>
<a href="#">P.CHV management</a>	<a href="#">OE.CHV Management</a>	<a href="#">Section 9.1.2</a>

**Tableau 3 OSPs and Security Objectives - Coverage**

Security Objectives	Organisational Security Policies
<a href="#">O.CHV</a>	
<a href="#">O.Authentication</a>	
<a href="#">O.TOE Usurpation</a>	
<a href="#">O.Export</a>	
<a href="#">O.Import</a>	
<a href="#">O.Confidentiality Protection</a>	
<a href="#">O.Integrity Protection</a>	
<a href="#">O.replay Protection</a>	
<a href="#">O.Access Control</a>	
<a href="#">O.Crypto</a>	<a href="#">P.Crypto</a>
<a href="#">O.Tamper</a>	
<a href="#">O.Operate</a>	
<a href="#">OE.Usage</a>	
<a href="#">OE.Perso</a>	
<a href="#">OE.CHV Management</a>	<a href="#">P.CHV management</a>

**Tableau 4 Security Objectives and OSPs - Coverage**

Assumptions	Security objectives for the Operational Environment	Rationale
<a href="#">A.Usage</a>	<a href="#">OE.Usage</a>	<a href="#">Section 9.1.3</a>
<a href="#">A.Perso</a>	<a href="#">OE.Perso</a>	<a href="#">Section 9.1.3</a>

**Tableau 5 Assumptions and Security Objectives for the Operational Environment - Coverage**

Security objectives for the Operational Environment	Assumptions
<a href="#">OE.Usage</a>	<a href="#">A.Usage</a>
<a href="#">OE.Perso</a>	<a href="#">A.Perso</a>
<a href="#">OE.CHV Management</a>	

**Tableau 6 Security Objectives for the Operational Environment and Assumptions - Coverage**

## 9.2 Security requirements / security objectives

### 9.2.1 Objectives

#### 9.2.1.1 Security Objectives for the TOE

**O.CHV** This objective is covered by:

- o FIA\_UID.1/CHV and FIA\_UAU.1/CHV which requires identification and PIN authentication of the user,
- o FIA\_AFL.1/CHV which controls the number of fail attempt and therefore prevent against illicit authentications,
- o FIA\_USB.1/CHV which specifies rules concerning set and reset of CHV authentication status,
- o FIA\_ATD.1/Attributes which defines the CHV authentication status used in the access control,
- o FDP\_ACF.1/AccessControl which requires CHV authentication when ACs of the accessed file require it.

**O.Authentication** This objective is covered by:

- o FIA\_UID.1/ExtAuth and FIA\_UAU.1/ExtAuth which requires identification and authentication of the distant server,
- o FIA\_AFL.1/ExtAuth which control the number of fail attempt and therefore prevent against illicit authentications,
- o FIA\_USB.1/ExtAuth which specifies rules concerning set and reset of external authentication status,
- o FIA\_ATD.1/Attributes which defines the external authentication status used in the access control,
- o FDP\_ACF.1/AccessControl which requires external authentication when ACs of the accessed file require it,
- o FCS\_COP.1/TDES which ensure cryptographic computations are performed using 3DES approved standard,
- o FCS\_RNG.1/Random which ensures the same cryptogram will not be used twice.

**O.TOE\_Usurpation** This objective is covered by:

- o FDP\_DAU.1/InitAuth which ensures the computation of a proof of authenticity of the TOE and provides third parties means to verify it,
- o FCS\_COP.1/TDES which ensure cryptographic computations are performed using 3DES approved standard.

**O.Export** This objective is covered by:

- o FDP\_ACF.1/AccessControl which forbids reading confidential data,
- o FDP\_ETC.1/Export which restricts export to not confidential data.

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>47/66</b>
-----------------------	-----------------	--------------------------	--------------

**O.Import** This objective is covered by:

- o FDP\_ITC.1/Import and FDP\_ACF.1/AccessControl which ensures access control to ensure genuinity of commands are applied when importing them,
- o FDP\_UIT.1/Exchanges which ensures first that exchanges are always protected in integrity and second that entity sending the commands know the secret keys which is a proof of genuinity,
- o FTP\_ITC.1/Selectable which provides a secure channel enforcing authentication of end points,
- o FCS\_COP.1/TDES which ensure cryptographic computations are performed using 3DES approved standard,
- o FMT\_SMF.1/Selectable which switches application phase to personalised and activates ACs; secure channel is therefore no more useful.

**O.Confidentiality\_Protection** This objective is covered by:

- o FDP\_ACF.1/AccessControl which forbids reading confidential data,
- o FDP\_UCT.1/LoadKey which protects key loading in confidentiality,
- o FTP\_ITC.1/Selectable which provides a secure channel protecting data exchanged in confidentiality,
- o FMT\_SMF.1/Selectable which switches application phase to personalised and activates ACs; secure channel is therefore no more useful,
- o FCS\_COP.1/TDES which ensure cryptographic computations are performed using 3DES approved standard,
- o FCS\_CKM.4/Destruction which ensures keys are properly destroyed to ensure confidentiality,
- o FPT\_PHP.3 which ensures protection against physical attacks.

**O.Integrity\_Protection** This objective is covered by:

- o FDP\_ACF.1/AccessControl which specifies entities authorized to perform modification of sensitive data,
- o FDP\_UIT.1/Exchanges which protects External authentication and APDUs using Pro mode in integrity,
- o FTP\_ITC.1/Selectable which provides a secure channel protecting data exchanged in integrity,
- o FMT\_SMF.1/Selectable which switches application phase to personalised and activates ACs; secure channel is therefore no more useful,
- o FCS\_COP.1/TDES which ensure cryptographic computations are performed using 3DES approved standard,
- o FDP\_SDI.2/IntegrityControl which ensures integrity of stored sensitive data,
- o FPT\_PHP.3 which ensure protection against physical tampering.

**O.replay\_Protection** This objective is covered by:

- o FDP\_UIT.1/Exchanges which protects External authentication and APDUs using Pro mode against replay attacks,
- o FTP\_ITC.1/Selectable which provide a secure channel protecting against replay attacks,

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>48/66</b>
-----------------------	-----------------	--------------------------	--------------

- o FMT\_SMF.1/Selectable which switches application phase to personalised and activates ACs; secure channel is therefore no more useful,
- o FCS\_COP.1/TDES which ensure cryptographic computations are performed using 3DES approved standard,
- o FCS\_RNG.1/Random which ensures the same cryptogram can not be used twice.

**O.Access\_Control** This objective is covered by:

- o FDP\_ACC.1/AccessControl and FDP\_ACF.1/AccessControl which specifies the rules to access data stored in files based on authentication performed,
- o FIA\_UAU.1/CHV which authenticates users using a CHV,
- o FIA\_UAU.1/ExtAuth which authenticates users using a cryptogram.

**O.Crypto** This objective is covered by:

- o FCS\_COP.1/TDES which ensure cryptographic computations are performed using 3DES approved standard,
- o FCS\_RNG.1/Random which ensure the generation of random values of high quality without any bias,
- o FPT\_PHP.3 which ensures that physical attacks are not practical on the implementation.

**O.Tamper** This objective is covered by:

- o FPT\_PHP.3 which ensures physical tampering protection and avoid security mechanisms to be bypassed.

**O.Operate** This objective is covered by:

- o FPT\_FLS.1 which ensures protection against tearing that could disturb correct operation of security functionalities.

## 9.2.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
<a href="#">O.CHV</a>	<a href="#">FIA_ATD.1/Attributes</a> , <a href="#">FIA_UAU.1/CHV</a> , <a href="#">FIA_UID.1/CHV</a> , <a href="#">FIA_AFL.1/CHV</a> , <a href="#">FIA_USB.1/CHV</a> , <a href="#">FDP_ACF.1/AccessControl</a>	<a href="#">Section 9.2.1.1</a>
<a href="#">O.Authentication</a>	<a href="#">FIA_ATD.1/Attributes</a> , <a href="#">FIA_UAU.1/ExtAuth</a> , <a href="#">FIA_UID.1/ExtAuth</a> , <a href="#">FIA_AFL.1/ExtAuth</a> , <a href="#">FIA_USB.1/ExtAuth</a> , <a href="#">FDP_ACF.1/AccessControl</a> , <a href="#">FCS_COP.1/TDES</a> , <a href="#">FCS_RNG.1/Random</a>	<a href="#">Section 9.2.1.1</a>
<a href="#">O.TOE Usurpation</a>	<a href="#">FDP_DAU.1/InitAuth</a> , <a href="#">FCS_COP.1/TDES</a>	<a href="#">Section 9.2.1.1</a>
<a href="#">O.Export</a>	<a href="#">FDP_ETC.1/Export</a> , <a href="#">FDP_ACF.1/AccessControl</a>	<a href="#">Section 9.2.1.1</a>
<a href="#">O.Import</a>	<a href="#">FDP_ITC.1/Import</a> , <a href="#">FDP_UIT.1/Exchanges</a> , <a href="#">FTP_ITC.1/Selectable</a> , <a href="#">FDP_ACF.1/AccessControl</a> , <a href="#">FMT_SMF.1/Selectable</a> , <a href="#">FCS_COP.1/TDES</a>	<a href="#">Section 9.2.1.1</a>
<a href="#">O.Confidentiality Protection</a>	<a href="#">FDP_ACF.1/AccessControl</a> , <a href="#">FDP_UCT.1/LoadKey</a> , <a href="#">FCS_CKM.4/Destruction</a> , <a href="#">FTP_ITC.1/Selectable</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FMT_SMF.1/Selectable</a> , <a href="#">FCS_COP.1/TDES</a>	<a href="#">Section 9.2.1.1</a>
<a href="#">O.Integrity Protection</a>	<a href="#">FDP_SDI.2/IntegrityControl</a> , <a href="#">FDP_UIT.1/Exchanges</a> , <a href="#">FTP_ITC.1/Selectable</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FDP_ACF.1/AccessControl</a> , <a href="#">FMT_SMF.1/Selectable</a> , <a href="#">FCS_COP.1/TDES</a>	<a href="#">Section 9.2.1.1</a>
<a href="#">O.replay Protection</a>	<a href="#">FDP_UIT.1/Exchanges</a> , <a href="#">FTP_ITC.1/Selectable</a> , <a href="#">FMT_SMF.1/Selectable</a> , <a href="#">FCS_COP.1/TDES</a> , <a href="#">FCS_RNG.1/Random</a>	<a href="#">Section 9.2.1.1</a>
<a href="#">O.Access Control</a>	<a href="#">FDP_ACC.1/AccessControl</a> , <a href="#">FDP_ACF.1/AccessControl</a> , <a href="#">FIA_UAU.1/CHV</a> , <a href="#">FIA_UAU.1/ExtAuth</a>	<a href="#">Section 6.2.1</a>
<a href="#">O.Crypto</a>	<a href="#">FCS_COP.1/TDES</a> , <a href="#">FCS_RNG.1/Random</a> , <a href="#">FPT_PHP.3</a>	<a href="#">Section 9.2.1.1</a>
<a href="#">O.Tamper</a>	<a href="#">FPT_PHP.3</a>	<a href="#">Section 9.2.1.1</a>
<a href="#">O.Operate</a>	<a href="#">FPT_FLS.1</a>	<a href="#">Section 9.2.1.1</a>

Tableau 7 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
<a href="#">FIA_ATD.1/Attributes</a>	<a href="#">O.CHV</a> , <a href="#">O.Authentication</a>
<a href="#">FIA_UAU.1/CHV</a>	<a href="#">O.CHV</a> , <a href="#">O.Access_Control</a>
<a href="#">FIA_UID.1/CHV</a>	<a href="#">O.CHV</a>
<a href="#">FIA_AFL.1/CHV</a>	<a href="#">O.CHV</a>
<a href="#">FIA_USB.1/CHV</a>	<a href="#">O.CHV</a>
<a href="#">FIA_UAU.1/ExtAuth</a>	<a href="#">O.Authentication</a> , <a href="#">O.Access_Control</a>
<a href="#">FIA_UID.1/ExtAuth</a>	<a href="#">O.Authentication</a>
<a href="#">FIA_AFL.1/ExtAuth</a>	<a href="#">O.Authentication</a>
<a href="#">FIA_USB.1/ExtAuth</a>	<a href="#">O.Authentication</a>
<a href="#">FDP_DAU.1/InitAuth</a>	<a href="#">O.TOE_Usurpation</a>
<a href="#">FDP_ETC.1/Export</a>	<a href="#">O.Export</a>
<a href="#">FDP_ITC.1/Import</a>	<a href="#">O.Import</a>
<a href="#">FMT_SMF.1/Selectable</a>	<a href="#">O.Import</a> , <a href="#">O.Confidentiality_Protection</a> , <a href="#">O.Integrity_Protection</a> , <a href="#">O.replay_Protection</a>
<a href="#">FDP_SDI.2/IntegrityControl</a>	<a href="#">O.Integrity_Protection</a>
<a href="#">FDP_ACC.1/AccessControl</a>	<a href="#">O.Access_Control</a>
<a href="#">FDP_ACF.1/AccessControl</a>	<a href="#">O.CHV</a> , <a href="#">O.Authentication</a> , <a href="#">O.Export</a> , <a href="#">O.Import</a> , <a href="#">O.Confidentiality_Protection</a> , <a href="#">O.Integrity_Protection</a> , <a href="#">O.Access_Control</a>
<a href="#">FDP_UIT.1/Exchanges</a>	<a href="#">O.Import</a> , <a href="#">O.Integrity_Protection</a> , <a href="#">O.replay_Protection</a>
<a href="#">FDP_UCT.1/LoadKey</a>	<a href="#">O.Confidentiality_Protection</a>
<a href="#">FTP_ITC.1/Selectable</a>	<a href="#">O.Import</a> , <a href="#">O.Confidentiality_Protection</a> , <a href="#">O.Integrity_Protection</a> , <a href="#">O.replay_Protection</a>
<a href="#">FCS_COP.1/TDES</a>	<a href="#">O.Authentication</a> , <a href="#">O.TOE_Usurpation</a> , <a href="#">O.Import</a> , <a href="#">O.Confidentiality_Protection</a> , <a href="#">O.Integrity_Protection</a> , <a href="#">O.replay_Protection</a> , <a href="#">O.Crypto</a>
<a href="#">FCS_RNG.1/Random</a>	<a href="#">O.Authentication</a> , <a href="#">O.replay_Protection</a> , <a href="#">O.Crypto</a>
<a href="#">FCS_CKM.4/Destruction</a>	<a href="#">O.Confidentiality_Protection</a>
<a href="#">FPT_PHP.3</a>	<a href="#">O.Confidentiality_Protection</a> , <a href="#">O.Integrity_Protection</a> , <a href="#">O.Crypto</a> , <a href="#">O.Tamper</a>
<a href="#">FPT_FLS.1</a>	<a href="#">O.Operate</a>

**Tableau 8 SFRs and Security Objectives**

### 9.3 Dependencies

#### 9.3.1 SFRs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
<a href="#">FIA_ATD.1/Attributes</a>	No dependencies	
<a href="#">FIA_UAU.1/CHV</a>	(FIA_UID.1)	<a href="#">FIA_UID.1/CHV</a>
<a href="#">FIA_UID.1/CHV</a>	No dependencies	
<a href="#">FIA_AFL.1/CHV</a>	(FIA_UAU.1)	<a href="#">FIA_UAU.1/CHV</a>
<a href="#">FIA_USB.1/CHV</a>	(FIA_ATD.1)	<a href="#">FIA_ATD.1/Attributes</a>
<a href="#">FIA_UAU.1/ExtAuth</a>	(FIA_UID.1)	<a href="#">FIA_UID.1/ExtAuth</a>
<a href="#">FIA_UID.1/ExtAuth</a>	No dependencies	
<a href="#">FIA_AFL.1/ExtAuth</a>	(FIA_UAU.1)	<a href="#">FIA_UAU.1/ExtAuth</a>
<a href="#">FIA_USB.1/ExtAuth</a>	(FIA_ATD.1)	<a href="#">FIA_ATD.1/Attributes</a>
<a href="#">FDP_DAU.1/InitAuth</a>	No dependencies	
<a href="#">FDP_ETC.1/Export</a>	(FDP_ACC.1 or FDP_IFC.1)	<a href="#">FDP_ACC.1/AccessControl</a>
<a href="#">FDP_ITC.1/Import</a>	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	<a href="#">FDP_ACC.1/AccessControl</a>
<a href="#">FMT_SMF.1/Selectable</a>	No dependencies	
<a href="#">FDP_SDI.2/IntegrityControl</a>	No dependencies	
<a href="#">FDP_ACC.1/AccessControl</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/AccessControl</a>
<a href="#">FDP_ACF.1/AccessControl</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FDP_ACC.1/AccessControl</a>
<a href="#">FDP_UIT.1/Exchanges</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP_ACC.1/AccessControl</a>
<a href="#">FDP_UCT.1/LoadKey</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP_ACC.1/AccessControl</a>
<a href="#">FTP_ITC.1/Selectable</a>	No dependencies	
<a href="#">FCS_COP.1/TDES</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FDP_ITC.1/Import</a> , <a href="#">FCS_CKM.4/Destruction</a>
<a href="#">FCS_RNG.1/Random</a>	No dependencies	
<a href="#">FCS_CKM.4/Destruction</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	<a href="#">FDP_ITC.1/Import</a>
<a href="#">FPT_PHP.3</a>	No dependencies	
<a href="#">FPT_FLS.1</a>	No dependencies	

Tableau 9 SFRs dependencies

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>52/66</b>
-----------------------	-----------------	--------------------------	--------------

### 9.3.1.1 Rationale for the exclusion of dependencies

**The dependency FMT\_MSA.3 of FDP\_ITC.1/Import is unsupported.** Initial values of attributes and conditions to perform modifications are still specified in FIA\_USB.1 requirements. Therefore, this dependency is irrelevant.

**The dependency FMT\_MSA.3 of FDP\_ACF.1/AccessControl is unsupported.** Initial values of attributes and conditions to perform modifications are still specified in FIA\_USB.1 requirements. Therefore, this dependency is irrelevant.

**The dependency FTP\_ITC.1 or FTP\_TRP.1 of FDP UIT.1/Exchanges is unsupported.** In Selectable state this dependency is enforced by FTP\_ITC.1/Selectable. In Personalised state data are protected directly by cipherment and adding cryptogram without using a Secure Channel In this case the dependency is therefore not useful.

**The dependency FTP\_ITC.1 or FTP\_TRP.1 of FDP\_UCT.1/LoadKey is unsupported.** In Selectable state this dependency is enforced by FTP\_ITC.1/Selectable. In Personalised state data are protected directly by cipherment and adding cryptogram without using a Secure Channel In this case the dependency is therefore not useful.

### 9.3.2 SARs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
<a href="#">ADV ARC.1</a>	(ADV_FSP.1) and (ADV_TDS.1)	<a href="#">ADV FSP.4</a> , <a href="#">ADV TDS.3</a>
<a href="#">ADV FSP.4</a>	(ADV_TDS.1)	<a href="#">ADV TDS.3</a>
<a href="#">ADV IMP.1</a>	(ADV_TDS.3) and (ALC_TAT.1)	<a href="#">ADV TDS.3</a> , <a href="#">ALC TAT.1</a>
<a href="#">ADV TDS.3</a>	(ADV_FSP.4)	<a href="#">ADV FSP.4</a>
<a href="#">AGD OPE.1</a>	(ADV_FSP.1)	<a href="#">ADV FSP.4</a>
<a href="#">AGD PRE.1</a>	No Dependencies	
<a href="#">ALC CMC.4</a>	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	<a href="#">ALC CMS.4</a> , <a href="#">ALC DVS.2</a> , <a href="#">ALC LCD.1</a>
<a href="#">ALC CMS.4</a>	No Dependencies	
<a href="#">ALC DEL.1</a>	No Dependencies	
<a href="#">ALC DVS.2</a>	No Dependencies	
<a href="#">ALC LCD.1</a>	No Dependencies	
<a href="#">ALC TAT.1</a>	(ADV_IMP.1)	<a href="#">ADV IMP.1</a>
<a href="#">ASE CCL.1</a>	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	<a href="#">ASE ECD.1</a> , <a href="#">ASE INT.1</a> , <a href="#">ASE REQ.2</a>
<a href="#">ASE ECD.1</a>	No Dependencies	
<a href="#">ASE INT.1</a>	No Dependencies	

<a href="#">ASE_OBJ.2</a>	(ASE_SPD.1)	<a href="#">ASE_SPD.1</a>
<a href="#">ASE_REQ.2</a>	(ASE_ECD.1) and (ASE_OBJ.2)	<a href="#">ASE_ECD.1</a> , <a href="#">ASE_OBJ.2</a>
<a href="#">ASE_SPD.1</a>	No Dependencies	
<a href="#">ASE_TSS.1</a>	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	<a href="#">ADV_FSP.4</a> , <a href="#">ASE_INT.1</a> , <a href="#">ASE_REQ.2</a>
<a href="#">ATE_COV.2</a>	(ADV_FSP.2) and (ATE_FUN.1)	<a href="#">ADV_FSP.4</a> , <a href="#">ATE_FUN.1</a>
<a href="#">ATE_DPT.1</a>	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	<a href="#">ADV_ARC.1</a> , <a href="#">ADV_TDS.3</a> , <a href="#">ATE_FUN.1</a>
<a href="#">ATE_FUN.1</a>	(ATE_COV.1)	<a href="#">ATE_COV.2</a>
<a href="#">ATE_IND.2</a>	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	<a href="#">ADV_FSP.4</a> , <a href="#">AGD_OPE.1</a> , <a href="#">AGD_PRE.1</a> , <a href="#">ATE_COV.2</a> , <a href="#">ATE_FUN.1</a>
<a href="#">AVA_VAN.5</a>	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	<a href="#">ADV_ARC.1</a> , <a href="#">ADV_FSP.4</a> , <a href="#">ADV_IMP.1</a> , <a href="#">ADV_TDS.3</a> , <a href="#">AGD_OPE.1</a> , <a href="#">AGD_PRE.1</a> , <a href="#">ATE_DPT.1</a>

**Tableau 10 SARs dependencies**

#### 9.4 SFRs / TSS

Security Functional Requirements	TOE Summary Specification
<a href="#">FIA_ATD.1/Attributes</a>	<a href="#">Cardholder authentication</a> , <a href="#">External Authentication</a> , <a href="#">Access Control</a>
<a href="#">FIA_UAU.1/CHV</a>	<a href="#">Cardholder authentication</a>
<a href="#">FIA_UID.1/CHV</a>	<a href="#">Cardholder authentication</a>
<a href="#">FIA_AFL.1/CHV</a>	<a href="#">Cardholder authentication</a>
<a href="#">FIA_USB.1/CHV</a>	<a href="#">Cardholder authentication</a>
<a href="#">FIA_UAU.1/ExtAuth</a>	<a href="#">External Authentication</a>
<a href="#">FIA_UID.1/ExtAuth</a>	<a href="#">External Authentication</a>
<a href="#">FIA_AFL.1/ExtAuth</a>	<a href="#">External Authentication</a>
<a href="#">FIA_USB.1/ExtAuth</a>	<a href="#">External Authentication</a>
<a href="#">FDP_DAU.1/InitAuth</a>	<a href="#">Internal Authentication</a>
<a href="#">FDP_ETC.1/Export</a>	<a href="#">Access Control</a>
<a href="#">FDP_ITC.1/Import</a>	<a href="#">Access Control</a>
<a href="#">FMT_SMF.1/Selectable</a>	<a href="#">Secure personnalisation</a>
<a href="#">FDP_SDI.2/IntegrityControl</a>	<a href="#">Access Control</a>
<a href="#">FDP_ACC.1/AccessControl</a>	<a href="#">Pro mode</a> , <a href="#">External Authentication</a> , <a href="#">Access Control</a>
<a href="#">FDP_ACF.1/AccessControl</a>	<a href="#">Pro mode</a> , <a href="#">External Authentication</a> , <a href="#">Access Control</a>
<a href="#">FDP_UIT.1/Exchanges</a>	<a href="#">Pro mode</a> , <a href="#">External Authentication</a> , <a href="#">Access Control</a> , <a href="#">Secure personnalisation</a>
<a href="#">FDP_UCT.1/LoadKey</a>	<a href="#">Access Control</a>
<a href="#">FTP_ITC.1/Selectable</a>	<a href="#">Secure personnalisation</a>
<a href="#">FCS_COP.1/TDES</a>	<a href="#">Pro mode</a> , <a href="#">External Authentication</a> , <a href="#">Internal Authentication</a>
<a href="#">FCS_RNG.1/Random</a>	<a href="#">Random generation</a>
<a href="#">FCS_CKM.4/Destruction</a>	<a href="#">Pro mode</a> , <a href="#">External Authentication</a> , <a href="#">Internal Authentication</a>
<a href="#">FPT_PHP.3</a>	<a href="#">Cardholder authentication</a> , <a href="#">Pro mode</a> , <a href="#">External Authentication</a> , <a href="#">Internal Authentication</a> , <a href="#">Random generation</a> , <a href="#">Access Control</a> , <a href="#">Secure personnalisation</a>
<a href="#">FPT_FLS.1</a>	<a href="#">Cardholder authentication</a> , <a href="#">Pro mode</a> , <a href="#">External Authentication</a> , <a href="#">Internal Authentication</a> , <a href="#">Random generation</a> , <a href="#">Access Control</a> , <a href="#">Secure personnalisation</a>

**Tableau 11 SFRs and TSS - Coverage**

TOE Summary Specification	Security Functional Requirements
<a href="#">Cardholder authentication</a>	<a href="#">FIA_ATD.1/Attributes</a> , <a href="#">FIA_UAU.1/CHV</a> , <a href="#">FIA_UID.1/CHV</a> , <a href="#">FIA_AFL.1/CHV</a> , <a href="#">FIA_USB.1/CHV</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FPT_FLS.1</a>
<a href="#">Pro mode</a>	<a href="#">FDP_ACC.1/AccessControl</a> , <a href="#">FDP_ACF.1/AccessControl</a> , <a href="#">FDP_UIT.1/Exchanges</a> , <a href="#">FCS_COP.1/TDES</a> , <a href="#">FCS_CKM.4/Destruction</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FPT_FLS.1</a>
<a href="#">External Authentication</a>	<a href="#">FIA_ATD.1/Attributes</a> , <a href="#">FIA_UAU.1/ExtAuth</a> , <a href="#">FIA_UID.1/ExtAuth</a> , <a href="#">FIA_AFL.1/ExtAuth</a> , <a href="#">FIA_USB.1/ExtAuth</a> , <a href="#">FDP_ACC.1/AccessControl</a> , <a href="#">FDP_ACF.1/AccessControl</a> , <a href="#">FDP_UIT.1/Exchanges</a> , <a href="#">FCS_COP.1/TDES</a> , <a href="#">FCS_CKM.4/Destruction</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FPT_FLS.1</a>
<a href="#">Internal Authentication</a>	<a href="#">FDP_DAU.1/InitAuth</a> , <a href="#">FCS_COP.1/TDES</a> , <a href="#">FCS_CKM.4/Destruction</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FPT_FLS.1</a>
<a href="#">Random generation</a>	<a href="#">FCS_RNG.1/Random</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FPT_FLS.1</a>
<a href="#">Access Control</a>	<a href="#">FIA_ATD.1/Attributes</a> , <a href="#">FDP_ETC.1/Export</a> , <a href="#">FDP_ITC.1/Import</a> , <a href="#">FDP_SDI.2/IntegrityControl</a> , <a href="#">FDP_ACC.1/AccessControl</a> , <a href="#">FDP_ACF.1/AccessControl</a> , <a href="#">FDP_UIT.1/Exchanges</a> , <a href="#">FDP_UCT.1/LoadKey</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FPT_FLS.1</a>
<a href="#">Secure personnalisation</a>	<a href="#">FMT_SMF.1/Selectable</a> , <a href="#">FDP_UIT.1/Exchanges</a> , <a href="#">FPT_ITC.1/Selectable</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FPT_FLS.1</a>

**Tableau 12 TSS and SFRs - Coverage**

## 9.5 EAL rationale

EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this security target is just such a product.

## 9.6 EAL augmentations rationale

### 9.6.1 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.

Advanced methodical 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 with ADV\_ARC.1 "Security architecture description", ADV\_FSP.2 "Security-enforcing functional specification", ADV\_IMP.1 "Implementation representation of the TSF", ADV\_TDS.3 "Basic modular design", AGD\_PRE.1 "Preparative procedures" and AGD\_OPE.1 "Operational user Guidance".

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>56/66</b>
-----------------------	-----------------	--------------------------	--------------

All these dependencies are satisfied by EAL4.

### 9.6.2 ALC\_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. This assurance component is a higher hierarchical component to EAL4 (only ALC\_DVS.1). Due to the nature of the TOE, there is a need for any justification of the sufficiency of these procedures to protect the confidentiality and integrity of the TOE.

ALC\_DVS.2 has no dependencies.

## 10 Statement of Compatibility

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

### 10.1 Compatibility between SFRs

The following table shows how the SFRs of the Composite TOE are supported by the SFRs of the underlying platform given in [COSMO-ST].

SFRs of the TOE	Supported by SFRs of the platform	Compatibility
FIA_ATD.1/Attributes	No correspondence	For CHVs status are stored in applet based on IAS ECC CHV result. No contradiction with the platform.
FIA_UAU.1/CHV	No correspondence	CHV is performed by IAS. Access control and adequateFile computations are performed by the applet. No contradiction with the platform.
FIA_UID.1/CHV	No correspondence	CHV is performed by IAS. Access control and adequateFile computations are performed by the applet. No contradiction with the platform.
FIA_AFL.1/CHV	No correspondence	All is managed by IAS ECC. No contradiction with the platform.
FIA_USB.1/CHV	No correspondence	It Deals only with CHV status which is internal to the applet. No contradiction with the platform.
FIA_UAU.1/ExtAuth	No correspondence	No contradiction with the platform.
FIA_UID.1/ExtAuth	No correspondence	No contradiction with the platform.
FIA_AFL.1/ExtAuth	No correspondence	No contradiction with the platform.
FIA_USB.1/ExtAuth	No correspondence	No contradiction with the platform.
FDP_DAU.1/InitAuth	No correspondence	No contradiction with the platform.
FDP_ETC.1/Export	No correspondence	No contradiction with the platform.
FDP_ITC.1/Import	No correspondence	No contradiction with the platform.
FMT_SMF.1/Selectable	No correspondence	No contradiction with the platform.
FDP_SDI.2/IntegrityControl	FDP_SDI.2	Files data are protected by a checksum during storage; this is managed by the applet. CHV are stored in secure IAS ECC objects. Keys are stored in key secure containers of the platform. They are all protected such as error detection lead to a kill card. No contradiction with the platform:
FDP_ACC.1/AccessControl	No correspondence	No contradiction with the platform.
FDP_ACF.1/AccessControl	No correspondence	No contradiction with the platform.

FDP_UIT.1/Exchanges	FDP_UIT.1/CM	Integrity is enforced by the cryptogram computed in Pro Mode or in External Authentication; this is managed by the applet. The platform can also ensure integrity when using a GP secure channel. It can be used any time but is mandatory in Selectable state. No contradiction with the platform.
FDP_UCT.1/LoadKey	No correspondence	Managed by the applet. Keys are always encrypted during import so there no need to add an encryption layer through a GP secure channel. No contradiction with the platform.
FTP_ITC.1/Selectable	FTP_ITC.1/CM	GP secure channel are enforced by the platform. Nevertheless, the applet must support it for functional reasons when using security level 2 or 3. Indeed, the applet must ask for the Card Manager to decrypt data or to check cryptogram validity. No contradiction with the platform.
FCS_COP.1/TDES	FCS_COP.1	No contradiction with the platform.
FCS_RNG.1/Random	FCS_RNG.1/SCP	No contradiction with the platform.
FCS_CKM.4/Destruction	FCS_CKM.4	This is ensured by the usage of key secure containers of the platform. No contradiction with the platform.
FPT_PHP.3	FPT_PHP.3/SCP	No contradiction with the platform.
FPT_FLS.1	FPT_FLS.1, FPT_FLS.1/Installer FPT_FLS.1/ADEL FPT_FLS.1/ODEL FPT_FLS.1/SCP, FAU_ARP.1	No contradiction with the platform.

## 10.2 Compatibility between OTs

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

Platform Security Objectives	Composite Security Objectives	Compatibility
O.SID	No correspondence	No contradiction to this ST
O.FIREWALL	No correspondence	No contradiction to this ST
O.GLOBAL_ARRAYS_CONFID	No correspondence	No contradiction to this ST
O.GLOBAL_ARRAYS_INTEG	No correspondence	No contradiction to this ST
O.NATIVE	No correspondence	No contradiction to this ST
O.OPERATE	O.Operate	No contradiction to this ST
O.REALLOCATION	No correspondence	No contradiction to this ST
O.RESOURCES	O.Operate	No contradiction to this ST
O.ALARM	O.Operate	No contradiction to this ST
O.CIPHER	O.Authentication, O.TOE_Usurpation, O.Import, O.Confidentiality_Protection, O.Integrity_Protection, O.replay_Protection, O.Crypto	No contradiction to this ST
O.KEY-MNGT	O.Authentication, O.TOE_Usurpation, O.Import, O.Confidentiality_Protection, O.Integrity_Protection, O.replay_Protection, O.Crypto	No contradiction to this ST
O.PIN-MNGT	O.Integrity_Protection	No contradiction to this ST

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>59/66</b>
-----------------------	-----------------	--------------------------	--------------

O.BIO-MNGT	O.Integrity_Protection	No contradiction to this ST
O.TRANSACTION	No correspondence	No contradiction to this ST
O.OBJ-DELETION	O.Operate	No contradiction to this ST
O.DELETION	O.Operate	No contradiction to this ST
O.LOAD	O.Import, O.Integrity_Protection, O.replay_Protection, O.Confidentiality_Protection,	No contradiction to this ST
O.INSTALL	O.Import, O.Confidentiality_Protection, O.Integrity_Protection, O.replay_Protection, O.Operate	No contradiction to this ST
O.SCP.IC	O.Tamper, O.Authentication, O.replay_Protection, O.Crypto, O.Confidentiality_Protection, O.Integrity_Protection, O.Operate	No contradiction to this ST
O.SCP.RECOVERY	O.Operate	No contradiction to this ST
O.SCP.SUPPORT	No correspondence	No contradiction to this ST
O.CARD-MANAGEMENT	O.Import, O.Confidentiality_Protection, O.Integrity_Protection, O.replay_Protection	No contradiction to this ST
O.RESIDENT_APPLICATION	No correspondence	No contradiction to this ST
O.SECURE_COMPARE	No correspondence	No contradiction to this ST
O.PATCH_LOADING	O.Import, O.Confidentiality_Protection, O.Integrity_Protection, O.replay_Protection	No contradiction to this ST

### 10.3 Compatibility between OEs

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

Platform OE	Composite OE	Compatibility
OE.APPLLET	No Native API can be nested within Applet loaded in post issuance as the platform only allows the loading of Java Card bytecode.	No contradiction to this ST
OE.VERIFICATION	This objective is fulfilled by the applet included in the TOE. The applet is verified then included in the generated platform in IDEMIA facilities.	No contradiction to this ST
OE.CODE-EVIDENCE	The verified applet is included in the TOE pre-issuance in IDEMIA facilities then the whole TOE is sent to the manufacturer according to audited organizational measures. It ensures that it has not been changed since the code verification required in OE.VERIFICATION.	No contradiction to this ST

### 10.4 Compatibility between As

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

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>60/66</b>
-----------------------	-----------------	--------------------------	--------------

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

### 10.5 Compatibility between OSPs

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

Platform OSP	Composite OSP	Compatibility
OSP.VERIFICATION	Guidance of the Platform-Developer for the Application-Developer and recommendations related to the isolation property of the platform have to be applied in the application code	No contradiction to this ST

### 10.6 Compatibility between Ts

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

Platform T	Composite T	Compatibility
T.CONFID-APPLI-DATA	T.Tearing, T.DistantServer_Usurpation, T.TOE_Usurpation, T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay, T.Replay	No contradiction to this ST
T.CONFID-JCS-CODE	T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.CONFID-JCS-DATA	T.Tearing, T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.INTEG-APPLI-CODE	T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.INTEG-APPLI-CODE.LOAD	T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.INTEG-APPLI-DATA	T.Tearing, T.DistantServer_Usurpation, T.TOE_Usurpation, T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.INTEG-APPLI-DATA.LOAD	T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.INTEG-JCS-CODE	T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.INTEG-JCS-DATA	T.Tearing, T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.SID.1	T.Tearing, T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.SID.2	T.Tearing, T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST

T.EXE-CODE.1	No correspondence	No contradiction to this ST
T.EXE-CODE.2	No correspondence	No contradiction to this ST
T.NATIVE	No correspondence	No contradiction to this ST
T.RESOURCES	T.Tearing, T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.DELETION	T.Tearing, T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.INSTALL	T.Tearing, T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST
T.OBJ-DELETION	T.Tearing	No contradiction to this ST
T.PHYSICAL	T.Tearing, T.DistantServer_Usurpation, T.Keys_Disclosure, T.CHV_Disclosure, T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.PTC_Corruption, T.CHV_Corruption, T.Replay, T.User_Usurpation, T.TOE_Usurpation	No contradiction to this ST
T.CONFIGURATION	No correspondence	No contradiction to this ST
T.CONF_DATA_APPLET	No correspondence	No contradiction to this ST
T.PATCH_LOADING	T.Keys_Corruption, T.Files_Corruption, T.ACs_Corruption, T.CHV_Corruption, T.Keys_Disclosure, T.CHV_Disclosure, T.PTC_Corruption, T.Replay	No contradiction to this ST

## 10.7 Compatibility between SFs

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

Platform TSF	Usage by TOE
SF_ATOMIC_TRANSACTION	Relevant SF, used by Cardholder authentication, Pro mode, External Authentication, Internal Authentication, Random generation, Access Control, Secure personalisation
SF_CARD_CONTENT_MANAGEMENT	Relevant SF, used by Secure personalisation, Cardholder authentication, Pro mode, External Authentication, Internal Authentication, Random generation, Access Control
SF_CARD_MANAGEMENT_ENVIRONMENT	Not relevant
SF_CARDHOLDER_VERIFICATION	Not relevant
SF_CLEARING_OF_SENSITIVE_INFORMATION	Relevant SF, used by Cardholder authentication, Pro mode, External Authentication, Internal Authentication, Random generation, Access Control, Secure personalisation

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>63/66</b>
-----------------------	-----------------	--------------------------	--------------

Platform TSF	Usage by TOE
SF_DAP_VERIFICATION	Relevant SF, used by Pro mode, External Authentication, Access Control, Secure personalisation
SF_DATA_COHERENCY	Relevant SF, used by Cardholder authentication, Pro mode, External Authentication, Internal Authentication, Random generation, Access Control, Secure personalisation
SF_DATA_INTEGRITY	Relevant SF, used by Access Control, Cardholder authentication, Pro mode, External Authentication, Internal Authentication, Random generation, Secure personalisation
SF_ENCRYPTION_AND_DECRYPTION	Relevant SF, used by Pro mode, External Authentication, Access Control, Secure personalisation, Internal Authentication
SF_ENTITY_AUTHENTICATION/SECURE_CHANNEL	Not relevant
SF_EXCEPTION	Relevant SF, used by Cardholder authentication, Pro mode, External Authentication, Internal Authentication, Random generation, Access Control, Secure personalisation
SF_FIREWALL	Relevant SF, used by Cardholder authentication, Pro mode, External Authentication, Internal Authentication, Random generation, Access Control, Secure personalisation
SF_GP_DISPATCHER	Relevant SF, used by Secure personalisation
SF_HARDWARE_OPERATING	Relevant SF, used by Cardholder authentication, Pro mode, External Authentication, Internal Authentication, Random generation, Access Control, Secure personalisation
SF_KEY_ACCESS	Not relevant
SF_KEY_AGREEMENT	Relevant SF, used by Pro mode, External Authentication, Internal Authentication
SF_KEY_DESTRUCTION	Relevant SF, used by Pro mode, External Authentication, Internal Authentication
SF_KEY_DISTRIBUTION	Not relevant
SF_KEY_GENERATION	Not relevant
SF_KEY_MANAGEMENT	Not relevant
SF_MANUFACTURER_AUTHENTICATION	Not relevant
SF_MESSAGE_DIGEST	Relevant SF, used by Pro mode, External Authentication, Internal Authentication
SF_MEMORY_FAILURE	Relevant SF, used by Cardholder authentication, Pro mode, External Authentication, Internal Authentication, Random generation, Access Control, Secure personalisation
SF_PREPERSONALISATION	Relevant SF, used by Secure personalisation
SF_RANDOM_NUMBER	Relevant SF, used by Random generation
SF_RESIDENT_APPLICATION_DISPATCHER	Not relevant
SF_RUNTIME_VERIFIER	Not relevant
SF_SECURITY_FUNCTIONS_OF_THE_IC	Relevant SF, used by Random generation
SF_SIGNATURE	Relevant SF, used by Pro mode, External Authentication, Internal Authentication
SF_UNOBSERVABILITY	Not relevant

## 10.8 Compatibility of Assurance Requirements

The level of assurance of the:

- TOE is EAL4 augmented with ALC\_DVS.2 and AVA\_VAN.5
- JC Platform is EAL5 augmented with ALC\_DVS.2 and AVA\_VAN.5

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

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>64/66</b>
-----------------------	-----------------	--------------------------	--------------

**11 Glossary**

DF	Dedicated File
EF	Elementary File
MF	Master File
CHV	Card Holder Verification
CHVx methods	CHV number 1 (CHV1) or CHV number 2 (CHV2) – Authentication
CHVx/AUTH	Stands for the requirement of both CHVx and AUTH authentications
CHVx/Pro	Stands for the requirement of both CHVx and Pro mode authentications
PRO	Authentication method by symmetric signature of data
AUTH	Authentication method by external authentication
ALWAYS	Means that the access to a file is always granted
NEVER	Means that the access to a file is always denied
IAS	Identification, Authentication and Signature
ECC	Electronic Citizen Card
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
IC	Integrated Circuit
BIOS	Basic Input/Output System
API	Application programming interface
CPS2ter	name of the old "ASIP santé" smartcard and its current emulation
PIN	Personal Identification Number
APDU	Application Protocol Data Unit
CLA	Class parameter in the [ISO 7816-4] APDU format
INS	Instruction parameter in the [ISO 7816-4] APDU format
HID	Human Interface Device
SF	Security Functionality
AC	Access Condition
PTC	PIN Try Counter
PC	Personal Computer
3DES	Triple Data Encryption Standard
PUK	PIN Unlock Key (note that it is just a regular PIN with a specific unlocking purpose)
GP	Global Platform

## 12 References

- [CC-1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017. CCMB-2017-04-001.
- [CC-2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-002.
- [CC-3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-003.
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004.
- [COSMO-ST] ID-One Cosmo v8.2 – Public Security Target, FQR 110 9067, Ed 11. IDEMIA.
- [FIPS 46-3] "FIPS PUB 46-3, Data Encryption Standard", October 25, 1999 (ANSI X3.92), National Institute of Standards and Technology.
- [FIPS 81] "3FIPS PUB 81, DES Modes of Operation", April 17, 1995, National Institute of Standards and Technology.
- [GP] Global Platform, Card Specification, Version 2.2.1 – January 2011.
- [IAS] European Card for e-Services and national e-ID Applications - IAS ECC v1.0.1.
- [IAS ECC-ST] IAS ECC v2, version 1.3, in configuration #1 on ID-One Cosmo v8.2 open platform on NXP P6022M VB - Public Security Target, FQR 110 9184, Ed 2. IDEMIA.
- [IC-cert] NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software certified by the BSI (BSI-DSZ-CC-1059-V4-2021) on 24-06-2021.
- [ISO 7816-4] ISO/IEC 7816-4:2013, Identification Cards — Integrated circuit cards— Part 4: Organization, security and commands for interchange.
- [JCAPI] "Java Card - API" Application Programming Interfaces, Classic Edition Version 3.0.4, May, 2009, Sun Microsystems.
- [JCRE] "Java Card – JCRE" Runtime Environment Specification, Classic Edition Version 3.0.4, September, 2011, Sun Microsystems.
- [JCVM] "Java Card - Virtual Machine Specifications" Classic Edition, Version 3.0.4 May, 2009, Sun Microsystems.
- [NIST SP 800-90] The NIST SP 800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revise), March 2007.
- [PLT] ID-One Cosmo v8.2 certified under references:  
 2019/28, 19 July 2019  
 2019/28-M02 - 30/07/2020  
 2019/28-S01 – 17/11/2022
- [SRS] CPS2ter Java Applet, Software Requirements Specifications, 070837 00 SRS.

<b>FQR : 110 9044</b>	<b>Issue: 6</b>	<b>Date : 07/04/2023</b>	<b>66/66</b>
-----------------------	-----------------	--------------------------	--------------