jTOPv27-ASEv1 — Security Target

Emission Date	:	25-feb-2009
Project Name	:	Escarpe
Document Type	:	Technical report
Ref./Version	:	PU-2008-RT-356/1.4
Classification	:	Public Diffusion
Number of pages	:	72 (including 1 header pages)

Table of contents

Table of figures

Table of tables

1 Introduction

This chapter identifies this Security Target, its TOE, presents its general structure and introduces the references, notation conventions and technical terms to be used in the following chapters.

1.1 ST Identification

Title :	jTOPv27-ASEv1 composite ST
Author :	Trusted Labs S.A.S.
Address :	5, rue du Bailliage 78000 Versailles, France
Version :	1.4
Date of creation :	May 2008
Keywords :	Electronic Signature Application; Smart Card; Java Card; GlobalPlatform; JTOP

1.2 TOE Identification

1.2.1 Composite TOE

Commercial name :	JCASE
TOE version :	1.0
Product type :	Java Card Smart Card with Java Card Application for Electronic Signature

1.2.2 Configuration of composite TOE

TOE part 1	
Commercial name :	JCLX80jTOP20ID
Platform Version :	jTOP IFX#27.01 with patch v1.4
IC identifier :	SLE66CLX800PE
IC design step :	*E13, A14*

TOE part 2	
Application name :	ASE
Version :	20080917-121344

1.3 Diffusion List

1.4 Revisions and Comments

Version	Issue date	Comments
1.4	25/02/2009	Update of documents version number
1.3	13/10/2008	Use of RSA instead of ECDSA
1.2	7/10/2008	Minor changes in SFR
1.1	11/09/2008	Comments from intermediate RTE
1.0	01/07/2008	Initial version

1.5 CC Conformance and Evaluation Assurance Level

This Composite Security Target is compliant with the following Common Criteria for Information Technology Security Evaluation documents:

- Part 1: Introduction and general model, August 2005, Version 2.3, CCMB-2005-08-001,
- Part 2: Security functional requirements, August 2005, Version 2.3, CCMB-2005-08-002,
- Part 3: Security assurance requirements, August 2005, Version 2.3, CCMB-2005-08-003,
- Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0, CCDB-2007-09-001

and with the Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, August 2005, Version 2.3, CCMB-2005-08-004.

This Security Target claims the following ISO/IEC 15408:2005 conformance:

- Part 1: conformant
- Part 2: conformant
- Part 3: EAL 4 augmented with ADV_IMP.2 and AVA_VLA.4 with SOF-high as the minimum strength for the security functions.

1.6 PP Claims

This security target is inspired from PP SSCD Type 3 [PP0006]. However, the conformance to that PP is not claimed.

2 Overview

This document is the Composite Security Target of the Electronic Signature Application on top of the jTOP (Java™ Trusted Open Platform) of [ST-jTOP].

The intended TOE of this ST is a smart card consisting of Hardware and Software.

The first portion of the TOE is composed of a piece of software embedded into a SLE66CLX800PE chip which transforms the IC into a secure platform device (Java™ Trusted Open Platform hereinafter referred to as "TOE part 1"), and the second portion of the TOE is the Electronic Signature Application (ASE hereinafter referred to as "TOE part 2") operating on TOE part 1.

TOE part 1 is compliant with Java Card 2.2.1 and Visa GlobalPlatform 2.2.1-Configuration 2 standards and is independently evaluated and certified with the evaluation assurance level EAL 5+.

TOE part 2 offers a set of electronic signature services compliant with the security characteristics of the electronic signature creation devices.

This ST presents a description of the TOE and its the security environment, identifies the assets to be protected, the threats to be countered by the TOE or its environment, describes the security objectives for the TOE and for its environment, states the security functional requirements and the security assurance requirements and finally provides a TOE summary specification.

2.1 Associated Documents

2.1.1 Reference Documents

The following documents are cited in this document.

[ST-jTOP]	Trusted Logic, *JCLX80jTOP20ID — Java™ Trusted Open Platform Security Target,* ref. CP-2007-RT-075-1.1.
[CC]	Common Criteria for Information Technology Security Evaluation : *Part 1: Introduction and general model*, August 2005, version 2.3, ref CCMB-2005-08-001; *Part 2: Security functional requirements*, August 2005, version 2.3, ref CCMB-2005-08-002; *Part 3: Security assurance requirements*, August 2005, version 2.3, ref CCMB-2005-08-003.
[CEM]	Common Methodology for Information Technology Security, *Evaluation : Evaluation Methodology*, August 2005, version 2.3, ref CCMB-2005-08-004.
[PP0006]	Protection Profile — *Secure Signature-Creation Device Type 3*, Version: 1.05, 25 July 2001. *Certified by the BSI with the reference BSIPP-0006-2002T.*

[ST-jTOP]	Trusted Logic, *JCLX80jTOP20ID — Java™ Trusted Open Platform Security Target,* ref. CP-2007-RT-075-1.1.
[DIRECTIVE]	Directive 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signature
[JCRE]	Sun Microsystems, *Java Card 2.2.1 Runtime environment specification*, October 2003
[SSCD]	European Committee for Standardization (CEN), *Application Interface for Smart Card used as Secure Signature Creation Devices*, CWA 14890-1:2004 (E), 22 December 2003
[CPESC]	*Composite product evaluation for Smart Cards and similar devices*, Version 1.0, Revision 1, CCDB-2007-09-001, September 2007

2.1.2 Related Documents

[ACM]	Trusted Labs, *jTOPv27-ASEv1 —Configuration Management Plan*, ref. CP-2008-RT-361
[ADM]	Trusted Labs, *jTOPv27-ASEv1 — Administration Guide*, ref. CP-2008-RT-357
[ATE]	Trusted Labs, *jTOPv27-ASEv1 — Test Documentation*, ref. CP-2008-RT-408
[DEL]	Trusted Labs, *jTOPv27-ASEv1 — Delivery and Operation*, ref. CP-2008-RT-359
[DVS]	Trusted Labs, *jTOPv27-ASEv1 — Development Security*, ref. CP-2008-RT-362
[FSP]	Trusted Labs, *jTOPv27-ASEv1 — Functional Specification*, ref. CP-2008-RT-370
[HLD]	Trusted Labs, *jTOPv27-ASEv1 — High Level Design*, ref. CP-2008-RT-368
[IGS]	Trusted Labs, *jTOPv27-ASEv1 — Initialization Phase*, ref. CP-2008-RT-409
[LCD]	Trusted Labs, *jTOPv27-ASEv1 — Software Life Cycle*, ref. CP-2008-RT-360
[LLD]	Trusted Labs, *jTOPv27-ASEv1 — Low Level Design*, ref. CP-2008-RT-369
[TAT]	Trusted Labs, *jTOPv27-ASEv1 — Tools and Techniques*, ref. CP-2008-RT-364
[SOF]	Trusted Labs, *jTOPv27-ASEv1 — Strength Of Functions*, ref. CP-2008-RT-365
[SPM]	Trusted Labs, *jTOPv27-ASEv1 — Security Policy Model*, ref. CP-2008-RT-367
[USR]	Trusted Labs, *jTOPv27-ASEv1 — User Guide*, ref. CP-2008-RT-358
[VLA]	Trusted Labs, *jTOPv27-ASEv1 — Vulnerability Analysis*, ref. CP-2008-RT-363

2.2 Acronyms

Acronym	Meaning
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface

Acronym	Meaning
CC	Common Criteria
DES	Data Encryption Standard
DTBS	Data To Be Signed
ECDSA	Elliptic Curve DSA
GP	GlobalPlatform
IC	Integrated Circuit
ISD	Issuer Security Domain
jTOP	Java Trusted Open Platform
MAC	Message Authentication Code
OS	Operating System
PIN	Personal Identification Number
PP	Protection Profile
RSA	Rivert Shamir Adleman
SCP	Smart Card Platform
SAR	Security Assurance Requirement
SF	Security Function
SFR	Security Functional Requirement
SP	Service Provider
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functions
VGP	Visa GlobalPlatform

3 TOE Description

This chapter presents the general IT features of the TOE and the main security concerns.

TOE part 1 (jTOP) is independently evaluated and certified to the evaluation assurance level EAL 5+.

TOE part 2 (ASE) is compositely evaluated, with TOE part 1, to the evaluation assurance level EAL4+ (EAL4 augmented with AVA_VLA.4).

The composite evaluation aims to certify the TOE (TOE part 1 + TOE part 2) to the evaluation assurance level EAL 4+ (EAL4 augmented with AVA_VLA.4 and ADV_IMP.2).

3.1 Product type

jTOP for Java Trusted Open Platform (TOE part 1) is an open smart card composed of a piece of software embedded into a SLE66CLX800PE chip. By open smart card is meant a smart card enabling the possibility of enlarging and restricting the set of applications installed on the card. The Platform is compliant with Java Card 2.2.1 and Visa GlobalPlatform 2.2.1-Configuration 2 standards

The signature application (TOE part 2) is a Java Card application (applet) installed on the smart card and intended to securely create electronic signatures.

The TOE to be evaluated is composed of TOE part 1 and TOE part 2 (see Figure 1).

The TOE communicates with a terminal device (for example a PC with a card reader) by APDU messages compliant with the ISO/IEC 7816-4 standard.

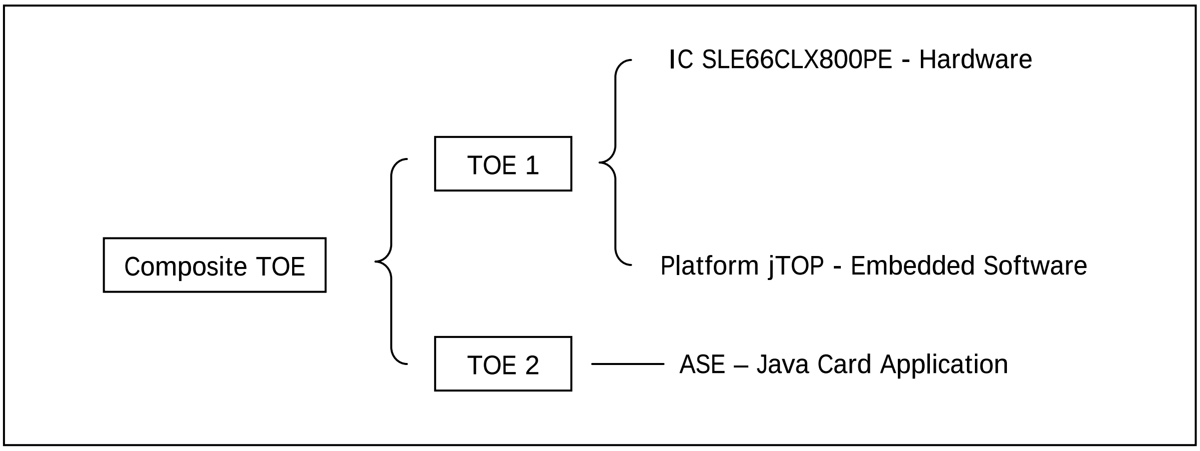
IC SLE66CLX800PE - Hardware
TOE 1
Composite TOE
Platform jTOP - Embedded Software
TOE 2
ASE – Java Card Application

Figure 1: Product type of the TOE

3.2 Physical scope of the TOE

The physical scope of the TOE is as illustrated in Figure 2. The physical scope of the TOE is the part inside by the dashed line. For more details on the architecture of jTOP refer to §3.1 of [ST-jTOP].

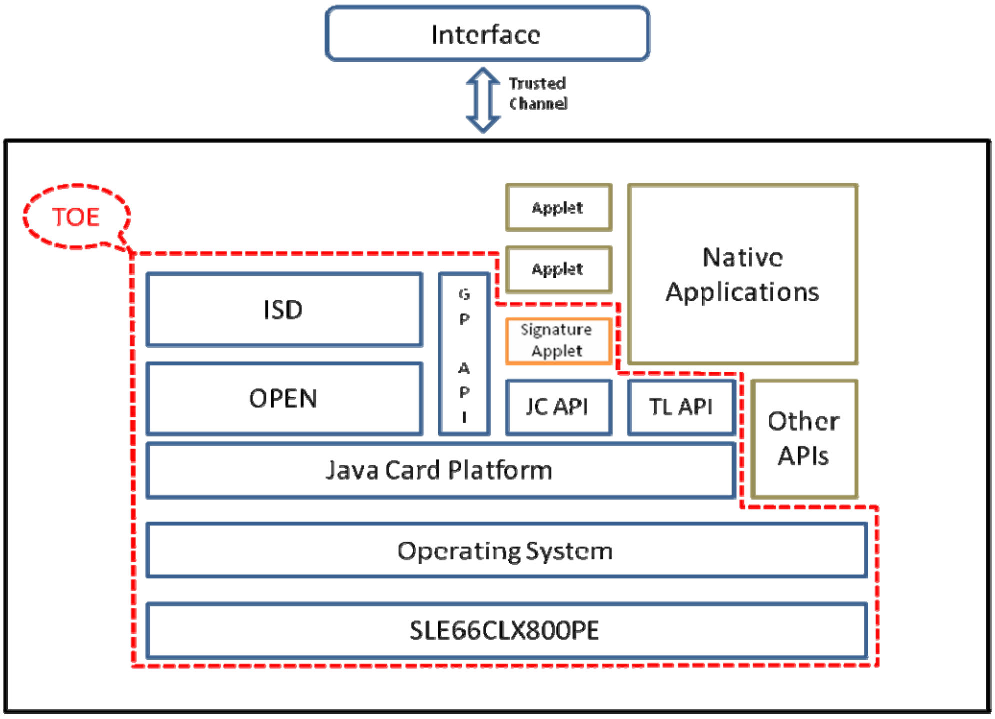

Figure 2: Physical scope of the TOE

3.3 Logical scope of the TOE

The logical scope of the TOE is as presented in Figure 3 and Figure 4.

The logical range of the TOE is the part bordered by the dashed line.

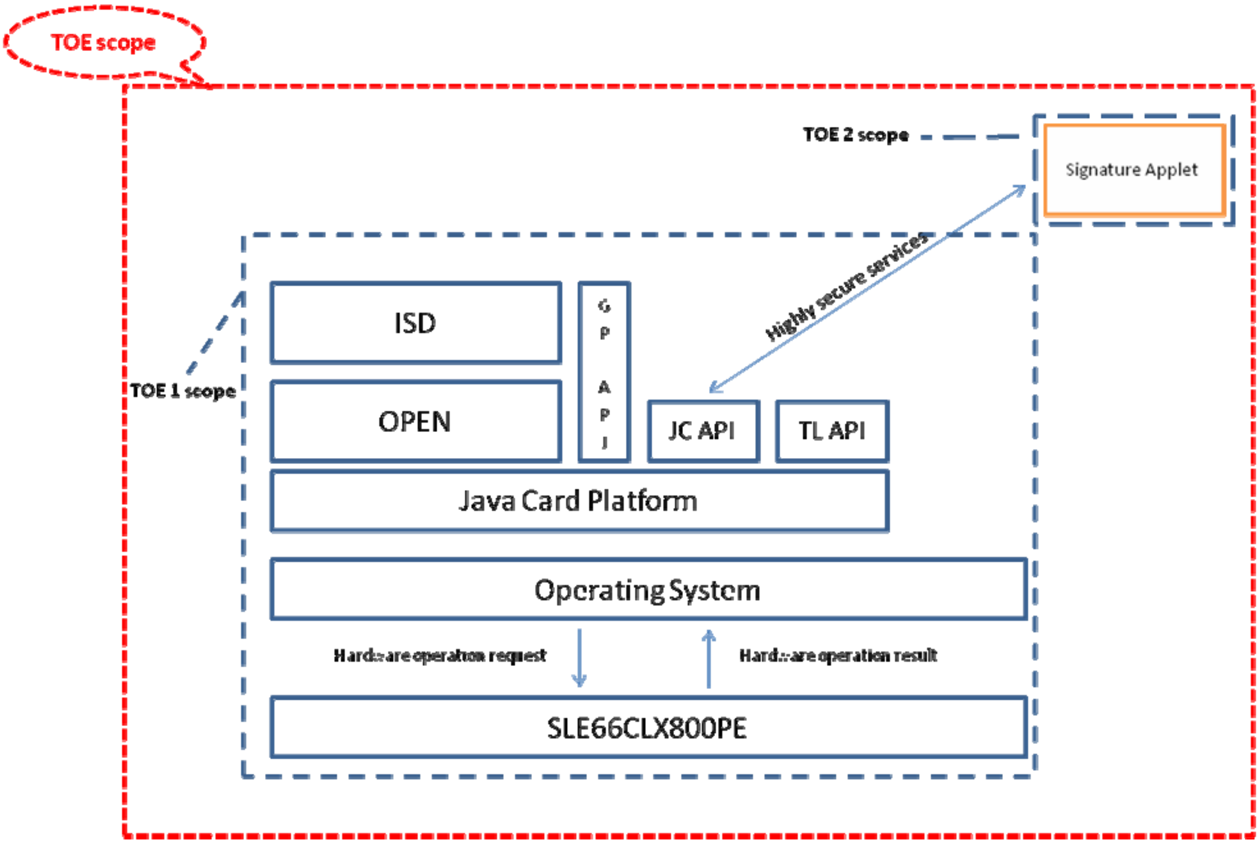

Figure 3: Logical scope of the TOE

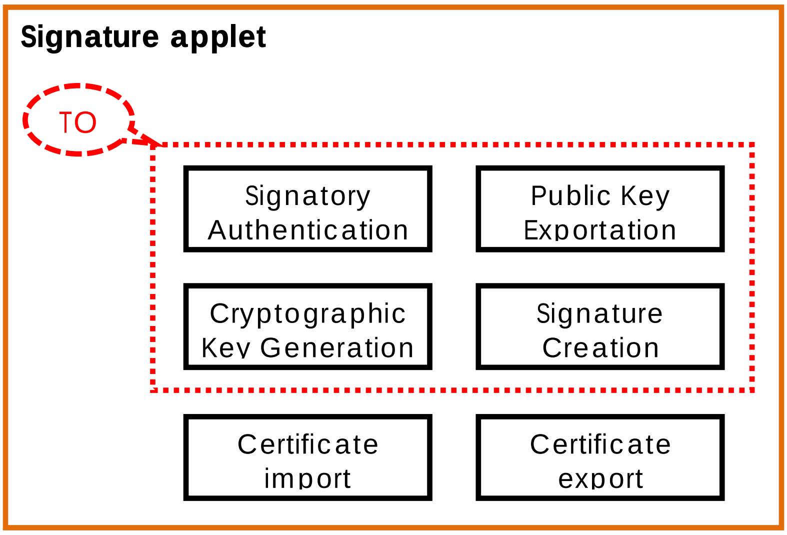

Figure 4: Logical scope of the TOE for the Signature Application

The jTOP platform provides the Signature Application with a collection of highly secure services available through the JC API. Those services are listed hereafter in §3.4. The security functions provided by the Signature Applet are detailed in §3.5. The functions related to certificate management are outside the scope of evaluation since the certificates are not considered as assets.

3.4 Functions of TOE part 1

The jTOP platform provides the following principal highly secure services:

- Cardholder authentication and management of the PIN
- Cryptography services including encryption and decryption, electronic signature generation and verification, and generation of random data.
- Life cycle management.
- Administration services including downloading, installation and suppression of the applet (OPEN and ISD)
- Management of the APIs access.
- Applications isolation (Java Card firewall)

For further details on the TSF of jTOP refer to the §3 of [ST-jTOP].

3.5 Functions of TOE part 2

The Signature Application manages:

- A PIN to authenticate the signatory.
- A set of asymmetric cryptographic key pairs, with a unique identifier, for signature purposes.
- A symmetric cryptographic key, hereafter called *Admin key*, used to authenticate messages issued by the application.
- Another symmetric cryptographic key, hereafter called *SP key*, used to decrypt the data sent to the application (PIN and message to be sign).

The Signature Application offers the following security features:

Cryptographic keys generation

Upon request of the administrator, the application generates a public/private key pair (format RSA 1536 bits) and takes charge of its management. This operation is carried out under the control of the administrator, who must first authenticate himself through a secure channel via the ISD of the jTOP platform.

Public key export

Once a key pair is generated, the corresponding public key is returned to the Administrator through the controlling application on the terminal device (e.g. a PC), protected in authenticity with a MAC created from the Admin key.

Signatory authentication

The signature application allows signatory authentication by comparing the value of the PIN entered by the signatory with the value of the reference PIN managed by the application. This PIN code is encrypted (with the data to be signed) before being sent to the TOE using the shared SP key stored in the SP application and the TOE.

Electronic Signature

After signatory authentication (PIN code decryption and verification), the signature application is able to sign the data to be signed and to return the signature.

The Signature Application also offers storage facilities for certificates:

Certificates storage

The Signature Application can store electronic certificates corresponding to the signature, by an off-card Certification Authority, of the public keys stored on-card. Only the administrator, after authentication with the ISD secure channel, can import electronic certificates. Export of these certificates does not require authentication.

3.6 Users and roles

The Users and roles defined in §3.2.2 of [ST-jTOP] remain valid for the composite TOE. The following actors can interact with the Electronic Signature Application:

Card Administrator

The Card Administrator is also the administrator of the signature application. He manages the electronic signature applet and requests cryptographic key generation.

Signatory (Card User)

The cardholder uses the electronic signature application for signing messages he approves.

ASE Application Provider

The ASE Application Provider is the organization that develops the Java Card Electronic Signature Application.

Service provider

This actor can ask the cardholder to sign messages so as to obtain the message approval.

Application integrator

This actor loads and installs the signature application on top of jTOP within the IC and personalizes it with a PIN code, a shared key for the Administrator, a shared key for the Service Provider and a serial number.

3.7 TOE Life Cycle

3.7.1 Overview of the TOE Life Cycle

The life-cycle of the composite TOE is the life cycle of the smart card (IC + OS + Signature Applet), from the development to the operational stage through manufacturing and personalisation. The life cycle of the TOE part 1 is described in §3.2.3 of [ST-jTOP] and integrates the composition TOE life cycle, as described in Figure 5.

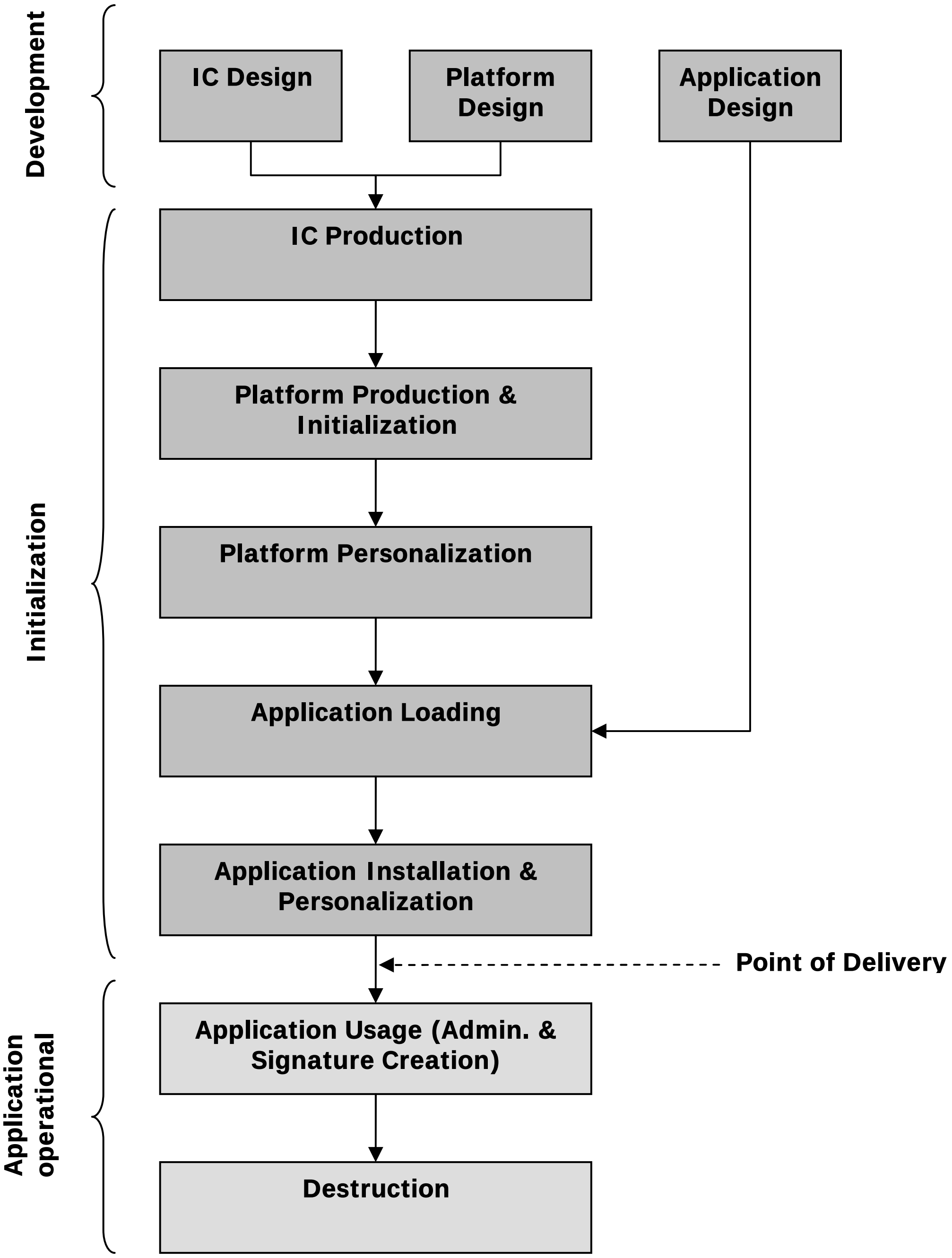

Figure 5: Composite TOE life cycle

The development phase includes:

- Platform development, which starts by the design of the IC and all the components of the Embedded Software: Operating System, Java Card Runtime Environment and the Card Manager. This phase is carried out by the Platform Developer.
- Application development of the Electronic Signature applet. This phase is carried out by the ASE Application Provider.

The initialization phase includes:

- Platform initialization, which consists of masking the Embedded Software on the IC, initializing this software, loading a patch if necessary and embedding the IC into its plastic or paper carrier. This phase is carried out by the Platform Developer.
- Platform personalization, which consists on loading Card Issuer's data (ISD keys and other initial data) on the IC. After this phase, the card enters reaches its INITIALIZED state. This phase is carried out by the Platform Developer.
- Signature Applet initialization, which consists of bytecode verifying and loading the applet and then on installing and personalizing this applet. This phase is carried out by the Platform Developer.

The TOE enters its operation phase once the platform and Signature Applet have been successfully initialized. At this point, all the security functions defined in this Security Target are activated and operational.

After being initialized with the Cardholder's data, the TOE is delivered to the Cardholder. The Card Issuer provides the Cardholder with user guides for accessing to the services provided by the smart card in the most secured way. During this stage, the Card Administrator also performs all the card management activities described in Section 3.1.5 of [ST-jTOP] following the same administrator guides provided by the Platform Developer for the personalization step. This includes downloading new applets on the smart card, according to the instructions of the Card Issuer.

The delivery of the TOE occurs after personalization of the Signature Application.

3.7.2 Signature Applet on-card life cycle

The on-card life cycle of the Signature Applet (see Figure 6) is compliant with the GlobalPlatform standard life cycle. GlobalPlatform specifications define three basic life cycle states:

- **Installed** state corresponding to the status of the applet after its installation. During this step, the applet can also be personalized. This is the case of the Signature Applet, personalized with the PIN code of the signatory, a serial number, shared keys and the type of supported cryptography (RSA) for the operation phase ;
- **Selectable** state in which the application can be selected to send commands and is ready to acquire one or more cryptographic key pairs (up to 5 key pairs);
- **Locked** state which is a reversible state in which the application is non-selectable and its services are temporarily blocked.

The applet specification also includes specific states:

- **Usage** state corresponding to the signature creation process once it's installed, personalized, selected and contains one or more cryptographic key pairs.
- **Terminated** state which is an irreversible state in which the applet and its data are destroyed.

The transition from **Installed** to **Selectable** and the transition of a **Locked** state in the previous blocking state are done through the ISD, by sending the SET STATUS command. The transitions for the other states are carried by the signature application through API calls.

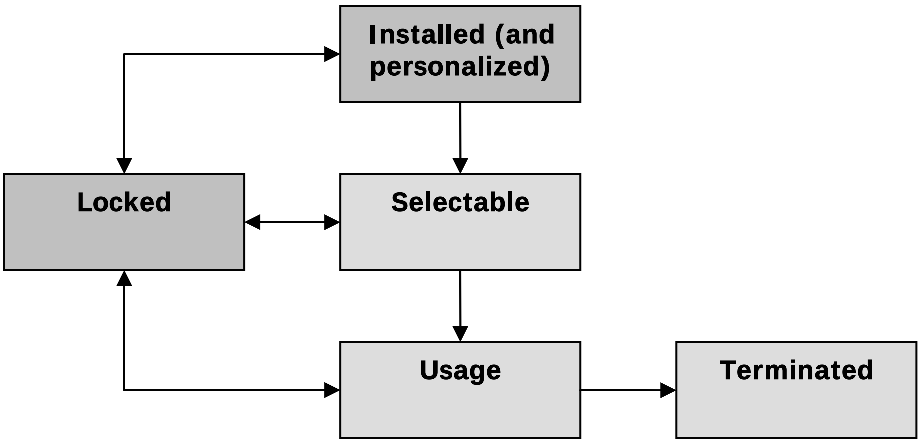

Figure 6: Signature Applet on-card life cycle

3.8 TOE intended usage

Usage of the jTOP platform is described in [ST-jTOP].

The main use of the signature application embedded in a smart card is to ensure the integrity and the authenticity of the messages transmitted from sender to recipient. The signature application supports RSA cryptographic algorithms for signature creation. The algorithm that will be used for signature creation is specified during the personalization phase, prior to the operation phase.

To preserve the confidentiality of the private key which is used to encrypt the message, this private key is stored in the smart card which is designed to be tamper-resistant.

This section describes a typical usage of the Signature Applet and the required components to unroll the scenario.

At the beginning of the scenario, the card with the Signature Applet is supposed to be in its point of delivery (see Figure 5), with the card in its INITIALIZED phase, the Signature Applet loaded, install and personalized with the PIN code of the signatory, the shared keys (Admin Key, SP Key), its serial number and the type of supported cryptography (RSA).

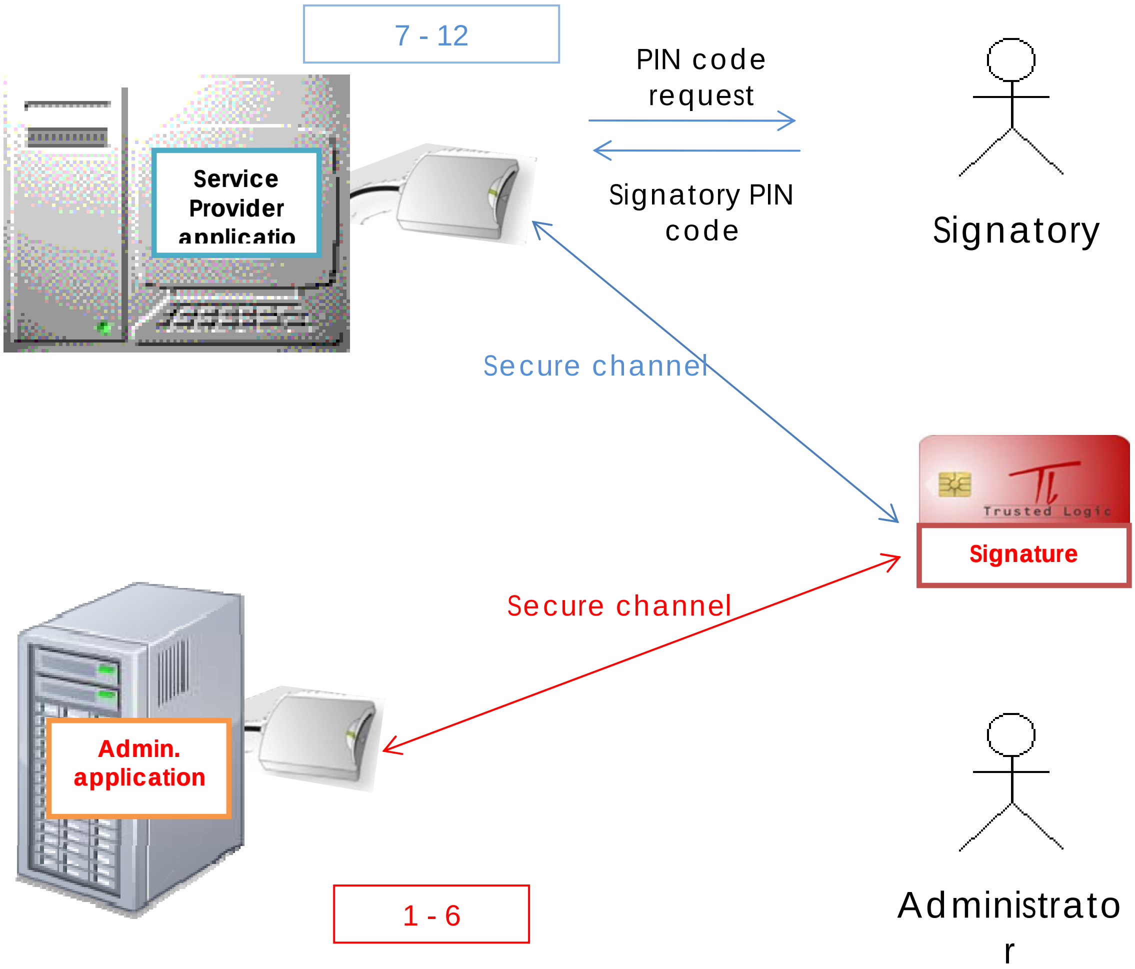

Figure 7: TOE usage scenario

Service Provider application

This application on the PC belongs to the Service Provider and is aimed at handling the input data of the signatory. It communicates with the signatory through an interface and with the signature application through a card reader.

The SP application offers the following features to the signatory:

- Data field for inserting authentication data (PIN code)
- Presentation of the data to be signed
- Selection of the certificate to be used
- A mean to express the signatory agreement to sign
- Interruption of the signature creation process before sending the data to be signed to the TOE.

Administration application

This application on a PC belongs to the administrator and is intended to handle the input data of the administrator. It communicates with the administrator through an interface and with the signature application embedded with the card through a card reader.

3.8.1 Administration

The following scenario (see Figure 7) addresses the administration of the TOE:

1. The smart card with the personalized signature applet embedded-in is inserted in a card reader connected to the administration PC.

2. A dedicated application on the PC interrogates the signature application to verify that its life-cycle state is Selectable or Usage.

3. The administration application establishes a GlobalPlatform secure channel with the signature application on the smart card, via the ISD, prior to any on-card key generation operation.

4. The administration application asks the signature application to generate a cryptographic key pair. The generated public key is sent back to the PC, protected in authenticity with a MAC using the Admin Key. The public key is subsequently checked for authenticity on the administration PC.

5. Optionally, the administration application asks an external Certification Authority to generate a certificate for the public key and imports the corresponding certificate to the signature application.

6. The Administrator closes the secure channel between the administration PC and the signature application.

3.8.2 Usage

The following scenario (see Figure 7) addresses a typical usage of the TOE:

7. The application on the service provider PC offers the user to subscribe to a service provider offer (credit, service ...) and then to approve the purchase by an electronic signature using the signature application. The signatory accepts.

8. The smart card with the personalized signature applet embedded-in is inserted in a card reader connected to a service provider PC.

9. The application on the PC verifies the existence of a recognized and valid certificate for the cryptographic key pairs stored on the signature application. It asks the signature application to export the certificates it holds.

10. The application on the PC asks the user to validate:

a. The key pair used by the signature application for this transaction ;

b. The subscription characteristics of the offer.

by entering his PIN code

11. The signatory enters his PIN code.

a. The SP application encrypts the PIN code and the data to be signed before sending it to the TOE, to protect them in confidentiality and integrity. The encrypted data is sent to the TOE.

This process involves the use of a shared key on the service provider PC to encrypt the data. This key can be stored on Secure Access Module (SAM) that processes and encrypts APDU commands to send to the TOE.

b. The TOE decrypts the received data using a shared key stored in the TOE and verifies the PIN legitimacy.

c. The TOE signs with the private key the data characterizing the accepted offer and sends the result back to the application on the PC.

12. The application on the service provider PC uses the public key corresponding to the recognized certificate previously retrieved from the smart card to check the signed data. It then displays the offer subscription confirmation.

4 TOE security environment

4.1 Assets

The following assets are security relevant elements to be directly protected by the TOE.

4.1.1 Assets of TOE part 1

For a detailed description of the assets of TOE part 1 concerning the underlying IC and the jTOP platform refer to [ST-jTOP].

4.1.2 Assets of TOE part 2

All the TOE's assets concerning the dedicated Signature Application are listed below:

Private Keys

Private keys used to perform an electronic signature creation.

Protection: integrity and confidentiality

Public Keys

Public keys linked to the private key and used to perform electronic signature verification.

Protection: integrity

Data to be signed

Set of data which is intended to be signed after the signatory approval.

Protection: integrity

Signatory PIN code

PIN code entered by the signatory and transmitted to the TOE to perform a signature operation.

Protection: confidentiality

Reference PIN code

Reference PIN code stored initialy in the smart card and used to identify and authenticate the signatory.

Protection: integrity and confidentiality

Admin Key

The cryptographic key used for ensuring the integrity and origin of messages issued by the signature application (MAC generation). It is stored in both the card and the administrator application.

Protection: integrity and confidentiality

SP Key

The cryptographic key used for ensuring the integrity and origin of the PIN code and the data to be signed (MAC generation). It is stored in both the card and the service provider application.

Protection: integrity and confidentiality

Signed Data

The data returned by the signature application corresponding to the signature of the data to be signed.

Protection: unforgeabilty

4.2 Assumptions

This section describes the assumptions that are made regarding the TOE security environment. All the assumptions mentioned in the security target [ST-jTOP] are relevant.

4.3 Threats

The TOE as defined in chapter 2 is required to counter the threats referenced or described hereafter. An attacker who wishes to abuse the assets can proceed either by functionnal attacks, environmental manipulations, specific hardware manipulations or by any other type of attack.

Each attack is introduced giving its identifier and a short description of the general method used by the attacker. Each threat is always associated with one or more assets that are directly impacted and with the users that may be involved in the attack. Such information will be displayed in the TOE rationale associated to each threat.

The threats listed below, which focus on the Signature Application, are largely inspired from [PP0006]. Some of them refine those already present in [ST-jTOP].

All the platform threats of [ST-jTOP] are also relevant to the composite security target.

4.3.1 Disclosure

T.Private_Key_Disclosure

An attacker discloses the private key stored in the TOE in order, for instance, to use it for signature creation outside the TOE.

T.SP_Key_Disclosure

An attacker discloses the SP key stored in the TOE in order to disclose the PIN code entered by the Signatory or to modify the data to be signed.

T.Admin_Key_Disclosure

An attacker discloses the Admin key stored in the TOE in order to use it to authenticate messages issued by the smart card.

T.PIN_Code_Disclosure

An attacker discloses the value of the reference PIN stored in the TOE in order, for instance, to illegitimately and subsequently authenticate as the signatory to a service.

4.3.2 Counterfeiting

T.Public_Key_Counterfeiting

An attacker counterfeits public key during its transmission outside the TOE. Therefore the authenticity of the exported public key is compromised.

T.Signed_Data_Counterfeiting

An attacker counterfeits signed data by duplication or falsification of authentic signature creation attributes.Therefore, the signed data integrity is violated without the knowledge of the signatory or third parties.

4.3.3 Repudiation

T.Signature_Repudiation

The signature application performs signature creation without the signatory authentication. This can lead to a repudiation of the signature process, the signatory denying having signed data with the private key in the TOE.

4.3.4 Integrity

T.Physical

This threat concerns physical attacks, by tampering means, on the smart card chip so as to disclose secrets managed by the Signature Applet. It is directly connected to the *T.PHYSICAL* and *T.PHYS-TAMPER* threats in [ST-jTOP].

T.Private_Key_Derivation

An attacker derives the private key from the public key, the signature created or the certificate, which is a threat against the secrecy of the private key.

4.4 Organisational security policies

This section describes the rules to which both the TOE and its human environment shall comply when addressing security needs related to the generation of qualified electronic signature.

All the OSPs listed in the [ST-jTOP] are relevant for the composite TOE.

This security targets adds the following OSP related to the signature application:

P.Trustworthy_SP

The Service Provider protects from misuses the PIN entered by the signatory. The Service Provider generates and sends the DTBS the signatory wishes to sign in a form appropriate for signing by the TOE.

P.Secrets

Only the Signature Application Personalizer may load secrets protecting the assets of the signature application: SP key, Admin Key, Reference PIN code. Those secrets shall be generated, distributed and stored off-card, destroyed and exported to the card in a secure manner, which prevents the attacker to obtain them from the IT or non-IT environment. A trusted channel shall ensure the origin, integrity and confidentiality of:

- the Reference PIN code transmitted to the Cardholder
- the SP Key transmitted to the Service Provider
- the Admin Key transmitted to the Administrator.

5 Security objectives

5.1 Security objectives for the TOE

This section defines the security objectives for the composite TOE.

All the platform security objectives given in [ST-jTOP] are considered as included into this composite security target. The security objectives given hereafter are those specifically relevant for the Signature Applet on the platform. They are satisfied either by technical countermeasures implemented by the Signature Applet, by the platform or by a combination of the two.

O.Design

The smart card must be designed in a way to provide protection against disclosure of confidential TSF or User data stored and/or processed in the TOE.

O.Tamper_Detection

The TOE provides security means to detect physical tampering of the TOE components, and use those features to limit security breaches.

O.Tamper_Resistant

The TOE provides security features intended to prevent an attacker from extracting or altering the TOE sensitive data. The physical device should be tamper resistant.

O.Keys_Generation_Quality

The TOE shall guarantee a high cryptographic quality for public/private keys pair generation. The private key should be unique and cannot be derived from the public key.

O.Electronic_Signature_Robustness

The TOE generates electronic signature that cannot be forged without knowledge of the private key. The private key cannot be reconstructed using the electronic signatures. High encryption techniques guarantee the robustness of signatures.

O.SP_Key_Secrecy

The TOE shall protect SP key stored on-card, used to decrypt the PIN code and the data to be signed, in integrity and confidentiality.

O.Admin_Key_Secrecy

The TOE shall protect Admin key stored on-card, used to authenticate the messages (public keys) exported from the TOE, in integrity and confidentiality.

O.PIN_Code_Secrecy

The TOE shall protect the Reference PIN code stored on-card in integrity and confidentiality.

O.Private_Key_Secrecy

The TOE shall protect private keys stored on-card, used to create an electronic signature, in integrity and confidentiality.

O.Public_Key_Authenticity

The TOE provides means to enable the administrator application to verify the authenticity of the public key exported from the TOE.

O.Data_To_Be_Signed_Integrity

The TOE provides means to verify the integrity of the data to be signed sent to the TOE.

O.Key_Destruction

The TOE shall provide safe destruction techniques for private keys stored in the applet in case of replacement of the key or deletion of the applet.

O.Administrator_Authentication

The TOE shall ensure that the administrator is authenticated before enabling generation of public/private key pairs.

O.Signatory_Authentication

The TOE shall authenticate the signatory before providing him the signature creation function.

5.2 Security objectives for the environment

This section defines the security objectives for the environment of the TOE.

The significant security objectives for the environment of the platform security target are those linked to relevant assumptions.

All the security objectives for the environment of the jTOP are relevant to this security target. The specific objectives concerning the signature application are listed below:

OE.PIN_Entry

The human interface for signatory authentication should guarantee the confidentiality and the integrity of the PIN code as needed by the authentication process employed.

OE.Secrets

The attacker shall not be able to obtain the reference PIN codes or secret keys stored in the card (SP key, Admin key) from the TOE non-IT environment.

OE.Public_Key_Authenticity

The Service Provider verifies the authenticity of the public key of the key pair intended to be used in the TOE and the correspondence between the private key used for signature creation in the TOE and the public key.

OE.Data_Intended_To_Be_Signed

The Service Provider

- generates the DTBS the signatory intends to sign in a form appropriate for signing by the TOE,
- sends the DTBS to the TOE protected in integrity.

6 IT security requirements

6.1 TOE security functional requirements

This section describes the requirements imposed on the TOE in order to achieve the security objectives laid down in the previous chapter. All the requirements identified in this section are instances of those stated in [CC2].

All the platform security functional requirements are relevant to the composite security target. All the operations performed on the platform SFR are appropriate for the composite TOE since the TOE includes the full platform.

The minimum SOF level for the TOE security functional requirements is SOF-High.

The SFRs listed below state requirements specific to the signature application.

6.1.1 Cryptographic support

FCS_COP.1/ Public key export MAC generation Cryptographic operation

FCS_COP.1.1/ Public key export MAC generation The TSF shall perform **Public key export MAC generation** in accordance with a specified cryptographic algorithm **DES_MAC8** and cryptographic key sizes **112 bits** that meet the following: **FIPS PUB 46-3, ISO 9797 (method 2 padding scheme)**.

Application note:

This functional security requirement is handled by the jTOP platform security functions.

FCS_COP.1/ PIN and DTBS decryption Cryptographic operation

FCS_COP.1.1/ PIN and DTBS decryption The TSF shall perform **PIN code and data to be signed decryption** in accordance with a specified cryptographic algorithm **Triple DES in CBC mode** and cryptographic key sizes **112 bits** that meet the following: **FIPS PUB 46-3, ANSI X9.52, ISO 9797 (method 2 padding scheme)**.

FCS_COP.1/ Signature creation RSA Cryptographic operation

FCS_COP.1.1/ Signature creation RSA The TSF shall perform **electronic signature creation** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1536 bits** that meet the following: **PKCS#1 (padding algorithm)**.

Application note:

This functional security requirement is handled by the jTOP platform security functions.

FCS_CKM.1/ Key generation RSA Cryptographic key generation

FCS_CKM.1.1/ Key generation RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA-CRT key components generation using a true random number generator and Miller-Rabin algorithm for testing key components primality** and specified cryptographic key sizes **1536 bits** that meet the following: **Annex A of IEEE P1363-2000**.

Application note:

This functional security requirement is handled by the jTOP platform security functions

FCS_CKM.4/ Key destruction Cryptographic key destruction

FCS_CKM.4.1/ Key destruction The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **physical erasure of private key value** that meets the following: **none**.

6.1.2 User data protection

FDP_IFC.1/ Public key export Subset information flow control

FDP_IFC.1.1/ Public key export The TSF shall enforce the **Public key export SFP** on

- **subject: on-card Signature application and off-card subjects**
- **information: Public key sent through APDU responses**
- **operation: Public key export**.

FDP_IFF.1/ Public key export Simple security attributes

FDP_IFF.1.1/ Public key export The TSF shall enforce the **Public key export SFP** based on the following types of subject and information security attributes:

- **The APDU messages exchanged between the on-card and the off-card subjects for public key export have a single security attribute, namely, the MAC ensuring the integrity and the origin of the message.**.

FDP_IFF.1.2/ Public key export The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **For public key export, a MAC of the public key, generated from the Admin key, is appended to the APDU response.**.

FDP_IFF.1.3/ Public key export The TSF shall enforce the **none**.

FDP_IFF.1.4/ Public key export The TSF shall provide the following **none**.

FDP_IFF.1.5/ Public key export The TSF shall explicitly authorise an information flow based on the following rules: **Any public key export request.**.

FDP_IFF.1.6/ Public key export The TSF shall explicitly deny an information flow based on the following rules: **none**.

FDP_ETC.1/ Public key export Export of user data without security attributes

FDP_ETC.1.1/ Public key export The TSF shall enforce the **Public key export SFP** when exporting user data, controlled under the SFP(s), outside of the TSC.

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

Global refinement:

User data is a public key

FDP_UIT.1/ Public key export Data exchange integrity

FDP_UIT.1.1/ Public key export The TSF shall enforce the **Public key export SFP** to be able to **transmit** user data in a manner protected from **modification and insertion** errors.

FDP_UIT.1.2/ Public key export The TSF shall be able to determine on receipt of user data, whether **modification and insertion** has occurred.

Global refinement:

User data is public key

FDP_ACC.1/ Keys generation Subset access control

FDP_ACC.1.1/ Keys generation The TSF shall enforce the **Key generation SFP** on

- **subject: Signature application**

- **object: private / public key pair**
- **operation: generation of private / public key pair**.

FDP_ACF.1 / Keys generation Security attribute based access control

FDP_ACF.1.1 / Keys generation The TSF shall enforce the **Keys generation SFP** to objects based on the following: **signature application key management status: either "authorised" or "not authorised"**.

FDP_ACF.1.2 / Keys generation The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **Key generation is allowed if the signature application key management status is set to "authorised"**.

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

FDP_ACF.1.4 / Keys generation The TSF shall explicitly deny access of subjects to objects based on the

- **The signature application key management status is set to "not authorised"**.

FDP_ACC.1 / Signature creation Subset access control

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

- **subject: Signature application**
- **object: DTBS and private key**
- **operation: Signature**.

FDP_ACF.1 / Signature creation Security attribute based access control

FDP_ACF.1.1 / Signature creation The TSF shall enforce the **Signature creation SFP** to objects based on the following:

- **signature application authorised service provider: either "yes" or "no"**
- **signature application authenticated signatory: either "yes" or "no"**.

FDP_ACF.1.2 / Signature creation The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **Signature of DTBS with the private key is allowed if the signatory has the authenticated signatory attribute set to "yes" and if the DTBS is sent by a service provider with the authorised service provider attribute set to "yes"**.

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

FDP_ACF.1.4/ Signature creation The TSF shall explicitly deny access of subjects to objects based on the

- **Signature of DTBS with the private key is not allowed if the signatory has the authenticated signatory attribute set to "no"**
- **Signature of DTBS with the private key is not allowed if the DTBS is sent by a service provider with the authorised service provider attribute set to "no"**.

FDP_UIT.1/ DTBS and PIN code Data exchange integrity

FDP_UIT.1.1/ DTBS and PIN code The TSF shall enforce the **Signature creation SFP** to be able to **receive** user data in a manner protected from **insertion, modification and deletion** errors.

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

Global refinement:

User data consists of Data To Be Signed and PIN code.

FDP_RIP.1/ Signatory PIN Subset residual information protection

FDP_RIP.1.1/ Signatory PIN The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **Signatory PIN code**.

6.1.3 Identification and authentication

FIA_UAU.1/ User authentication Timing of authentication

FIA_UAU.1.1/ User authentication The TSF shall allow

- **Exporting public keys from the TOE to a remote IT product and the TOE by means of TSF required by FDP_UIT.1/ Public key export**
- **Establishing a trusted channel between a remote IT product and the TOE by means of TSF required by FTP_ITC.1/ DTBS and PIN code import**

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

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

Global refinement:

User stands for Administrator and Signatory.

FIA_UID.1/ User identification Timing of identification

FIA_UID.1.1/ User identification The TSF shall allow

- **Exporting public keys from the TOE to a remote IT product and the TOE by means of TSF required by FDP_UIT.1/ Public key export**
- **Establishing a trusted channel between a remote IT product and the TOE by means of TSF required by FTP_ITC.1/ DTBS and PIN code import**

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

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

Global refinement:

User stands for Administrator and Signatory.

FIA_AFL.1/ Signatory authentication failure Authentication failure handling

FIA_AFL.1.1/ Signatory authentication failure The TSF shall detect when **3** unsuccessful authentication attempts occur related to **consecutive failed Signatory authentication attempts**.

FIA_AFL.1.2/ Signatory authentication failure When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **block Reference PIN code**.

6.1.4 Security management

FMT_MSA.1/ Administrator Management of security attributes

FMT_MSA.1.1/ Administrator The TSF shall enforce the **Key generation SFP** to restrict the ability to **modify** the security attributes **signature application key management status** to **Administrator**.

FMT_MSA.1/ Signatory Management of security attributes

FMT_MSA.1.1/ Signatory The TSF shall enforce the **Signature creation SFP** to restrict the ability to **modify** the security attributes **signature application authenticated signatory attribute and signature application authorised service provider attribute** to **Signatory**.

FMT_MSA.2 / Authentication Secure security attributes

FMT_MSA.2.1 / Authentication The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 / Signature creation Static attribute initialisation

FMT_MSA.3.1 / Signature creation The TSF shall enforce the **Signature creation SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 / Signature creation The TSF shall allow the **none** to specify alternative initial values to override the default values when an object or information is created.

Global refinement:

The restrictive default value for the security attributes:

- signature application authenticated signatory
- signature application authorised service provider is "no".

FMT_MSA.3 / Public key export Static attribute initialisation

FMT_MSA.3.1 / Public key export The TSF shall enforce the **Public key export SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 / Public key export The TSF shall allow the **none** to specify alternative initial values to override the default values when an object or information is created.

Global refinement:

The restrictive default value for the security attribute is the MAC of the public key.

FMT_SMR.1 / User's role Security roles

FMT_SMR.1.1 / User's role The TSF shall maintain the roles **Administrator and Signatory**.

FMT_SMR.1.2 / User's role The TSF shall be able to associate users with roles.

6.1.5 Trusted path/channels

FTP_ITC.1/ DTBS and PIN code import Inter-TSF trusted channel

FTP_ITC.1.1/ DTBS and PIN code import The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/ DTBS and PIN code import The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/ DTBS and PIN code import The TSF shall initiate communication via the trusted channel for **DTBS and PIN code import**.

Global refinement:

The trusted channel protects the DTBS and PIN code in integrity and confidentiality.

Application note:

This communication channel is defined as following: Once the signatory enters his PIN code and before sending it to the TOE, the SP application encrypts the PIN, the DTBS and a hash of the message using the SP key. After receiving the encrypted PIN code from the SP application, the TOE decrypts it using the shared SP key.

6.2 TOE security assurance requirements

Composite-SAR is weaker or equal than Platform-SAR. That is, for each assurance requirement in Composite-SAR there is an assurance requirement in Platform-SAR that is either the same or higher in the CC hierarchy of the assurance family.

The security assurance requirement level is EAL4. The EAL is augmented with AVA_VLA.4 and ADV_IMP.2.

6.3 Security requirements for the IT environment

6.3.1 IT environment functional requirements

The significant security functional requirements for the environment of the platform security target are those linked to significant security objectives for the environment

This section describes the requirements for the environment of the TOE. All the requirements identified in this section are instances of those stated in [CC2].

All the platform security functional requirements for the environment are relevant to the composite security target.

The SFRs listed below state requirements specific to the environment of the signature application.

FDP_UIT.1/ SP DTBS and PIN code Data exchange integrity

FDP_UIT.1.1/ SP DTBS and PIN code The TSF shall enforce the **Signature creation SFP** to be able to **transmit** user data in a manner protected from **insertion, modification and deletion** errors.

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

Global refinement:

User data consists of Data To Be Signed and PIN code

FDP_UIT.1/ Admin Public key export Data exchange integrity

FDP_UIT.1.1/ Admin Public key export The TSF shall enforce the **Public key export SFP** to be able to **receive** user data in a manner protected from **modification and insertion** errors.

FDP_UIT.1.2/ Admin Public key export The TSF shall be able to determine on receipt of user data, whether **modification and insertion** has occurred.

Global refinement:

User data is public key

FTP_ITC.1/ SP DTBS and PIN code import Inter-TSF trusted channel

FTP_ITC.1.1/ SP DTBS and PIN code import The TSF shall provide a communication channel between itself and a remote 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/ SP DTBS and PIN code import The TSF shall permit **the TSF** to initiate communication via the trusted channel.

FTP_ITC.1.3/ SP DTBS and PIN code import The TSF shall initiate communication via the trusted channel for **DTBS and PIN code import**.

Application note:

This communication channel is defined as following: Once the signatory enters his PIN code and before sending it to the TOE, the SP application encrypts the PIN, the DTBS and a hash of the message using the SP key. After receiving the encrypted PIN code from the SP application, the TOE decrypts it using the shared SP key.

7 TOE summary specification

7.1 TOE security functions

This chapter introduces the TOE Security Functions (TSF) that instantiate the security requirements stated in the previous section. Each function is introduced providing its name and a description.

All the Platform-TSFs [ST-jTOP] are relevant to the TOE composite security target since the composite product offers the full security functionality of the platform.

The TSF mentioned hereafter are specific to the signature application.

The minimum strength for the security functions is SOF-high.

Administrator authentication

This TSF enforces the authentication of the Administrator before providing him the authorization to generate public/private key pairs. This process is done through a secure channel with the ISD. The corresponding protocol, Secure Channel Protocol (SCP02), is described in [ST-jTOP].

This function has no strength.

Public Key Export

On an user request of a public key export, this TSF enforces the authentication of the exported public key by a MAC generated from the admin key and appended to the request response.

This function has no strength.

Signatory and DTBS authentication

This TSF enforces the authentication of the Signatory and the DTBS before providing the Signatory the authorization to create electronic signature. To create electronic signature, the PIN counter must not have reached the maximal number of consecutive attempts. Once the signature application receives the encrypted Signatory PIN code and the DTBS, this TSF decrypts them using the SP key and verifies their legitimacy by checking the integrity of the message (presence of a hash code) and by comparing the submitted PIN code with the reference PIN code stored in the signature application. If the signatory PIN code and the reference PIN code match, then the presumed Signatory is given the authority to create electronic signature and the PIN counter is reset. Otherwise, the PIN counter is increased.

The strength of this function is SOF-high.

Key generation

This TSF enforces the generation of a new private/public key pair (RSA). When the index assigned to this key pair is already occupied (key replacement), the previously stored private key is first erased. This TSF uses the platform supplied cryptographic functionalities to create key pairs of size 1536 bits for RSA.

This function has no strength.

Cryptographic operations

This TSF uses the platform supplied cryptographic functionalities to perform the cryptographic operations required by the other TSFs:

- MAC generation with a 112 bits key length
- 3DES decryption with a 112 bits key length
- RIPEMD-160 hash value calculation
- RSA signature algorithm with 1536 bits key size

This function has no strength.

7.2 Assurance measures

Configuration Management Plan

The assurance measures concerning Configuration Management are detailed in the Configuration Management Plan [ACM]. That document describes the configuration items under the control of the plan, the roles and the responsibilities involved in the signature application Configuration Management activities, and the rules and procedures to be observed when accomplishing those activities.

Initialization Phase Specification

The assurance measures concerning the initialization, generation and start-up of the TOE are detailed in [IGS]. That document describes the procedures to transform the chip containing the Embedded Software into a smart card ready to be used.

Delivery and Operation

The assurance measures concerning delivery and operation of the TOE are detailed in [DEL]. That document describes the distribution procedure used to deliver the binary code of the signature application embedded to the IC Manufacturer. The procedure is aimed to prevent any tampering with the actual version, or substitution of a false version. It also describes the mechanisms used to prevent that other persons apart from the intended receiver can use the code of the product and the validation procedures performed upon reception of the samples.

Administration Guide

The assurance measures concerning administration guidance are detailed in [ADM]. That document presents the administration procedures to securely manage the TOE. It details the precise sequences of commands to be sent in order to load and install new applet instances on the smart card.

User Guide

The assurance measures concerning user guidance are detailed in [USR]. That document describes some security guidelines to be applied when programming Java Card applets. Those guidelines enable to take the best of the Java Card Technology and the proprietary security functions of the TOE.

Development Security

The assurance measures concerning development security at the Signature application development site are detailed in [DEV]. That document provides a summary of the procedures, organizational security polices and physical devices that protect the access to the assets related to the TOE during its development phase.

Software Life Cycle

The assurance measures concerning the definition of the signature application life cycle are detailed in [LCD]. The description includes the main stages Concept, Development, Transition and Support, as well as the technical processes involved in the achievement of the stages' outcomes, in accordance to the standard ISO/IEC 15288.

Tools and Techniques

The assurance measures concerning tools and techniques used to develop the Embedded Software are detailed in [TAT]. That document covers the programming languages, source code editors and compilers, development environment tools and code linkers used to implement the signature application.

Strength of Functions Analysis

The assurance measures concerning analysis of the strength of the security functions defined in this Security Target are detailed in [SOF].

Vulnerability Analysis

The assurance measures concerning the vulnerability analysis of the security functions defined in this Security Target are detailed in [VLA]. That document identifies all the potential vulnerabilities of the TOE provides non-exploitation arguments for each of them.

Security Policy Model

The Security Policy Model of the TOE is detailed in [SPM]. The SPM is formed of a collection of labeled abstract state machines, each one detailing one of the security policies (SP) introduced in this Security Target.

Functional Specification

The Functional Specification of the TOE is detailed in [FSASE].

High Level Design

The High Level Design of the TOE is detailed in [HLD]. That document provides an overview of the systems that compose the architecture of the signature application and describe the main services that each of them provides.

Low Level Design

The Low Level Design of the signature application is detailed in [LLD]. This document provides an overview of the documentation of each of the modules that compose its implementation and refers to the documents detailing each module.

Implementation

The implementation of the signature application is provided by the tarball containing its commented source code files in Java.

Refinement Correspondance

The assurance measures concerning the refinement correspondence between the different representations of the Embedded Software are detailed in [ISD], [GPAPI], [JCAPI], [FSASE], [HLD] et [LLD]. For each representation, the associated documents contain a special chapter that provides the correspondence rationale with respect to the precedent representation level.

Test Documentation

The assurance requirements of the ATE class are satisfied by the tarball containing the Test Suites, the Test Logs resulting from their execution on the TOE, and the document [ATE]. This latter document includes three different parts:

- the Test Plan for the external interfaces defined in the Functional Specification and the interfaces of each system defined in the High Level Design of the signature application;
- the Test Procedure, describing how the test goals defined in the Test Plan are implemented;
- the Coverage Analysis, relating each security function to a collection of test goals in the Test Plan, each test goal to a collection of test cases in the Test Procedure and each test case to a collection of scripts of the Test Suite.
- the Depth Analysis, relating the systems (and services) defined in [HLD] to the test goals stated in the Test Plan.

8 Rationale

8.1 Security objectives rationale

8.1.1 Threats

8.1.1.1 Disclosure

T.Private_Key_Disclosure This threat is covered by the following security objectives: - O.Private_Key_Secrecy which assures the protection of the private key stored in the TOE.

- o O.Administrator_Authentication which ensures that nobody but the administrator can have the authority to create cryptographic private key in the TOE.
- o O.Design contributes in covering this threat by guaranteeing a security design that protects the private key from disclosure.
- o O.Key_Destruction which ensures that the private key is securely erased after key replacement, key deletion or applet deletion.

T.SP_Key_Disclosure This threat is covered by the security objective O.SP_Key_Secrecy which guarantees the secrecy of the custom key stored in the smart card against attacks with high level potential. The security objective O.Design also contributes in covering this threat by guaranteeing a security design that protects the admin key from disclosure.

T.Admin_Key_Disclosure This threat is covered by the security objective O.Admin_Key_Secrecy which guarantee the secrecy of the custom key stored in the smart card against attacks with high level potential. The security objective O.Design also contributes in covering this threat by guaranteeing a security design that protects the admin key from disclosure.

T.PIN_Code_Disclosure This threat is covered by the security objective O.PIN_Code_Secrecy which guarantees a high level of protection of the PIN code stored in the TOE. The security objective O.Design contributes in covering this threat by guaranteeing a security design that protects the PIN code from disclosure.

It is also covered by the security objective for the environment OE.PIN_Entry which assures that the integrity and confidentiality of the PIN code are protected by the SP application.

8.1.1.2 Counterfeiting

T.Public_Key_Counterfeiting This threat is covered by the following security objectves:

- o O.Public_Key_Authenticity which ensures that the TOE provides means to the administrator application to verify the authenticity of the public key exported from the TOE. and by the security objective and the environnement
- o OE.Public_Key_Authenticity that ensures that the Service Provider verifies the authenticity of the public key used for verification of signatures created by the TOE.

T.Signed_Data_Counterfeiting This threat is covered by the following security objectives:

- O.Key_Destruction which protects the private key by providing safe destruction techniques in case of regeneration.
- O.Private_Key_Secrecy which protects the private key against high level attacks.
- O.SP_Key_Secrecy which protects the custom key against high level attacks.
- O.PIN_Code_Secrecy which protects the PIN code stored in the TOE against high level attacks.
- O.Public_Key_Authenticity which ensures that the TOE provides means to the administrator application to verify the authenticity of the public key exported by the TOE.
- O.Tamper_Detection which ensures that the security functions of the TOE can detect physical tampering.
- O.Tamper_Resistant which ensures that the security functions of the TOE can resist to physical tampering.
- O.Keys_Generation_Quality which guarantees a high cryptographic quality for public/private keys pair generation
- O.Signatory_Authentication which imposes an authentication of the signatory before having access to the electonic signature function of the TOE.
- O.Electronic_Signature_Robustness which ensures that the TOE uses high encryption techniques in creating electronic signatures.
- O.Data_To_Be_Signed_Integrity which ensure that the TOE verifies the integrity for of the data sent for signature.
- OE.Data_Intended_To_Be_Signed which ensure that the Service Provider protects the data intended to be signed in integrity when sent to the TOE.
- OE.PIN_Entry which ensures that the PIN is protected by the signatory application in integrity and confidentiality.

8.1.1.3 Repudiation

T.Signature_Repudiation This threat is covered by the following security objectives:

- O.Signatory_Authentication which imposes an authentication of the signatory before having access to the electonic signature function of the TOE.
- O.Electronic_Signature_Robustness which ensures that the TOE uses high encryption techniques in creating electronic signatures.
- O.Data_To_Be_Signed_Integrity which ensure that the TOE verifies the integrity for of the data sent for signature.
- OE.Data_Intended_To_Be_Signed which ensure that the Service Provider protects the data intended to be signed in integrity when sent to the TOE.

8.1.1.4 Integrity

T.Physical This threat is countered by the following security objectives:

- O.Tamper_Detection which guarantee a that the security functions of the TOE detect physical tampering attacks.
- O.Tamper_Resistant which guarantee a high resistance of the TOE to physical tampering attacks.

- O.Private_Key_Secrecy which ensures that the private key is protected against physical attacks.
- O.SP_Key_Secrecy which ensures that the SP key is protected against physical attacks.
- O.Admin_Key_Secrecy which ensures that the Admin key is protected against physical attacks.
- O.PIN_Code_Secrecy which ensures that the PIN code stored in the TOE is protected against physical attacks.

T.Private_Key_Derivation This threat is covered by the following security objectives:

- O.Keys_Generation_Quality which ensures a high cryptographic quality for public/private keys pair generation and that the pirvate key should be unic and cannot be derived from the public key.
- O.Electronic_Signature_Robustness which guarantees a robust electonic signature by the use of high encryption techniques.

8.1.2 Organisational security policies

P.Trustworthy_SP This organisational security policy is covered by the security objectives on the environment:

- OE.PIN_Entry that protects the confidentiality and the integrity of the PIN code entered by the signatory,
- OE.Data_Intended_To_Be_Signed that specify how the Service Provider shall process the DTBS and by the security objective on the TOE O.Data_To_Be_Signed_Integrity which ensures the integrity verification of the DTBS sent by the TOE.

P.Secrets This organisational security policy is directly covered by the security objective on the environment OE.Secrets.

8.1.3 Rationale tables of environment elements and security objectives

Threats	Security objectives	Rationale
T.Private_Key_Disclosure	O.Private_Key_Secrecy, O.Design, O.Administrator_Authentication, O.Key_Destruction	Section 5.1.1
T.SP_Key_Disclosure	O.SP_Key_Secrecy, O.Design	Section 5.1.1
T.Admin_Key_Disclosure	O.Design, O.Admin_Key_Secrecy	Section 5.1.1
T.PIN_Code_Disclosure	O.PIN_Code_Secrecy, OE.PIN_Entry, O.Design	Section 5.1.1
T.Public_Key_Counterfeiting	O.Public_Key_Authenticity, OE.Public_Key_Authenticity	Section 5.1.1

Threats	Security objectives	Rationale
T.Signed_Data_Counterfeiting	O.Key_Destruction, O.Private_Key_Secrecy, O.SP_Key_Secrecy, O.PIN_Code_Secrecy, O.Public_Key_Authenticity, O.Tamper_Detection, O.Tamper_Resistant, O.Keys_Generation_Quality, O.Signatory_Authentication, O.Electronic_Signature_Robustness, OE.PIN_Entry, O.Data_To_Be_Signed_Integrity, OE.Data_Intended_To_Be_Signed	Section 5.1.1
T.Signature_Repudiation	O.Signatory_Authentication, O.Electronic_Signature_Robustness, O.Data_To_Be_Signed_Integrity, OE.Data_Intended_To_Be_Signed	Section 5.1.1
T.Physical	O.Tamper_Detection, O.Tamper_Resistant, O.Private_Key_Secrecy, O.PIN_Code_Secrecy, O.SP_Key_Secrecy, O.Admin_Key_Secrecy	Section 5.1.1
T.Private_Key_Derivation	O.Keys_Generation_Quality, O.Electronic_Signature_Robustness	Section 5.1.1

Table 1 Threats towards security objectives rationale

Security objectives	Threats	Rationale
O.Design	T.Private_Key_Disclosure, T.SP_Key_Disclosure, T.Admin_Key_Disclosure, T.PIN_Code_Disclosure	
O.Tamper_Detection	T.Signed_Data_Counterfeiting, T.Physical	
O.Tamper_Resistant	T.Signed_Data_Counterfeiting, T.Physical	
O.Keys_Generation_Quality	T.Signed_Data_Counterfeiting, T.Private_Key_Derivation	
O.Electronic_Signature_Robustness	T.Signed_Data_Counterfeiting, T.Signature_Repudiation, T.Private_Key_Derivation	
O.SP_Key_Secrecy	T.SP_Key_Disclosure, T.Signed_Data_Counterfeiting, T.Physical	
O.Admin_Key_Secrecy	T.Admin_Key_Disclosure, T.Physical	
O.PIN_Code_Secrecy	T.PIN_Code_Disclosure, T.Signed_Data_Counterfeiting, T.Physical	
O.Private_Key_Secrecy	T.Private_Key_Disclosure, T.Signed_Data_Counterfeiting, T.Physical	

Security objectives	Threats	Rationale
O.Public_Key_Authenticity	T.Public_Key_Counterfeiting, T.Signed_Data_Counterfeiting	
O.Data_To_Be_Signed_Integrity	T.Signed_Data_Counterfeiting, T.Signature_Repudiation	
O.Key_Destruction	T.Private_Key_Disclosure, T.Signed_Data_Counterfeiting	
O.Administrator_Authentication	T.Private_Key_Disclosure	
O.Signatory_Authentication	T.Signed_Data_Counterfeiting, T.Signature_Repudiation	
OE.PIN_Entry	T.PIN_Code_Disclosure, T.Signed_Data_Counterfeiting	
OE.Secrets		
OE.Public_Key_Authenticity	T.Public_Key_Counterfeiting	
OE.Data_Intended_To_Be_Signed	T.Signed_Data_Counterfeiting, T.Signature_Repudiation	

Table 2 Security objectives towards threats rationale

Assumptions	Security objectives for the environment	Rationale

Table 3 Assumptions towards security objectives for the environment rationale

Security objectives for the environment	Assumptions	Rationale
OE.PIN_Entry		
OE.Secrets		
OE.Public_Key_Authenticity		
OE.Data_Intended_To_Be_Signed		

Table 4 Security objectives for the environment towards assumptions rationale

Organisational security policies	Security objectives	Rationale
P.Trustworthy_SP	OE.PIN_Entry, O.Data_To_Be_Signed_Integrity, OE.Data_Intended_To_Be_Signed	Section 5.1.2
P.Secrets	OE.Secrets	Section 5.1.2

Table 5 Organisational security policies towards security objectives rationale

Security objectives	Organisational security policies	Rationale
O.Design		

Security objectives	Organisational security policies	Rationale
O.Tamper_Detection		
O.Tamper_Resistant		
O.Keys_Generation_Quality		
O.Electronic_Signature_Robustness		
O.SP_Key_Secrecy		
O.Admin_Key_Secrecy		
O.PIN_Code_Secrecy		
O.Private_Key_Secrecy		
O.Public_Key_Authenticity		
O.Data_To_Be_Signed_Integrity	P.Trustworthy_SP	
O.Key_Destruction		
O.Administrator_Authentication		
O.Signatory_Authentication		
OE.PIN_Entry	P.Trustworthy_SP	
OE.Secrets	P.Secrets	
OE.Public_Key_Authenticity		
OE.Data_Intended_To_Be_Signed	P.Trustworthy_SP	

Table 6 Security objectives towards organisational security policies rationale

8.2 Security requirements rationale

8.2.1 Objectives

8.2.1.1 Security objectives for the TOE

O.Design This security objective is handled in the jTOP [ST-jTOP] by the following security objectives O.PROT_INF_LEAK.

O.Tamper_Detection This security objective is handled in the jTOP [ST-jTOP] by the security objective O.PROT_PHYS_TAMPER.

O.Tamper_Resistant This security objective is handled in the jTOP [ST-jTOP] by the following security objectives O.PROT_PHYS_TAMPER and O.IC_SUPPORT.

O.Keys_Generation_Quality This security objective is partially handled in the jTOP [ST-jTOP] by the security objective O.KEY-MNGT. This Security Target contributes in covering this objective with the security requirement FCS_CKM.1/ Key generation RSA which specify the algorithms and key sizes for key generation.

O.Electronic_Signature_Robustness This security objective is handled in the jTOP [ST-jTOP] by the security objective O.CIPHER which ensure that the cryptographic operation offered by the platform resist to attack that are state of the art.

This Security Target also contribute to cover this objective with FCS_COP.1/ Signature creation RSA that specify the used cryptographic algorithms, that are part of the platform supported algorithms.

Those requirements ensure that the TOE provides means to the signatory to creat robust electronic signature.

O.SP_Key_Secrecy This security objective is handled in the jTOP [ST-jTOP] by the security objective O.PROT-INF-LEAK and O.KEY-MNGT that protect the secret keys stored on the platform.

O.Admin_Key_Secrecy This security objective is handled in the jTOP [ST-jTOP] by the security objective O.PROT-INF-LEAK and O.KEY-MNGT that protect the secret keys stored on the platform.

O.PIN_Code_Secrecy This security objective is handled by:

- jTOP [ST-jTOP] security objectives O.PROT-INF-LEAK, O.IDENTIFICATION, O.INFO-CONFIDENTIALITY, O.PIN-MNGT that protect the PIN stored by the platform
- requirements FCS_COP.1/ PIN and DTBS decryption, FTP_ITC.1/ DTBS and PIN code import, FDP_UIT.1/ DTBS and PIN code that protect the Signatory PIN code during its transmission
- requirement FDP_RIP.1/ Signatory PIN that prevent residual information on the Signatory PIN code after comparison with the Reference PIN code

- o requirement FIA_AFL.1/ Signatory authentication failure that limit brute force attacks on the PIN code with a maximal number of unsuccessful PIN tries.

O.Private_Key_Secrecy This security objective is handled in the jTOP [ST-jTOP] by the security objective O.PROT-INF-LEAK, O.IDENTIFICATION and O.KEY-MNGT.

This Security Target also contribute to cover the objective O.Private_Key_Secrecy with the requirements:

- o FDP_ACC.1/ Keys generation, FDP_ACF.1/ Keys generation, FMT_MSA.1/ Administrator and FMT_SMR.1/ User's role which restrict the key generation function to the Administrator
- o FCS_CKM.4/ Key destruction that limit residual information on the private key after it is destroyed.

Those requirements guarantee the protection of the private key.

O.Public_Key_Authenticity The Security Objective O.Public_Key_Authenticity is covered by the following SFRs:

- o FCS_COP.1/ Public key export MAC generation that specifies a robust MAC algorithm to protect the public key in authenticity
- o FDP_IFC.1/ Public key export and FDP_IFF.1/ Public key export, FDP_ETC.1/ Public key export, FDP_UIT.1/ Public key export and FMT_MSA.3/ Public key export that require the protection in integrity of the public key, thjrough a MAC, during its transmission outside the TOE

Those requirements ensure the authenticity of the public key exported from the TOE.

O.Data_To_Be_Signed_Integrity The Security Objective O.Data_To_Be_Signed_Integrity is covered by the following SFRs:

- o FTP_ITC.1/ DTBS and PIN code import and FDP_UIT.1/ DTBS and PIN code that require the transmission of the DTBS protected in integrity
- o FCS_COP.1/ PIN and DTBS decryption that specifies a cryptographic algorithm to protect the DTBS in integrity
- o FDP_ACC.1/ Signature creation and FDP_ACF.1/ Signature creation that require the verification of the integrity of the DTBS before signature creation

Those requirements ensure the integrity of the DTBS sent to the TOE.

O.Key_Destruction In the case of the deletion of the applet, this security objective is handled in the jTOP [ST-jTOP] by the security objective O.KEY-MNGT.

In the case of the replacement of an existing key pair, this security objective is covered by the SFR FCS_CKM.4/ Key destruction

O.Administrator_Authentication This security objective is handled in the jTOP [ST-jTOP] by the security objective O.INFO_ORIGIN that authenticates the Card Administrator.

This Security Target also contributes to cover this objective with the requirements:

- o FDP_ACC.1/ Keys generation and FDP_ACF.1/ Keys generation that define access control for the Administrator to the keys generation function
- o FIA_UAU.1/ User authentication, FIA_UID.1/ User identification, FMT_MSA.1/ Administrator, FMT_MSA.2/ Authentication and FMT_SMR.1/ User's role that define

the role of the Administrator and require authentication before any administration action

Those requirements ensure that the administrator is authenticated before enabling the generation of public/private pair of keys or public key export.

O.Signatory_Authentication This security objective is covered by the following SFRs:

- FDP_ACC.1/ Signature creation and FDP_ACF.1/ Signature creation that define access control for the Signatory to the signature creation function.
- FMT_MSA.1/ Signatory, FMT_MSA.2/ Authentication and FMT_MSA.3/ Signature creation, FMT_SMR.1/ User's role, FIA_UAU.1/ User authentication, FIA_UID.1/ User identification, that define the role of the Signatory and require authentication before signature creation.
- FDP_RIP.1/ Signatory PIN and FIA_AFL.1/ Signatory authentication failure that provide protection against brute force attacks on the PIN code and cryptographic extraction of residual information on the Signatory PIN code.

Those requirements ensure that the signatory is authenticated before signing the data to be signed.

8.2.1.2 Security objectives for the environment

OE.PIN_Entry OE.PIN_Entry is provided by FTP_ITC.1/ SP DTBS and PIN code import and FDP_UIT.1/ SP DTBS and PIN code which protect the Signatory PIN code during its transmission to the TOE.

OE.Public_Key_Authenticity OE.Public_Key_Authenticity is provided by FDP_UIT.1/ Admin Public key export and FTP_ITC.1/ Admin Public key export which ensure authenticity verification of the exported public key.

OE.Data_Intended_To_Be_Signed OE.Data_Intended_To_Be_Signed is provided by FDP_UIT.1/ SP DTBS and PIN code and FTP_ITC.1/ SP DTBS and PIN code import which assures the integrity of the DTBS sent to the TOE.

8.2.2 Rationale tables of security objectives and security requirements

Security objectives	Functional requirements for the TOE	Rationale
O.Design		
O.Tamper_Detection		
O.Tamper_Resistant		
O.Keys_Generation_Quality	FCS_CKM.1/ Key generation RSA	Section 5.2.1
O.Electronic_Signature_Robustness	FCS_COP.1/ Signature creation RSA	Section 5.2.1
O.SP_Key_Secrecy		
O.Admin_Key_Secrecy		

Security objectives	Functional requirements for the TOE	Rationale
O.PIN_Code_Secrecy	FCS_COP.1/ PIN and DTBS decryption, FTP_ITC.1/ DTBS and PIN code import, FDP_UIT.1/ DTBS and PIN code, FDP_RIP.1/ Signatory PIN, FIA_AFL.1/ Signatory authentication failure	Section 5.2.1
O.Private_Key_Secrecy	FDP_ACC.1/ Keys generation, FMT_MSA.1/ Administrator, FMT_SMR.1/ User's role, FCS_CKM.4/ Key destruction, FDP_ACF.1/ Keys generation	Section 5.2.1
O.Public_Key_Authenticity	FCS_COP.1/ Public key export MAC generation, FDP_ETC.1/ Public key export, FDP_IFC.1/ Public key export, FMT_MSA.3/ Public key export, FDP_IFF.1/ Public key export, FDP_UIT.1/ Public key export	Section 5.2.1
O.Data_To_Be_Signed_Integrity	FCS_COP.1/ PIN and DTBS decryption, FDP_UIT.1/ DTBS and PIN code, FDP_ACC.1/ Signature creation, FDP_ACF.1/ Signature creation, FTP_ITC.1/ DTBS and PIN code import	Section 5.2.1
O.Key_Destruction	FCS_CKM.4/ Key destruction	Section 5.2.1
O.Administrator_Authentication	FMT_MSA.1/ Administrator, FDP_ACC.1/ Keys generation, FDP_ACF.1/ Keys generation, FMT_MSA.2/ Authentication, FMT_SMR.1/ User's role, FIA_UAU.1/ User authentication, FIA_UID.1/ User identification	Section 5.2.1
O.Signatory_Authentication	FMT_MSA.3/ Signature creation, FDP_ACC.1/ Signature creation, FDP_ACF.1/ Signature creation, FDP_RIP.1/ Signatory PIN, FIA_AFL.1/ Signatory authentication failure, FMT_MSA.1/ Signatory, FMT_MSA.2/ Authentication, FMT_SMR.1/ User's role, FIA_UAU.1/ User authentication, FIA_UID.1/ User identification	Section 5.2.1

Table 7 Security objectives towards functional requirements for the TOE, rationale

Functional requirements for the TOE	Security objectives	Rationale

Functional requirements for the TOE	Security objectives	Rationale
FCS_COP.1/ Public key export MAC generation	O.Public_Key_Authenticity	
FCS_COP.1/ PIN and DTBS decryption	O.PIN_Code_Secrecy, O.Data_To_Be_Signed_Integrity	
FCS_COP.1/ Signature creation RSA	O.Electronic_Signature_Robustness	
FCS_CKM.1/ Key generation RSA	O.Keys_Generation_Quality	
FCS_CKM.4/ Key destruction	O.Private_Key_Secrecy, O.Key_Destruction	
FDP_IFC.1/ Public key export	O.Public_Key_Authenticity	
FDP_IFF.1/ Public key export	O.Public_Key_Authenticity	
FDP_ETC.1/ Public key export	O.Public_Key_Authenticity	
FDP_UIT.1/ Public key export	O.Public_Key_Authenticity	
FDP_ACC.1/ Keys generation	O.Private_Key_Secrecy, O.Administrator_Authentication	
FDP_ACF.1/ Keys generation	O.Private_Key_Secrecy, O.Administrator_Authentication	
FDP_ACC.1/ Signature creation	O.Data_To_Be_Signed_Integrity, O.Signatory_Authentication	
FDP_ACF.1/ Signature creation	O.Data_To_Be_Signed_Integrity, O.Signatory_Authentication	
FDP_UIT.1/ DTBS and PIN code	O.PIN_Code_Secrecy, O.Data_To_Be_Signed_Integrity	
FDP_RIP.1/ Signatory PIN	O.PIN_Code_Secrecy, O.Signatory_Authentication	
FIA_UAU.1/ User authentication	O.Administrator_Authentication, O.Signatory_Authentication	
FIA_UID.1/ User identification	O.Administrator_Authentication, O.Signatory_Authentication	
FIA_AFL.1/ Signatory authentication failure	O.PIN_Code_Secrecy, O.Signatory_Authentication	
FMT_MSA.1/ Administrator	O.Private_Key_Secrecy, O.Administrator_Authentication	
FMT_MSA.1/ Signatory	O.Signatory_Authentication	

Functional requirements for the TOE	Security objectives	Rationale
FMT_MSA.2/ Authentication	O.Administrator_Authentication, O.Signatory_Authentication	
FMT_MSA.3/ Signature creation	O.Signatory_Authentication	
FMT_MSA.3/ Public key export	O.Public_Key_Authenticity	
FMT_SMR.1/ User's role	O.Private_Key_Secrecy, O.Administrator_Authentication, O.Signatory_Authentication	
FTP_ITC.1/ DTBS and PIN code import	O.PIN_Code_Secrecy, O.Data_To_Be_Signed_Integrity	

Table 8 Functional requirements towards security objectives for the TOE, rationale

Security objectives	Assurance requirements for the TOE	Rationale
O.Design		
O.Tamper_Detection		
O.Tamper_Resistant		
O.Keys_Generation_Quality		
O.Electronic_Signature_Robustness		
O.SP_Key_Secrecy		
O.Admin_Key_Secrecy		
O.PIN_Code_Secrecy		
O.Private_Key_Secrecy		
O.Public_Key_Authenticity		
O.Data_To_Be_Signed_Integrity		
O.Key_Destruction		
O.Administrator_Authentication		
O.Signatory_Authentication		

Table 9 Security objectives towards assurance requirements for the TOE, rationale

Assurance requirements for the TOE	Security objectives	Rationale
ADV_FSP.2		
ADV_IMP.2		
ADV_HLD.2		
ADV_LLD.1		

Assurance requirements for the TOE	Security objectives	Rationale
ADV_RCR.1		
ADV_SPM.1		
AGD_ADM.1		
AGD_USR.1		
ATE_COV.2		
ATE_DPT.1		
ATE_FUN.1		
ATE_IND.2		
AVA_MSU.2		
AVA_SOF.1		
AVA_VLA.4		
ACM_AUT.1		
ACM_CAP.4		
ACM_SCP.2		
ADO_DEL.2		
ADO_IGS.1		
ALC_DVS.1		
ALC_LCD.1		
ALC_TAT.1		

Table 10 Assurance requirements towards security objectives for the TOE, rationale

Security objectives	Security requirements for the environment	Rationale
OE.PIN_Entry	FDP_UIT.1/ SP DTBS and PIN code, FTP_ITC.1/ SP DTBS and PIN code import	Section 5.2.1
OE.Secrets		
OE.Public_Key_Authenticity	FDP_UIT.1/ Admin Public key export	Section 5.2.1
OE.Data_Intended_To_Be_Signed	FDP_UIT.1/ SP DTBS and PIN code, FTP_ITC.1/ SP DTBS and PIN code import	Section 5.2.1

Table 11 Security objectives towards requirements for the environment rationale

Security requirements for the environment	Security objectives	Rationale

Security requirements for the environment	Security objectives	Rationale
FDP_UIT.1/ SP DTBS and PIN code	OE.PIN_Entry, OE.Data_Intended_To_Be_Signed	
FDP_UIT.1/ Admin Public key export	OE.Public_Key_Authenticity	
FTP_ITC.1/ SP DTBS and PIN code import	OE.PIN_Entry, OE.Data_Intended_To_Be_Signed	

Table 12 Requirements for the environment towards security objectives rationale

8.2.3 *EAL rationale*

The jTOP is independently evaluated and certified to the evaluation assurance level EAL 5+. The signature application is compositely evaluated, with the jTOP platform, to the evaluation assurance level EAL4+ (EAL4 augmented with AVA_VLA.4 and ADV_IMP.2).

The composite evaluation aims to certify the composite TOE to the evaluation assurance level EAL 4+.

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on sound industrial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources.

8.2.4 *EAL augmentations rationale*

8.2.4.1 AVA_VLA.4 Highly resistant

The selection of the component AVA_VLA.4 provides sufficient robustness to counter an attacker with high attack potential without the support of a protecting environment. This mainly concerns those attacks where the goal is to create a fake electronic signature.

8.2.4.2 ADV_IMP.2 Implementation of the TSF

The selection of component ADV_IMP.2 provides a higher assurance for the implementation of the signature application, especially for the absence of unintended functionality or unexpected interactions between TSP enforcing and non-TSP enforcing portions of the implementation.

8.2.5 *Security functional requirements dependencies*

Requirements	CC Dependencies	Satisfied Dependencies
FDP_UIT.1/ SP DTBS and PIN code	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FTP_ITC.1/ SP DTBS and PIN code import, FDP_ACC.1/ Signature creation
FDP_UIT.1/ Admin Public key export	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/ Public key export

Requirements	CC Dependencies	Satisfied Dependencies
FTP_ITC.1/ SP DTBS and PIN code import	No dependencies	
FCS_COP.1/ Public key export MAC generation	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) and (FMT_MSA.2)	FMT_MSA.2/ Authentication
FCS_COP.1/ PIN and DTBS decryption	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) and (FMT_MSA.2)	FMT_MSA.2/ Authentication
FCS_COP.1/ Signature creation RSA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) and (FMT_MSA.2)	FCS_CKM.1/ Key generation RSA, FCS_CKM.4/ Key destruction, FMT_MSA.2/ Authentication
FCS_CKM.1/ Key generation RSA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4) and (FMT_MSA.2)	FCS_COP.1/ Signature creation RSA, FCS_CKM.4/ Key destruction, FMT_MSA.2/ Authentication
FCS_CKM.4/ Key destruction	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FMT_MSA.2)	FCS_CKM.1/ Key generation RSA, FMT_MSA.2/ Authentication
FDP_IFC.1/ Public key export	(FDP_IFF.1)	FDP_IFF.1/ Public key export
FDP_IFF.1/ Public key export	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/ Public key export, FMT_MSA.3/ Public key export
FDP_ETC.1/ Public key export	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/ Public key export
FDP_UIT.1/ Public key export	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/ Public key export
FDP_ACC.1/ Keys generation	(FDP_ACF.1)	FDP_ACF.1/ Keys generation
FDP_ACF.1/ Keys generation	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ Keys generation
FDP_ACC.1/ Signature creation	(FDP_ACF.1)	FDP_ACF.1/ Signature creation
FDP_ACF.1/ Signature creation	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ Signature creation
FDP_UIT.1/ DTBS and PIN code	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/ Signature creation, FTP_ITC.1/ DTBS and PIN code import
FDP_RIP.1/ Signatory PIN	No dependencies	

Requirements	CC Dependencies	Satisfied Dependencies
FIA_UAU.1/ User authentication	(FIA_UID.1)	FIA_UID.1/ User identification
FIA_UID.1/ User identification	No dependencies	
FIA_AFL.1/ Signatory authentication failure	(FIA_UAU.1)	FIA_UAU.1/ User authentication
FMT_MSA.1/ Administrator	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ Keys generation, FMT_SMR.1/ User's role
FMT_MSA.1/ Signatory	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ Signature creation, FMT_SMR.1/ User's role
FMT_MSA.2/ Authentication	(ADV_SPM.1) and (FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.1/ Keys generation, FDP_ACC.1/ Signature creation, FMT_MSA.1/ Administrator, FMT_MSA.1/ Signatory, FMT_SMR.1/ User's role, ADV_SPM.1
FMT_MSA.3/ Signature creation	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/ Signatory, FMT_SMR.1/ User's role
FMT_MSA.3/ Public key export	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/ Administrator, FMT_MSA.1/ Signatory, FMT_SMR.1/ User's role
FMT_SMR.1/ User's role	(FIA_UID.1)	FIA_UID.1/ User identification
FTP_ITC.1/ DTBS and PIN code import	No dependencies	

Table 13 Functional requirements dependencies

8.2.5.1 Rationale for the exclusion of dependencies

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/ Admin Public key export is unsupported. The use of the MAC function to protect channel data (the public key) from modification or disclosure does not require the use of a trusted path or a trusted channel and the assured idenfication of the end points ot the communication channel.

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/ Public key export MAC generation is unsupported. The TOE does not provide any specific service for creating the Admin key value.

The dependency FCS_CKM.4 of FCS_COP.1/ Public key export MAC generation is unsupported. The TOE part 2 does not provide any specific service for destruction of the cryptographic Admin key value. The method used to destruct it is the responsibility of the jTOP platform.

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/ PIN and DTBS decryption is unsupported. The TOE does not provide any specific service for creating the SP key value.

The dependency FCS_CKM.4 of FCS_COP.1/ PIN and DTBS decryption is unsupported. The TOE part 2 does not provide any specific service for the destruction of SP key value. The method used to destruct it is the responsibility of the jTOP platform.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/ Public key export is unsupported. The use of the MAC function to protect channel data (the public key) from modification or disclosure does not require the use of a trusted path or a trusted channel and the assured idenfication of the end points ot the communication channel.

The dependency FMT_MSA.3 of FDP_ACF.1/ Keys generation is unsupported. The TOE 2 does not provide any specific service to specify alternative values for security attributes. This requirement is handled by the jTOP platform.

The dependency FMT_MSA.3 of FDP_ACF.1/ Signature creation is unsupported. The TOE 2 does not provide any specific service to specify alternative values for security attributes. This requirement is handled by the jTOP platform.

The dependency FMT_SMF.1 of FMT_MSA.1/ Administrator is unsupported. The Signature Application does not support management security functions.

The dependency FMT_SMF.1 of FMT_MSA.1/ Signatory is unsupported. The Signature Application does not support management security functions.

8.2.6 Security assurance requirements dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_FSP.2	(ADV_RCR.1)	ADV_RCR.1

Requirements	CC Dependencies	Satisfied Dependencies
ADV_IMP.2	(ADV_LLD.1) and (ADV_RCR.1) and (ALC_TAT.1)	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1
ADV_HLD.2	(ADV_FSP.1) and (ADV_RCR.1)	ADV_FSP.2, ADV_RCR.1
ADV_LLD.1	(ADV_HLD.2) and (ADV_RCR.1)	ADV_HLD.2, ADV_RCR.1
ADV_RCR.1	No dependencies	
ADV_SPM.1	(ADV_FSP.1)	ADV_FSP.2
AGD_ADM.1	(ADV_FSP.1)	ADV_FSP.2
AGD_USR.1	(ADV_FSP.1)	ADV_FSP.2
ATE_COV.2	(ADV_FSP.1) and (ATE_FUN.1)	ADV_FSP.2, ATE_FUN.1
ATE_DPT.1	(ADV_HLD.1) and (ATE_FUN.1)	ADV_HLD.2, ATE_FUN.1
ATE_FUN.1	No dependencies	
ATE_IND.2	(ADV_FSP.1) and (AGD_ADM.1) and (AGD_USR.1) and (ATE_FUN.1)	ADV_FSP.2, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.2	(ADO_IGS.1) and (ADV_FSP.1) and (AGD_ADM.1) and (AGD_USR.1)	ADV_FSP.2, AGD_ADM.1, AGD_USR.1, ADO_IGS.1
AVA_SOF.1	(ADV_FSP.1) and (ADV_HLD.1)	ADV_FSP.2, ADV_HLD.2
AVA_VLA.4	(ADV_FSP.1) and (ADV_HLD.2) and (ADV_IMP.1) and (ADV_LLD.1) and (AGD_ADM.1) and (AGD_USR.1)	ADV_FSP.2, ADV_IMP.2, ADV_HLD.2, ADV_LLD.1, AGD_ADM.1, AGD_USR.1
ACM_AUT.1	(ACM_CAP.3)	ACM_CAP.4
ACM_CAP.4	(ALC_DVS.1)	ALC_DVS.1
ACM_SCP.2	(ACM_CAP.3)	ACM_CAP.4
ADO_DEL.2	(ACM_CAP.3)	ACM_CAP.4
ADO_IGS.1	(AGD_ADM.1)	AGD_ADM.1
ALC_DVS.1	No dependencies	
ALC_LCD.1	No dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.2

Table 14 Assurance requirements dependencies

8.2.7 Rationale for the strength of functions

This maximum SOF has been chosen, because this security target is augmented with the AVA_VLA.4 assurance requirements, which requires resisting to attacks of high attack potential.

8.3 TOE summary specification rationale

8.3.1 TOE security functions rationale

8.3.1.1 TOE security functional requirements

Cryptographic support

FCS_COP.1/ Public key export MAC generation

- Public Key Export: This TSF enforces the authentication of the exported public key. This is accomplished by a MAC generated from the admin key appended to the request response and sent back to the administrator.
- Cryptographic operations: This TSF ensures the generation of the MAC with the required algorithm.

FCS_COP.1/ PIN and DTBS decryption

- Signatory and DTBS authentication: This TSF authenticates the signatory before giving him the possibility to create electronic signature.
- Cryptographic operations: This TSF ensures the decryption of the PIN and the DTBS with the required algorithms.

FCS_COP.1/ Signature creation RSA

- Cryptographic operations: This TSF ensures the signature creation with the required algorithm.

FCS_CKM.1/ Key generation RSA

- Key generation: In case of the generation of key pair, this TSF enforces the expected length of the key.

FCS_CKM.4/ Key destruction

- Key generation: In case of the replacement of an existing key pair, this TSF enforces the erasure of the previously stored key pair.

User data protection

FDP_IFC.1/ Public key export

- Public Key Export: This TSF enforces the authentication of the exported public key. This is accomplished by a MAC generated from the admin key and appended to the request response which is send back to the administrator.

FDP_IFF.1/ Public key export

- Public Key Export: This TSF enforces the authentication of the exported public key. This is accomplished by a MAC generated from the admin key and appended to the request response which is send back to the administrator.

FDP_ETC.1/ Public key export

- Public Key Export: This TSF enforces the authentication of the exported public key. This is accomplished by a MAC generated from the admin key and appended to the request response. The MAC can be verified by the administrator.
- Cryptographic operations: This TSF ensures the generation of the MAC with the required algorithm.

FDP_UIT.1/ Public key export

- Public Key Export: This TSF enforces the authentication of the exported public key. This is accomplished by a MAC generated from the admin key and appended to the request response which is send back to the administrator.
- Cryptographic operations: This TSF ensures the generation of the MAC with the required algorithm.

FDP_ACC.1/ Keys generation

- Administrator authentication: this TSF controls when the Administrator generates private/public key pairs on the signature application.

FDP_ACF.1/ Keys generation

- Administrator authentication: this TSF implements the access control to the Key generation function as described in this SFR. This access control is based on the existence of a secure channel initiated by the administrator via the ISD.

FDP_ACC.1/ Signature creation

- Signatory and DTBS authenticationn: this TSF controls when the Signatory is allowed to perform signature creation with the signature application.

FDP_ACF.1/ Signature creation

- Signatory and DTBS authentication: this TSF implements the access control to the Signature creation function as described in this SFR. This access control is based on the verification of the Signatory PIN code.

FDP_UIT.1/ DTBS and PIN code

- Signatory and DTBS authentication: This TSF verifies the integrity of the DTBS and PIN code before providing access to the signature creation function.
- Cryptographic operations: This TSF ensures the integrity verification a hash verification with the required algorithm.

FDP_RIP.1/ Signatory PIN

- Signatory and DTBS authentication: This TSF processes the Signatory PIN code for PIN verification before providing access to the signature creation function.

Identification and authentication

FIA_UAU.1 / User authentication

- Administrator authentication: This TSF enforces the authentication of the Administrator through a GP secure channel via the ISD before allowing him administrative operations.
- Signatory and DTBS authentication: This TSF authenticates the signatory through PIN verification before giving him the possibility to create electronic signature.

FIA_UID.1 / User identification

- Administrator authentication: This TSF enforces the authentication of the Administrator through a GP secure channel via the ISD before allowing him administrative operations.
- Signatory and DTBS authentication: This TSF authenticates the signatory through PIN verification before giving him the possibility to create electronic signature.

FIA_AFL.1 / Signatory authentication failure

- Signatory and DTBS authentication: This TSF verifies the PIN code before providing access to the signature creation function.

Security management

FMT_MSA.1 / Administrator

- Administrator authentication: This TSF enforces the authentication of the Administrator through a GP secure channel via the ISD before allowing him administrative operations.

FMT_MSA.1 / Signatory

- Signatory and DTBS authentication: This TSF authenticates the signatory before giving him the possibility to create electronic signature.

FMT_MSA.2 / Authentication

- Administrator authentication: This TSF enforces the authentication of the Administrator through a GP secure channel via the ISD before allowing him administrative operations.
- Signatory and DTBS authentication: This TSF authenticates the signatory before giving him the possibility to create electronic signature.

FMT_MSA.3 / Signature creation

- Signatory and DTBS authentication: This TSF authenticates the signatory before giving him the possibility to create electronic signature.

FMT_MSA.3 / Public key export

- Public Key Export: This TSF provides the authentication of the exported public key through a MAC.

FMT_SMR.1/ User's role

- Administrator authentication: This TSF authenticates the Administrator through a GP secure channel via the ISD before allowing him administrative operations.
- Signatory and DTBS authentication: This TSF authenticates the Signatory before giving him the possibility to create electronic signature.

Trusted path/channels

FTP_ITC.1/ DTBS and PIN code import

- Signatory and DTBS authentication: This TSF authenticates the signatory before giving him the possibility to create electronic signature.
- Cryptographic operations: This TSF ensures the authentication through a decryption and a hash verification with the required algorithms.

8.3.1.2 Rationale table of functional requirements and security functions

Functional requirements	TOE security functions	Rationale
FCS_COP.1/ Public key export MAC generation	Public Key Export, Cryptographic operations	Section 5.3.1
FCS_COP.1/ PIN and DTBS decryption	Signatory and DTBS authentication, Cryptographic operations	Section 5.3.1
FCS_COP.1/ Signature creation RSA	Cryptographic operations	Section 5.3.1
FCS_CKM.1/ Key generation RSA	Key generation	Section 5.3.1
FCS_CKM.4/ Key destruction	Key generation	Section 5.3.1
FDP_IFC.1/ Public key export	Public Key Export	Section 5.3.1
FDP_IFF.1/ Public key export	Public Key Export	Section 5.3.1
FDP_ETC.1/ Public key export	Public Key Export, Cryptographic operations	Section 5.3.1
FDP_UIT.1/ Public key export	Public Key Export, Cryptographic operations	Section 5.3.1
FDP_ACC.1/ Keys generation	Administrator authentication	Section 5.3.1
FDP_ACF.1/ Keys generation	Administrator authentication, Key generation	Section 5.3.1
FDP_ACC.1/ Signature creation	Signatory and DTBS authentication	Section 5.3.1
FDP_ACF.1/ Signature creation	Signatory and DTBS authentication	Section 5.3.1
FDP_UIT.1/ DTBS and PIN code	Signatory and DTBS authentication, Cryptographic operations	Section 5.3.1
FDP_RIP.1/ Signatory PIN	Signatory and DTBS authentication	Section 5.3.1
FIA_UAU.1/ User authentication	Administrator authentication, Signatory and DTBS authentication	Section 5.3.1

Functional requirements	TOE security functions	Rationale
FIA_UID.1/ User identification	Administrator authentication, Signatory and DTBS authentication	Section 5.3.1
FIA_AFL.1/ Signatory authentication failure	Signatory and DTBS authentication	Section 5.3.1
FMT_MSA.1/ Administrator	Administrator authentication	Section 5.3.1
FMT_MSA.1/ Signatory	Signatory and DTBS authentication	Section 5.3.1
FMT_MSA.2/ Authentication	Signatory and DTBS authentication, Administrator authentication	Section 5.3.1
FMT_MSA.3/ Signature creation	Signatory and DTBS authentication	Section 5.3.1
FMT_MSA.3/ Public key export	Public Key Export	Section 5.3.1
FMT_SMR.1/ User's role	Signatory and DTBS authentication, Administrator authentication	Section 5.3.1
FTP_ITC.1/ DTBS and PIN code import	Signatory and DTBS authentication, Cryptographic operations	Section 5.3.1

Table 15 Functional requirements towards security functions rationale

TOE security functions	Functional requirements	Rationale
Administrator authentication	FDP_ACC.1/ Keys generation, FDP_ACF.1/ Keys generation, FIA_UAU.1/ User authentication, FIA_UID.1/ User identification, FMT_MSA.1/ Administrator, FMT_MSA.2/ Authentication, FMT_SMR.1/ User's role	
Public Key Export	FCS_COP.1/ Public key export MAC generation, FDP_IFC.1/ Public key export, FDP_IFF.1/ Public key export, FDP_ETC.1/ Public key export, FDP_UIT.1/ Public key export, FMT_MSA.3/ Public key export	
Signatory and DTBS authentication	FCS_COP.1/ PIN and DTBS decryption, FDP_ACC.1/ Signature creation, FDP_ACF.1/ Signature creation, FDP_UIT.1/ DTBS and PIN code, FDP_RIP.1/ Signatory PIN, FIA_UAU.1/ User authentication, FIA_UID.1/ User identification, FIA_AFL.1/ Signatory authentication failure, FMT_MSA.1/ Signatory, FMT_MSA.2/ Authentication, FMT_MSA.3/ Signature creation, FMT_SMR.1/ User's role, FTP_ITC.1/ DTBS and PIN code import	
Key generation	FCS_CKM.1/ Key generation RSA, FCS_CKM.4/ Key destruction, FDP_ACF.1/ Keys generation	
Cryptographic operations	FCS_COP.1/ Public key export MAC generation, FCS_COP.1/ PIN and DTBS decryption, FCS_COP.1/ Signature creation RSA, FDP_ETC.1/ Public key export, FDP_UIT.1/ Public key export, FDP_UIT.1/ DTBS and PIN code, FTP_ITC.1/ DTBS and PIN code import	

Table 16 Security functions towards functional requirements rationale

8.3.2 Assurance measures rationale

8.3.2.1 Rationale table of assurance requirements and assurance measures

Assurance requirements	Assurance measures	Rationale
ADV_FSP.2	Functional Specification	
ADV_IMP.2	Implementation	
ADV_HLD.2	High Level Design	
ADV_LLD.1	Low Level Design	
ADV_RCR.1	Refinement Correspondance	
ADV_SPM.1	Security Policy Model	
AGD_ADM.1	Administration Guide	
AGD_USR.1	User Guide	
ATE_COV.2	Test Documentation	
ATE_DPT.1	Test Documentation	
ATE_FUN.1	Test Documentation	
ATE_IND.2	Test Documentation	
AVA_MSU.2	Vulnerability Analysis	
AVA_SOF.1	Strength of Functions Analysis	
AVA_VLA.4	Vulnerability Analysis	
ACM_AUT.1	Configuration Management Plan	
ACM_CAP.4	Configuration Management Plan	
ACM_SCP.2	Configuration Management Plan	
ADO_DEL.2	Delivery and Operation	
ADO_IGS.1	Initialization Phase Specification	
ALC_DVS.1	Development Security	
ALC_LCD.1	Software Life Cycle	
ALC_TAT.1	Tools and Techniques	

Table 17 Assurance requirements towards assurance measures rationale

Assurance measures	Assurance requirements	Rationale
Configuration Management Plan	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2	
Initialization Phase Specification	ADO_IGS.1	
Delivery and Operation	ADO_DEL.2	

Assurance measures	Assurance requirements	Rationale
Administration Guide	AGD_ADM.1	
User Guide	AGD_USR.1	
Development Security	ALC_DVS.1	
Software Life Cycle	ALC_LCD.1	
Tools and Techniques	ALC_TAT.1	
Strength of Functions Analysis	AVA_SOF.1	
Vulnerability Analysis	AVA_MSU.2, AVA_VLA.4	
Security Policy Model	ADV_SPM.1	
Functional Specification	ADV_FSP.2	
High Level Design	ADV_HLD.2	
Low Level Design	ADV_LLD.1	
Implementation	ADV_IMP.2	
Refinement Correspondance	ADV_RCR.1	
Test Documentation	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2	

Table 18 Assurance measures towards assurance requirements rationale

9 Statement of compatibility

This section contains a statement of compatibility of the composite TOE with the platform security target. This statement shall stand as developer evidence of the composite evaluation activity ASE_COMP.1 defined in [CPESC]:

“The aim of this activity is to determine whether the Security Target of the composite product does not contradict the Security Target of the underlying platform.”

9.1 Separation of TSF

All the Platform-TSF is relevant to the composite security target since the composite product offers the full security functionality of the platform. No separation is necessary.

9.2 Compatibility of assurance requirements

Let Platform-SAR be the set of SAR for the platform defined in [ST-jTOP] and Composite-SAR be the set of SAR of the composite TOE.

Composite-SAR is weaker or equal than Platform-SAR. That is, for each assurance requirement in Composite-SAR there is an assurance requirement in Platform-SAR that is either the same or higher in the CC hierarchy of the assurance family.

9.3 Compatibility of security functional requirements

All the platform security functional requirements are relevant to the composite security target.

All the operations performed on the platform SFRs are appropriate for the composite TOE since the TOE includes the full platform:

- The applet-specific SFRs from the Cryptographic support class (FCS_COP and FCS_CKM) directly use the cryptographic functions provided by the platform.
- The applet-specific SFRs from the User data protection class (FDP_ACC, FDP_ACF, FDP_ETC, FDP_UIT, FDP_RIP) correspond to requirements directly implemented by the signature application for its own access control policies and data protection. They do not interfere with access control policies or the platform or data protection provided by the platform.
- The applet-specific SFRs from the Identification and authentication class (FIA_UAU, FIA_UID, FIA_AFL) correspond to requirements on the actions provided by the signature application (signature creation, key generation). These actions are not related to the actions of the platform requiring identification and authentication (card management operations).
- The applet-specific SFRs from the Security management class (FMT_MSA, FMT_SMR) correspond to requirements on security attributes handled by the signature application. They may directly reuse security attributes provided by the platform (GlobalPlatform secure channels for the authentication of the Administrator) but do not interfere with these security attributes.
- The applet-specific SFRs from the Trusted path/channel class (FTP_ITC) correspond to requirements on trusted channels handled by the signature application for applet-specific data transmission. They complete the GlobalPlatform secure channels provided by the platform for the authentication of the Administrator.

9.4 Compatibility of TOE security objectives

All the platform security objectives for the TOE are relevant to the composite security target.

The security objectives of the platform are not contradictory to those of the composite security target. The security objectives of the composite security target can be divided into security objectives corresponding to:

- the refinement of security objectives of the platform to specific data handled by the signature application (secrets keys and PIN): O.Design, O.Tamper_Detection, O.Tamper_Resistant, O.SP_Key_Secrecy, O.Admin_Key_Secrecy, O.PIN_Code_Secrecy, O.Private_Key_Secrecy, O.Key_Destruction
- cryptographic algorithms properties provided by the platform: O.Keys_Generation_Quality, O.Electronic_Signature_Robustness,
- applet-specific properties concerning access control of the signature application functions and protection of the signature application data: O.Public_Key_Authenticity, O.Data_To_Be_Signed_Integrity, O.Administrator_Authentication, O.Signatory_Authentication

9.5 Compatibility of threats

All the platform threats are relevant to the composite security target.

The relevant threats of the platform security target are not contradictory to those of the composite security target. The threats of the composite security target can be divided into threats corresponding to:

- The refinement of threats of the platform to specific data handled by the signature application (secrets keys and PIN): T.Private_Key_Disclosure, T.SP_Key_Disclosure, T.Admin_Key_Disclosure, T.PIN_Code_Disclosure, T.Physical
- cryptographic algorithms threats: T.Public_Key_Counterfeiting, T.Signed_Data_Counterfeiting, T.Signature_Repudiation, T.Private_Key_Derivation
- applet-specific data protection threats during transmission: T.Public_Key_Counterfeiting, T.Signed_Data_Counterfeiting

The threats of the composite security target are not contradictory to the relevant OSPs of the platform security target, as the OSPs from the platform security target, apart of OSP.SECRETS from [ST-jTOP], hold on phases (loading, personalization) that are not considered in the threats of composite security target. For OSP.SECRETS, the OSP relate to the disclosure of secret data and these threats are also considered in the composite security target.

9.6 Compatibility of OSP

All the platform OSPs are relevant to the composite security target.

The OSPs of the platform security target are not contradictory to those of the composite security target, as the OSPs of the composite security target (P.Secrets and P.Trustworthy_SP) refine the OSP.SECRETS from [ST-jTOP] to applet-specific data.

9.7 Compatibility of assumptions

All the platform assumptions are relevant to the composite security target.

The current composite security target does not add new assumptions over the assumptions of the platform security target. Moreover, the only assumption of [ST-jTOP] specifically applicable to the ASE applet, the A.APPLET assumption, is fulfilled as the applet does not contain native methods. Thus, the set of assumptions of the platform security target is complete and consistent for the current composite security target.

9.8 Compatibility of security objectives for the environment

The significant security objectives for the environment of the platform security target are those linked to relevant assumptions.

The significant security objectives for the environment of the platform security target are not contradictory to those of the composite security target, as the security objectives of the composite security target hold on transmission of applet-specific data (OE.PIN_Entry, OE.Public_Key_Authenticity, OE.Data_Intended_To_Be_Signed) or refine the security objectives of the platform security target OE.Secrets.

9.9 Compatibility of security functional requirements for the environment

The significant security functional requirements for the environment of the platform security target are those linked to significant security objectives for the environment.

The significant security functional requirements for the environment of the platform security target are not contradictory to those of the composite security target:

- The applet-specific SFRs from the User data protection class (FDP_ACC, FDP_ACF, FDP_ETC, FDP_UIT, FDP_RIP) correspond to requirements directly implemented by the environment of the signature application for the protection of data exchanged with the signature application. They do not interfere with data protection provided by the platform.

10 Notice

This document has been generated with TL SET version 1.8.1, CC version (including interpretations: none). The Security Editing Tool of Trusted Labs is available at www.trusted-labs.com.

Index