BELPIC V1.8 applet On MultiApp V4.1 Platform

Common Criteria / ISO 15408
Security Target – Public version
EAL5+

Table of contents

Table of figures

Table of tables

1 Reference documents

1.1 External references [ER]

[CC]	**Common Criteria references**
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2017-04-001, version 3.1 rev 5, April 2017
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2017-04-002, version 3.1 rev 5, April 2017
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2017-04-003, version 3.1 rev 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology, CCMB-2017-04-004, version 3.1 rev 5, April 2017
[CCDB]	Common Criteria mandatory technical document – Composite product evaluation for smart cards and similar devices, Version 1.5.1, May 2018
[PP]	**Protection profiles**
[PP IC]	Security IC platform protection profile, version 1.0, January 2014. Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084.
[PP-JCS-Open]	Java Card System Protection Profile – Open Configuration ANSSI-PP-2010-03-M01, Version 3.0, May 18th 2012
[CRYPT]	"Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level" Version 1.11 – October 2008 – ANSSI-see www.ssi.gouv.fr
[PP SSCD2]	Protection profiles for secure signature creation device — Part 2: Device with key Generation, BSI-CC-PP-0059-2009-MA-01, Version 2.0.1, 23/01/2012
[PP SSCD5]	Protection profiles for secure signature creation device — Part 5: Extension for device wih key generation and trusted communication with signature creation application, BSI-CC-PP-0072, Version 1.0.1, 14/11/2012
[directive]	**European Electronic Signature Directive**
[directive]	1999/93/ec of the European parliament and of the council of 13 December 1999 on a community framework for electronic signatures
[EIDAS]	Regulation (EU) no 910/2014
[Samsung]	**Samsung references**
[ST-IC]	Security Target of Samsung Secure Smart Card Controllers S3FT9MH/S3FT9MV/S3FT9MG for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software — Rev. 3.2 — 27 March 2017
[CR-IC]	Certification Report for Samsung Secure Smart Card Controllers S3FT9MH/S3FT9MV/S3FT9MG for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software ANSSI-CC-2017/24, 11 May 2017

[ISO]	**ISO references**
[ISO7816]	Identification cards – Integrated circuit(s) cards with contacts - Books 1 to 9
[JCS]	**Javacard references**
[JCRE304]	Java Card 3.0.4 Runtime Environment (JCRE) Specification, Classic Edition – September 2011 – Published by Oracle
[JCVM304]	Java Card 3.0.4 Virtual Machine (JDVM) Specification, Classic Edition-– September 2011 – Published by Oracle
[JCAPI304]	Java Card 3.0.4 Application Programming Interface (API) Specification, Classic Edition-– September 2011 – Published by Oracle
[GP]	**Global Platform references**
[GP23]	GP2.3: GPC_Specification_v2.3.pdf Global platform Card Specification October 2015
[Belpic]	**Belpic specifications**
[BELPIC-SPEC]	General Technical Specification - Belpic V1.8 Applet (Annexe 08) Ref: General_Technical_Specification_Belpic_Applet_v1.8h

1.2 Internal references [IR]

[CR-PLTF]	Platforme ouverte Java card MultiApp V4.1 en configuration ouverte masque sur composant S3FT9MH – Certification Report Ref: ANSSI-CC-2018/32
[ST-PLTF]	MultiApp V4.1 Javacard Platform – Security Target Ref: D1417544 version: 1.12p
[AGD]	**Belpic V1.8 applet on MultiApp V4.1 platform – Guidance documentation**
[BELPIC-AGD]	BELPIC V1.8 Applet on MultiApp V4.1 Platform - AGD Top-level Document Ref: D14468995 v1.7
[PMA_BELPIC]	Personalization Manual Applet For BELPIC V1.8 on MPH117 Ref: BelpicV1.8_D1446778_PMA v1.12
[AGD_OPE]	General Technical Specification - Belpic V1.8 Applet Ref: D1459928 v1.8h
[AGD-PLT-Ref]	MultiApp ID Operating System –Reference Manual, D1392687E Mars 28, 2018
[Applet guidance]	Guidance for secure application development on Multiapp platforms, D1390326 Rev. A01, Feb 2016
	Verification process of Gemalto non sensitive applet, D1390670 Rev. A01, Feb 2016
	Verification process of Third Party non sensitive applet, D1390671 Rev. A01, Feb 2016
	Rules for applications on Multiapp certified product, D1390963 Rev. 1.2, Nov 2017

2 Acronyms and Glossary

2.1 Acronyms

APDU	Application Protocol Data Unit
CC	Common Criteria
CGA	Certificate generation application
CSP	Certification Service Provider
DTBS	Data to be signed
DTBS/R	Data to be signed or its unique representation
EAL	Evaluation Assurance Level
HID	Human Interface Device
IC	Integrated Circuit
IT	Information Technology
OS	Operating System
PIN	Personal Identification Number
PP	Protection Profile
PUK	PIN Unblocked Key
RAD	Reference Authentication Data
SAR	Security Assurance Requirements
SCA	Signature-creation application
SCD	Signature-creation data
SCS	Signature-creation system
SDO	Signed data object
SE	Security Environment
SF	Security Function
SFP	Security Function Policy
SFR	Security functional requirements
SSCD	Secure signature-creation device
ST	Security Target
SVD	Signature-verification data
TOE	Target Of Evaluation
TSF	TOE Security Functionality
VAD	Verification authentication data

2.2 Glossary

Authentication data information used to verify the claimed identity of a user
Certificate digital signature used as electronic attestation binding signature-verification data to a person confirming the identity of that person as legitimate signer
Certificate info information associated with an SCD/SVD pair that may be stored in a secure signature creation device NOTE 1: Certificate info is either ▪ a signer's public key certificate or, ▪ one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values. NOTE 2: Certificate info may contain information to allow the user to distinguish between several certificates.
Certificate-generation application (CGA) collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate
Certification service provider (CSP) entity that issues certificates or provides other services related to electronic signatures
Certificate verification The certificate verification is the process whereby the EID card verifies the digital signature of a certificate coming from an external application and retrieves the public key and the role identifier from the certificate. If the role identifier retrieved from the certificate corresponds with one that is programmed in the EID card then the external card application will get access to the corresponding data and functions in the EID card.
Data to be signed (DTBS) all of the electronic data to be signed including a user message and signature attributes
Data to be signed or its unique representation (DTBS/R) data received by a secure signature creation device as input in a single signature-creation operation NOTE: DTBS/R is either ▪ a hash-value of the data to be signed (DTBS), or ▪ an intermediate hash-value of a first part of the DTBS complemented with a remaining part of the DTBS, or ▪ the DTBS.
External Authentication without certificate verification The external authentication is the process whereby the EID card authenticates the external application by means of a signature based on challenge/response authentication scheme. If this verification process succeeds then the external card application will get access to the authorized data and functions in the EID card.
Internal Authentication The internal authentication process is used by the external application to authenticate the BelPIC EID card.
Legitimate user user of a secure signature creation device who gains possession of it from an SSCD-provisioning service provider and who can be authenticated by the SSCD as its signatory
Mutual Authentication The mutual authentication is the process whereby the EID card authenticates the external application and visa versa by means of a signature based on challenge/response authentication scheme. If this verification process succeeds then the external card application will get access to the authorized data and functions in the EID card. In the EID card, the mutual authentication shall be composed of an internal authentication process followed by an external authentication with certificate verification process. A successful mutual authentication shall also cause the setting of a secure message channel between the external application and the EID card.

Reference authentication data (RAD) data persistently stored by the TOE to authenticate a user as authorized for a particular role by cognition or by data derived from a user's biometric characteristics
Signatory legitimate user of an SSCD associated with it in the certificate of the signature-verification data and who is authorized by the SSCD to operate the signature-creation function
Signature attributes additional information that is signed together with a user message
Signature-creation application (SCA) application complementing an SSCD with a user interface with the purpose to create an electronic signature Note: A signature creation application is software consisting of a collection of application components configured to: ▪ present the data to be signed (DTBS) for review by the signatory, ▪ obtain prior to the signature process a decision by the signatory, ▪ if the signatory indicates by specific unambiguous input or action its intent to sign send a DTBS/R to the TOE ▪ process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.
Signature-creation data (SCD) private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature
Signature-creation system (SCS) complete system that creates an electronic signature consisting of an SCA and an SSCD
Signature-verification data (SVD) public cryptographic key that can be used to verify an electronic signature
SSCD-provisioning service service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD
User entity (human user or external IT entity) outside the TOE that interacts with the TOE
User Message data determined by the signatory as the correct input for signing
Verification authentication data (VAD) data provided as input to a secure signature creation device for authentication by cognition or by data derived from a user's biometric characteristics

3 Security Target introduction

3.1 Security Target Identification

Title	BelPIC V1.8 applet on MultiApp V4.1 Platform - Security Target
Version	1.1
Origin	Gemalto
IT Security Evaluation Facility	Serma Safety & Security
IT Security Certification scheme	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
ST Reference	D1459901_P
Date of Issue	26/02/2019

3.2 TOE Identification

Developer's Name	Gemalto
Product	BelPIC V1.8
TOE Name	BelPIC V1.8 on MultiApp V4.1
Commercial Name	BelPIC V1.8 on MultiApp V4.1
TOE Version	V1.8 revision 1.0
TOE Marketing Product Reference*	M1016244
TOE Technical Product Reference*	T1037465
Product Guidance	Guidance [AGD]
TOE Hardware part	Samsung S3FT9MH security controller
Composition elements:	
Composite TOE identifier	MultiApp V4.1 Platform
Composite TOE Version	4.1

(*) Note: PDM (Product Data Management) reference system

The TOE identification is provided by a dedicated command GET CARD DATA.
Please refer to TOE documentation for more details.

The response of the GET CARD DATA is described below. In yellow the field of the TOE identification

Response fields	Length (byte)	Value	Description
Serial Number	16	Card Serial number (For Gemalto, chip manufacturer serials)	The serial number is composed of: - 2 bytes reserved for Gemalto = 0x534C - 2 bytes identifying the chip manufacturer) 0x4250 (Samsung) - 12 bytes of Card Serial number (from GetData CPLC data tag '9F 7F')
Component code	1	0x20	Chip SAMSUNG-S3FT9MH (MSA153)
OS number	1	0x5B	OS Number: MSA153 – MultiApp v4.1
OS version	1	0x01	OS version v1
Softmask number	1	0x00	None
Softmask version	1	0x00	None
Applet version	1	0x18	Applet version 1.8
Applet revision	2	0x0001	Applet revision: Minor = 0x00 | Major = 0x01 (revision 1.0)
Applet interface version	1	0x00	None
…			

3.3 TOE Overview

The BELPIC V1.8 product on MultiApp V4.1 is a smartcard addressing the Belgium Identity Card market. Built upon a javacard platform, the smartcard application software implements identification, authentication, and secure signature creation services. These services are enabled through the personalization of the BELPIC V1.8 applet on top of the MultiApp V4.1 javacard platform.

The MultiApp V4.1 BELPIC product is a "contact-only" smartcard compliant with [ISO7816], and supporting T=0 communication protocol.

For the present ST, the Target of Evaluation (TOE) is the BELPIC V1.8 applet and the underlying platform which supports its functionality. Therefore, the TOE boundaries encompass:

- **The BELPIC V1.8 application software made of the following parts:**
  The BELPIC V1.8 Applet Software based on [BELPIC-SPEC]
- **The MultiApp V4.1 Javacard Platform**
  The platform is based on [JCS] and [GP], which supports the execution of the BELPIC V1.8 applet and provides card administration services
- **The Samsung S3FT9MH Integrated Circuit**
- **The guidance documentation [AGD]**

Notes: For this smartcard product, the other associated security elements (such as holograms, security printing…) are outside this TOE scope.

4 TOE Description

4.1 TOE boundaries

As illustrated by figure 1, the Target of Evaluation (TOE) is composed of:

- The BELPIC V1.8 application: Applet and data.
- The MultiApp V4.1 javacard platform, which supports the execution of the BELPIC Applet and provides the smartcard administration services.
- The associated guidance documentation [AGD].
- The Samsung S3FT9MH Security IC. The security IC provides hardware security that otherwise cannot be provided by the TOE logical components.

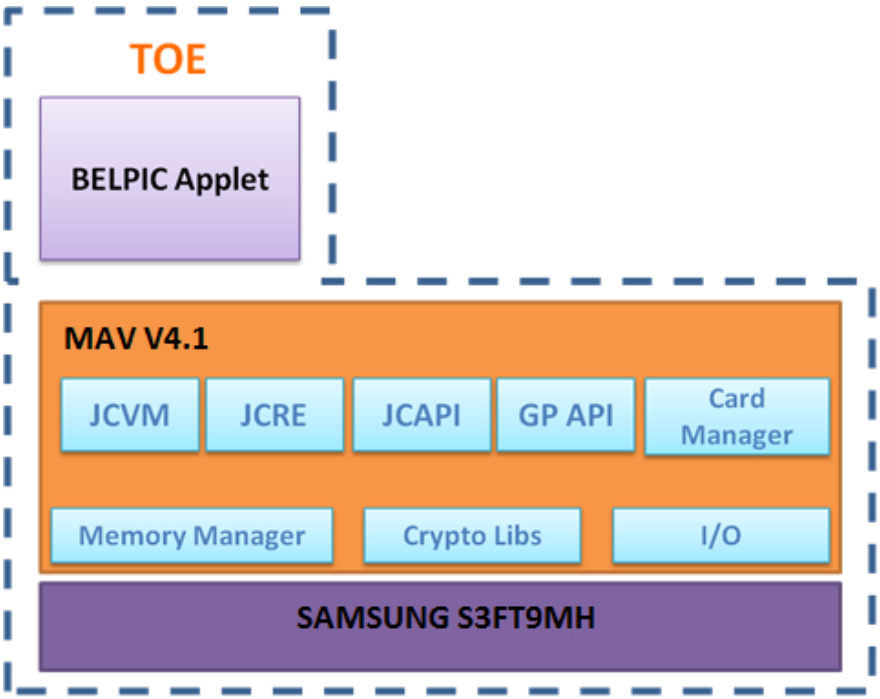

Figure 1: BELPIC TOE boundaries

The MultiApp V4.1 platform functionality (executable code) and the BELPIC V1.8 functionality are located in Flash memory. TOE data (related to the BELPIC applet or to the javacard platform) are located in Flash memory as well. The separation between these data is ensured by the javacard firewall as specified in [JCRE304].

The GDP applet (present in MAV 4.1 platform) was removed from the TOE of BELPIC V1.8 as it was not used for this product.

Other smart card product elements (such as holograms, magnetic stripes, security printing etc.) are outside the scope of this Security Target.

4.2 MultiApp V4.1 Javacard Platform description

The MultiApp V4.1 Platform is a smart card operating system developed by Gemalto [ST-MultiApp41]. It complies with two major industry standards:

- Sun's Java Card 3.0.4, which consists of the Java Card 3.0.4 Virtual Machine [JVCM304], the Java Card 3.0.4 Runtime Environment [JCRE304] and the Java Card 3.0.4 Application Programming Interface [JCAPI304].
- The Global Platform Card Specification version 2.3 [GP23].

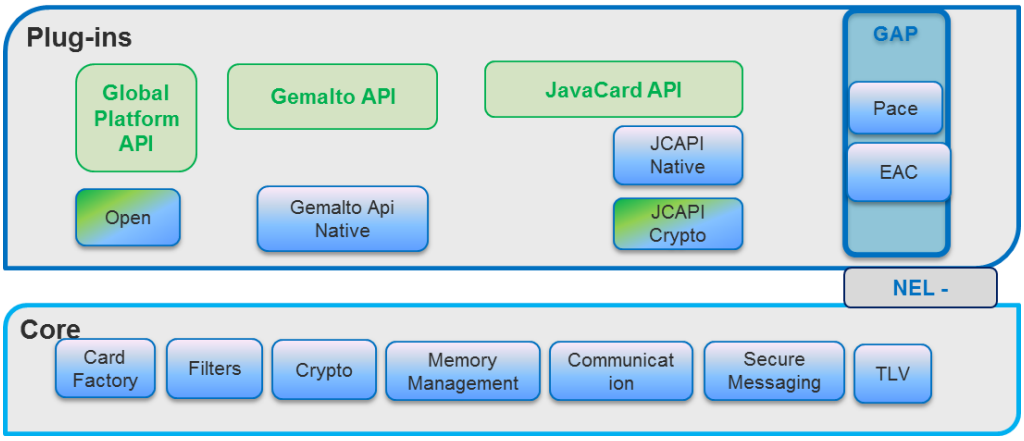

Figure 2: MultiApp V4.1 Javacard Platform Architecture

As described in figure 2, the MultiApp V4.1 Platform contains the following components:

- **The Core Layer**

  The Core layer remains unaffected as the basic smart card services (softmasks/filters, communication protocols, memory management, secure messaging) remain the same.

  It provides the basic card functionalities (memory management, I/O management and cryptographic primitives) with native interface with the underlying IC. The cryptographic features implemented in the native layer encompass the following algorithms:

  - ECDSA 256, 384, 512 and 521 bits
  - ECDH 256, 384, 512 and 521 bits
  - ECDSA Key Generation (OBKG)
  - RSA CRT 2048 bits
  - RSA Key Generation (OBKG)
  - SHA 256, 384, 512 bits
  - AES 256 bits for Secure Messaging

- **The Javacard Runtime Environment**
  It conforms to [JCRE304] and provides a secure framework for the execution of the Java Card programs and data access management (firewall).
  Among other features, multiple logical channels are supported, as well as extradition, DAP, Delegated management, SCP01, SCP02 and SCP03.
- **The Javacard Virtual Machine**
  It conforms to [JVCM304] and provides the secure interpretation of bytecodes.
- **The API**
  It includes the standard javacard API [JCAPI304] and the Gemalto proprietary API.
- **The Global Platform Card Manager**
  It conforms to [GP23] and provides card, key and applet management functions (contents and life-cycle) and security control.

4.3 Belpic V1.8 Applet description

BELPIC V1.8 is a Javacard application that provides a Secure Signature Creation Device (SSCD) as defined by a local (Belgian) regulation and the [EIDAS] European regulation.

The BELPIC applet is compliant to [BELPIC-SPEC] and provides the following services necessary for devices involved in creating qualified electronic signature:

- Key pair (SCD/SVD) generation and secure management
- SVD key export to a CGA for certification, and reception/storage of certificate information.
- Reference authentication data (RAD) initialization
- Identification and authentication of trusted users and applications (by means of PIN)
- Electronic signature creation
- Trusted channel creation

The signature key material is composed of ECC key pairs. Each key pair is composed of a private key (the signature-creation data: SCD) and the associated public key (the signature-verification data: SVD).

If in an operational state, the TOE is able to create qualified electronic signatures with the following steps:

a) Use appropriate hash functions that are suitable for electronic signatures
b) Use appropriate cryptographic signature function that employs appropriate cryptographic parameters
c) Select an SCD if multiple are present in the SSCD
d) Receive data to be signed or a unique representation thereof (DTBS/R)
e) Authenticate the signatory and determine its intent to sign,
f) Apply an appropriate cryptographic signature-creation function using the selected SCD to the DTBS/R.

The BELPIC V1.8 application is composed of three main functionalities:

- The electronic signature functionality

- The electronic identification functionality
- The trusted channel functionality

Those three functionalities are implemented through the same security environment.

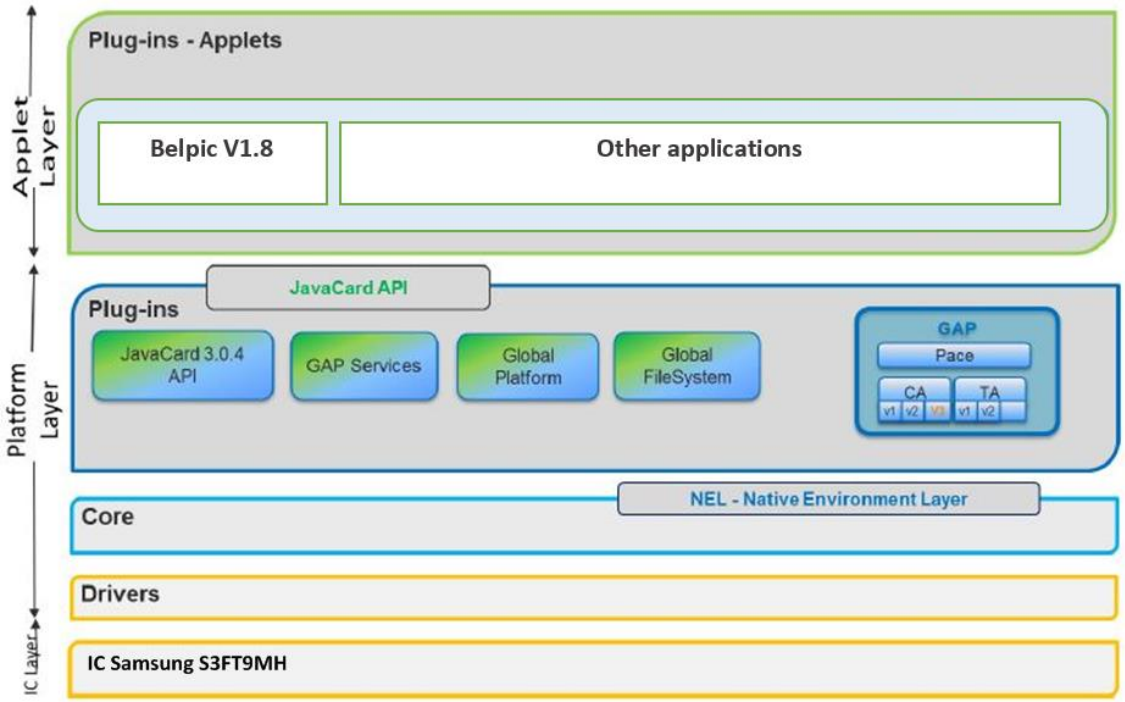

Figure 3: BELPIC Electronic Identity Card structure

The security functionalities of the TOE will be externally available to the user by means of APDU commands according to the access conditions specified by the appropriate policies considering the life cycle state, user role and security state.

4.4 Terminology

In this document the terminology of **[PP SSCD2]** and **[PP SSCD5]** is used (figure 4).

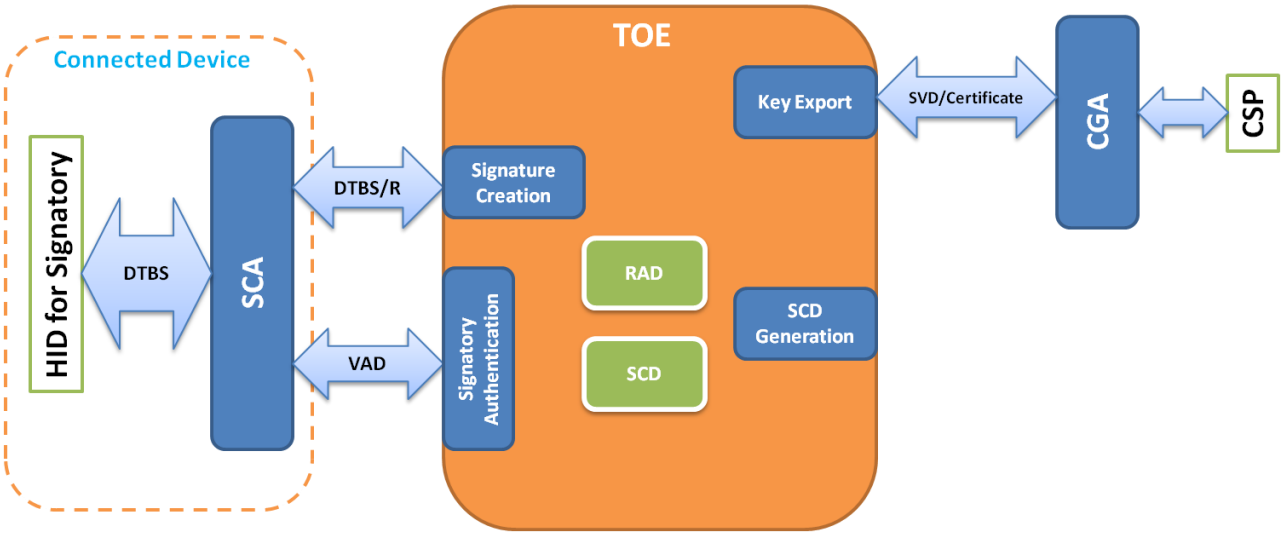

Figure 4: TOE Usage according to PP SSCD2 and PP SSCD5

The TOE is initialized by generating a pair of SCD and SVD. The SCD is protected so as to be solely used in the signature-creation process by the legitimate signatory during the validity of this SCD/SVD pair.

The TOE stores the SCD and may export the SVD. The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate service provider (CSP). The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory.

The TOE shall only be switched to an operational state if it is properly prepared for the signatory's use and sole control by:

- Generating at least one SCD/SVD pair, and
- Personalizing for the signatory by storing in the TOE:
  a) The signatory's reference authentication data (RAD)
  b) Certificate info for at least one SCD in the TOE.

To authenticate himself as the legitimate user of the TOE, the signatory submits Verification Authentication Data (VAD) in the form of a PIN. The TOE compares the VAD with Reference Authentication Data (RAD) securely stored in the card. The authentication is successful if VAD and RAD are identical.

The TOE implements all IT security functionalities, which are necessary to ensure the SCD and RAD secrecy. To prevent the unauthorized usage of the SSCD the TOE provides user authentication and access control.

The TOE is an SSCD on a smart card. A smart card terminal shall be deployed that provides the required secure environment to handle a request for signatory authorization. A signature can be obtained on a document prepared by a signature creation application component running on personal computer connected to the card terminal. The signature creation application, after presenting the document to the user and after obtaining the authorization PIN initiates the digital signature creation function of the smart card through the terminal. The TOE then returns the digital electronic signature to the signature creation application.

In accordance with [PP SSCD5], the TOE creates Trusted Channel with SCA to protect the DTBS/R. The Trusted Channel is implemented with ECDH to generate session keys that protect the communication to SCA.

4.5 Life-cycles

4.5.1 Product life-cycle

The product life cycle is composed of the 7 phases described in the following table. The table also mentions the authority involved in each phase.

BELPIC product life-cycle				
TOE	**Phase n°**	**Phase designation**	**Phase description**	**Comment**
TOE uneder construction	1	SC embedded software development	The SC embedded software developer is in charge of the specification, development and validation of the MultiApp V4.1 software (SC operating system & BELPIC applet). He also specifies the IC initialization data.	The SC embedded software developer is Gemalto.
	2	IC development	The IC developer designs the IC, develops the IC dedicated software and provides information, software or tools to the SC embedded software developer. From the IC design, the IC dedicated software; he builds the Smart Card IC database needed for the IC photomask fabrication.	The IC designer is Samsung
	3	IC manufacturing and testing	The IC manufacturer is responsible for producing the IC through three main steps: IC manufacturing, IC testing, and IC initialisation.	The IC manufacturer is Samsung
	4	IC Packaging	The IC Packager is responsible for the smartcard module manufacturing and testing.	The IC Packager is Gemalto
	5a	Pre-personalization	The Pre-personalizer loads embedded software components within the smartcard module, builds the Smartcard profile, loads the data needed for card personalization and performs tests.	The Prepersonalizer is Gemalto **TOE Delivery**
TOE operational	5b	SC Manufacturing	The SC Manufacturer embeds the smartcard module in plastic card bodies	The SC Manufacturer is Zetes
	6	Personalization	The Personalizer builds the card administration and the application profile (file creation and data loading) and performs final tests.	The Personalizer is Zetes. Loading of application data, SCD/SVD generation and SVD export for certificate are done in the phase 6.
	7	End-usage	The SC issuer is responsible for the SC product delivery to the SC end-user (cardholder), and the end of life process.	The cardholder is a customer of the SC issuer. Signature creation and SCD destruction correspond to the phase 7

Table 1: BELPIC product life-cycle

For the present evaluation (cf figure 5), the IC is manufactured at Samsung site. It is then shipped to Gemalto site where it is initialized and pre-personalized and then shipped to the Personalizer. During the shipment from Gemalto to ZETES (who is the SC Manufacturer and the Personalizer), the module is protected by a diversified key.

The TOE life cycle distinguishes stages for:

1. Development
2. Production: Storage, pre-personalization and testing
3. Preparation: Personalization and testing
4. Operational Use: Final usage

Development and production of the TOE together constitute the development phase of the TOE. The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class.

The TOE storage is not necessarily a single step in the life cycle since it can be stored in parts. The TOE delivery occurs before storage and may take place more than once if the TOE is delivered in parts.

These four stages map to the product life cycle phases as shown in figure 6.

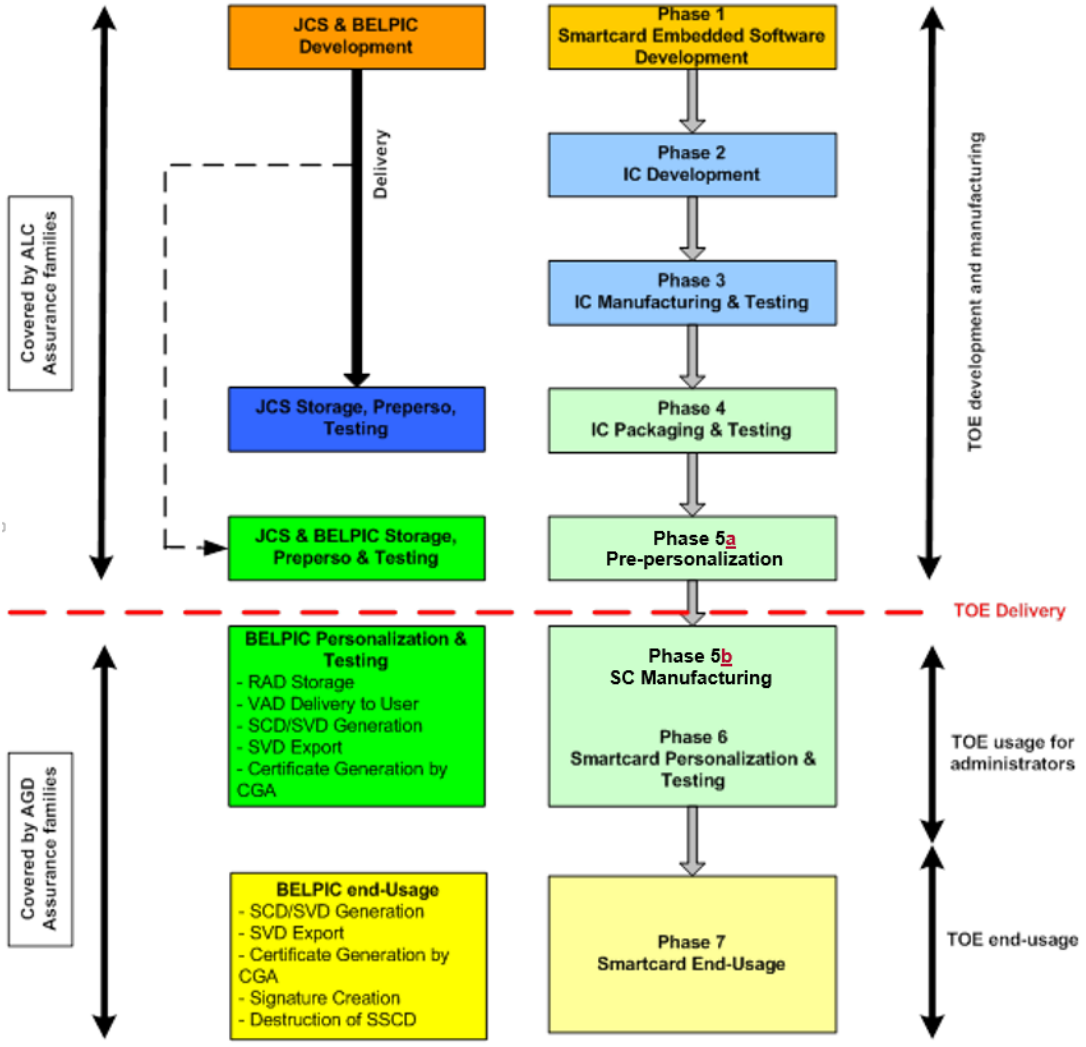

Figure 5: TOE Life Cycle within Product Life Cycle

The BELPIC & JCS development is performed during Phase 1. This includes BELPIC, JCS conception, design, implementation, testing and documentation. The development shall fulfill requirements of the final product, including conformance to Java Card Specifications, [SPEC-BELPIC], and recommendations of the SCP user guidance. The development shall occur in a controlled environment that avoids disclosure of source code, data and any critical documentation and that guarantees the integrity of these elements. The present evaluation includes the BELPIC & JCS development environment.

In Phase 3, the IC Manufacturer stores, initializes the TOE and potentially conduct tests on behalf of the TOE developer. The IC Manufacturing environment shall protect the integrity, confidentiality of the TOE and of any related material, for instance test suites. The present evaluation includes the whole IC Manufacturing environment, in particular those locations where the TOE is accessible for installation or testing. As the Security IC has already been certified against [PP IC] there is no need to perform the evaluation again.

In Phase 5a, the SC Pre-Personalizer loads the Belpic applet software, and pre-personalizes the TOE and potentially conducts tests on behalf of the TOE developer. The BELPIC applet installation is performed during phase 5a. The SC Pre-Personalization environment shall protect the integrity and confidentiality of the TOE and of any related material, for instance test suites.

(Part of) TOE storage in Phase 5a implies a TOE delivery during Phase 5a. The TOE in the form of modules are sent to the SC Manufacturing.

The SC Manufacturer then embeds the modules into plastic smasrtcard bodies during the phase 5b. The TOE delivery point is placed at the end of Phase 5a, since the entire TOE is then embedded in the Security IC.

The TOE is personalized in Phase 6: loading of the BELPIC applet data, RAD storage and VAD delivery to User. The SC Personalization environment is not included in the present evaluation. Appropriate security recommendations are provided to the SC Personalizer through the [AGD] documentation.

SCD/SVD generation, SVD export and certificate generation by the CGA may take place during both 6 and 7 phases.

Phase 7 corresponds to the TOE end-usage. Signature creation is performed during this phase. The SSCD destruction corresponds to the end of phase 7.

The operational phase (phase 7) of the TOE starts when a SCD/SVD pair is generated into the SSCD and when the signatory takes control over the TOE and makes the SCD operational. The signatory uses the TOE with a trustworthy SCA in a secured environment only.

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

The different guides accompanying the TOE and parts of the TOE are the ones specified in [AGD] section. They are delivered in form of electronic documents (*.pdf) by Gemalto's Technical representative.

4.5.2 Involved sites

The following development and manufacturing sites are involved in the development and construction of the TOE, and shall therefore be included within the scope of the present evaluation:

Life cycle phase	Involved sites
Embedded software development (Phase 1)	**Gemalto Meudon** site (development team) **Gemalto Singapore** site (development team)
IC development (Phase 2)	**Samsung** development site(s) mentioned in [CR-IC]
IC Manufacturing & Testing (Phase 3)	**Samsung** production site(s) mentioned in [CR-IC]
IC initialization, packaging & testing (Phase 4)	**Gemalto Gémenos** site **Gemalto Singapore** site
Prepersonalization & testing (Phase 5a)	**Gemalto Gémenos** site **Gemalto Singapore** site
TOE Delivery	
SC Manufacturing (Phase 5b)	**Zetes** site

4.6 TOE intended usage

The TOE is intended for electronic signatures creation and fulfills requirements specified in [PP SSCD2], [PP SSCD5] and other relevant documents.

PP SSCD2 Function	Description	TOE Conformity
SCD/SVD Key generation	1. The SCA authenticates itself to the TOE. 2. The signatory enters his PIN code. 3. The signatory requests the generation of a SCD / SVD key pair 4. The SCD / SVD are generated in the TOE. 5. The SVD is sent to the CGA. 6. The CGA generates the certificate and stores it to the TOE.	✓
Signature Creation	1. The signatory enters his PIN code. 2. The signatory sends the DTBS to the TOE. 3. The TOE computes the Signature. 4. The TOE sends the Signature to the SCA.	✓
Key Destruction	The TOE will destroy all keys.	✓

PP SSCD2 Function	Description	TOE Conformity
Initial RAD value	The initialization environment interacts with the TOE to personalize it with the initial value of the RAD.	✓
SCA use	Part of BELPIC functionality includes interaction and communication with the connected device.	✓
State change	The TOE can be switched from a non operational state to an operational state.	✓

PP SSCD5 Function	Description	TOE Conformity
Timing of authentication	1. The TOE allows self-test 2. The TOE performs user identification 3. The TOE establish secure channel between HID and TOE	✓
Data exchange integrity	1. The TOE protects user data 2. The TOE is able to determine whether modification and insertion has occurred on user data	✓
Trusted Channel – Human Interfce Device (HID)	The TOE provides a secure communication channel to HID	✓
Trusted Channel – Signature Creation Application (SCA)	The TOE provides a secure communication channel to SCA	✓

5 Conformance claims

5.1 Common Criteria conformance claims

Common criteria Version:
This ST claims to be conformant to the CC Version 3.1 revision 5, which comprise of: [CC-1] [CC-2], [CC-3] and [CEM].

Conformance to CC part 2 and 3:
- CC part 2 extended
- CC part 3 conformant

5.2 Protection profile claim

This security target claims conformance to the Common Criteria Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation [PP SSCD2] and to the Common Criteria Protection Profile for Secure Signature Creation Device – Part 5: Extension for device with key generation and trusted communication with signature creation application [PP SSCD5].

5.3 Assurance package claim

This security target is package conformant to evaluation assurance level 5 augmented (EAL5+) with AVA_VAN.5 and ALC_DVS.2.

5.4 Conformance Claim Rationale

This security target is compliant with the PP [PP SSCD2] and [PP SSCD5]. The conformance mode is the following:

Protection Profile	Conformance
[PP SSCD2]	Strict
[PP SSCD5]	Strict

A detailed justification is given in the following:

- The TOE description is based on the TOE overview of [PP SSCD2] and [PP SSCD5] and has only been added by product specific details.
- All definitions of the security problem definition in [PP SSCD2] and [PP SSCD5] have been included in the ST exactly in the same wording of the PP.
- All definitions of the security objectives in [PP SSCD2] and [PP SSCD5] have been included exactly in the same wording as the PP.

- The part of extended components definition of [PP SSCD2] and [PP SSCD5] has been included in the ST exactly in the same wording as the PP.
- All SFRs for the TOE from the [PP SSCD2] and [PP SSCD5] have been included in the ST with refinements.
- All text from introduction, TOE overview, and TOE description has been taken from the PP and has been only added by product specific details.
- The security assurance requirements (SARs) are originally taken from SARs of CC 3.1 Part 5 according to the package conformance EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5. The addition of ALC_DVS.2 exceeds the augmentation defined by the PP.
- The structure of the ST is taken from the PP [PP SSCD2] and [PP SSCD5] added by the Section 10 (TOE summary specification) and Section 8 (Extended Requirements).

5.5 Assurance Requirements compatibility

The level of assurance of the:

- TOE is EAL5 augmented with ALC DVS.2 and AVA_VAN.5
- Platform is EAL5 augmented by ALC_DVS.2 and AVA_VAN.5

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

5.6 Evaluation type

This is a composite evaluation, which relies on the MultiApp V4.1 Platform certificate and evaluation results.

MultiApp V4.1 certificate:

- Certification was done under the French ANSSI scheme
- Certification Report is decribed in [CR-PLTF]
- Security Targets [ST-PLTF] strictly conformant to Java Card System – Open Configuration Protection Profile [PP-JCS-Open]
- Common criteria version: 3.1 revision 5
- Assurance level: EAL5+ augmented by ALC_DVS.2 and AVA_VAN.5

Consequently, the composite product evaluation (i.e. the present evaluation) includes the additional composition tasks defined in the CC supporting document "Composite product evaluation for smart cards and similar devices" [CCDB].

The document [CCDB] shall be used in addition to the CC part 3 [CC] and to the CEM [CEM]. This document specifies the additional information to be provided by a developer, and the additional checks to be performed by the ITSEF (Information Technology Security Evaluation

Facility) when performing a "composite evaluation". This is the case for the current TOE which relies onthe underlying MultiApp V4.1 Platform.

6 Security Problem Definition

6.1 Assets

The assets of the TOE are those defined in [PP SSCD2], [PP SSCD5] and [PP-JCS-Open]. The present Security Target deals with the assets mentioned in [PP SSCD2] and [PP SSCD5]. The assets of [PP-JCS-Open] are studied in [ST-PLTF].

D.SCD

Signature Creation Data

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

D.SVD

Signature Verification Data

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

D.DTBS/R

Data to be signed or its unique Representation

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

6.2 Users / Subjects

6.2.1 Threat agents

S.Attacker

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

6.2.2 Miscellaneous

S.User

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

S.Admin

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

S.Signatory

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

6.3 Threats

T.SCD_Divulg

Storing, copying and releasing of the signature creation data

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

T.SCD_Derive

Derive the signature creation data

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

T.Hack_Phys

Physical attacks through the TOE interfaces

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

T.SVD_Forgery

Forgery of the signature verification data

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

T.SigF_Misuse

Misuse of the signature creation function of the TOE

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

T.DTBS_Forgery

Forgery of the DTBS/R

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

T.Sig_Forgery

Forgery of the electronic signature

An attacker forges a signed data object, maybe using an electronic signature which has been created by the TOE, and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature created by the TOE is subject

to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

6.4 Organisational Security Policies

This section defines OSPs related to the Digital Signature application as stated in [PP SSCD2] and [PP SSCD5].

P.CSP_QCert

Qualified certificate

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. the [directive], article 2, clause 9, and Annex I) for the SVD generated by the SSCD. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

P.QSign

Qualified electronic signatures

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. the [directive], article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the [directive] Annex I). The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

Application Note:

It is a non-qualified advanced electronic signature if it is based on a non-qualified certificate for the SVD.

P.Sigy_SSCD

TOE as secure signature creation device

The TOE meets the requirements for an SSCD laid down in Annex III of the [directive]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

P.Sig_Non-Repud

Non-repudiation of signatures

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

6.5 Assumptions

This section defines assumptions related to the Digital Signature application as stated in [PP SSCD2] and [PP SSCD5] and as stated in [PP-JCS-Open] for composite evaluation.

A.CGA

Trustworthy certificate generation application

The CGA protects the authenticity of the signatory's name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

A.SCA

Trustworthy signature creation application

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of data the signatory wishes to sign in a form appropriate for signing by the TOE.

A.APPLET

Applets loaded post-issuance do not contain native methods. The Java Card specification explicitly "does not include support for native methods" ([JCVM222], §3.3) outside the API.

A.VERIFICATION

All the bytecodes are verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time.

7 Security Objectives

7.1 Security Objectives for the TOE

The security objectives in this Security Target are those named and described in [PP SSCD2] and [PP SSCD5]. The security objectives stated in [PP-JCS-Open] can be found in [ST-PLTF].

OT.Lifecycle_Security

Lifecycle security

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall securely destroy the SCD on demand of the signatory.

Application Note:

The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

OT.SCD/SVD_Gen

Authorized SCD/SVD generation

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

OT.SCD_Unique

Uniqueness of the signature creation data

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

OT.SCD_SVD_Corresp

Correspondence between SVD and SCD

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD.

OT.SCD_Secrecy

Secrecy of the signature-creation data

The secrecy of the SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential.

Application Note:

The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and secure destruction.

OT.Sig_Secure

Cryptographic security of the electronic signature

The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.Sigy_SigF

Signature creation function for the legitimate signatory only

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

OT.DTBS_Integrity_TOE

DTBS/R integrity inside the TOE

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

OT.EMSEC_Design

Provide physical emanations security

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

OT.Tamper_ID

Tamper detection

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

OT.Tamper_Resistance

Tamper resistance

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

OT.TOE_TC_VAD_Imp

Trusted channel of TOE for VAD import

The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed.

Application note:

This security objective for the TOE is partly covering OE.HID_VAD from the core PP. While OE.HID_VAD in the core PP requires only the operational environment to protect VAD, this PP requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore this PP re-assigns partly the VAD protection

from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

OT.TOE_TC_DTBS_Imp

Trusted channel of TOE for DTBS import

The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE must not generate electronic signatures with the SCD for altered DTBS.

Application note:

This security objective for the TOE is partly covering OE.DTBS_Protect from the core PP. While OE.DTBS_Protect in the core PP requires only the operational environment to protect DTBS, this PP requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore this PP re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

7.2 Security Objectives for the Operational Environment

The security objectives for the environment in this Security Target are those named and described in [PP SSCD2] and [PP SSCD5]. The security objectives for the environment stated in [PP-JCS-Open] can be found in [ST-PLTF].

OE.SVD_Auth

Authenticity of the SVD

The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

OE.CGA_QCert

Generation of qualified certificates

The CGA shall generate a qualified certificate that includes (amongst others)

1. the name of the signatory controlling the TOE,
2. the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
3. the advanced signature of the CSP.

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

OE.SSCD_Prov_Service

Authentic SSCD provided by SSCD-provisioning service

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

OE.HID_VAD

Protection of the VAD

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

OE.DTBS_Intend

SCA sends data intended to be signed

The signatory shall use a trustworthy SCA that

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

Application Note:

The SCA should be able to support advanced electronic signatures. Currently, there exist three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CAdES, XAdES and PAdES. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.

OE.DTBS_Protect

SCA protects the data intended to be signed

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

OE.Signatory

Security obligation of the signatory

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

OE.HID_TC_VAD_Exp

Trusted channel of HID for VAD export

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.

Application Note:

This security objective for the TOE is partly covering OE.HID_VAD from the core PP. While OE.HID_VAD in the core PP requires only the operational environment to protect VAD, this PP requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore this PP re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

OE.SCA_TC_DTBS_Exp

Trusted channel of SCA for DTBS export

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

Application Note:

This security objective for the TOE is partly covering OE.DTBS_Protect from the core PP. While OE.DTBS_Protect in the core PP requires only the operational environment to protect DTBS, this PP requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore this PP re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

7.3 Security Objectives from the Platform

OE.VERIFICATION
All the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. See #.VERIFICATION for details.

Additionally the applet shall follow all recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform.
Application Note:
Constraints to maintain the isolation property of the platform are provided by the platform developer in application development guidance. The constraints apply to all application code loaded in the platform.

OE.APPLET
No applet loaded post-issuance shall contain native methods.

OE.CODE-EVIDENCE
For application code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that loaded application has not been changed since the code verifications required in OE.VERIFICATION.
For application code loaded post-issuance and verified off-card according to the requirements of OE.VERIFICATION, the verification authority shall provide digital evidence to the TOE that the application code has not been modified after the code verification and that he is the actor who performed code verification.

Application Note:
For application code loaded post-issuance and verified off-card, the integrity and authenticity evidence can be achieved by electronic signature of the application code, after code verification, by the actor who performed verification.

7.4 Security Objectives Rationale

The following table shows how the security objectives for the TOE and the security objectives for the environment cover the threats, organizational security policies and assumptions. Take note that this PP describes the same threats, organisational security policies and assumptions as the core PP, with the following two exceptions:

OE.HID_VAD from the core PP has been split into the objectives OE.HID_TC_VAD_Exp and OT.TOE_TC_VAD_Imp in this PP, i.e. a part of a security objective for the environment (namely OE.HID_VAD from the core PP) will be met by the TOE itself, which is allowed according to CC.

OE.DTBS_Protect from the core PP has been split into OE.SCA_TC_DTBS_Exp and OT.TOE_TC_DTBS_Imp in this PP, i.e. a part of a security objective for the environment (namely OE.DTBS_Protect from the core PP) will be met by the TOE itself, which is allowed according to CC.

Threats - Assumptions / Policies / Security Objectives	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.DTBS_Intend	OE.Signatory	OE.HID_TC_VAD_Exp	OE.SCA_TC_DTBS_Exp	OE.VERIFICATION	OE.APPLET	OE.CODE-EVIDENCE
T.SCD_Divulg					X																		
T.SCD_Derive		X				X																	
T.Hack_Phys					X				X	X	X												
T.SVD_Forgery				X											X								
T.SigF_Misuse	X						X	X				X	X				X	X	X	X			
T.DTBS_Forgery								X					X				X			X			
T.Sig_Forgery			X			X								X									
P.CSP_QCert	X			X										X									
P.QSign						X	X							X			X						
P.Sigy_SSCD	X	X	X		X	X	X	X	X		X					X							
P.Sig_Non-Repud	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
A.CGA														X	X								
A.SCA																	X						
A.APPLET																						X	
A.VERIFICATION																					X		X

Table 2: Threats, Assumptions, and Policies vs. Security objectives

7.4.1 Threats

T.SCD_Divulg addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in recital (18) of the [directive]. This threat is countered by **OT.SCD_Secrecy**, which assures the secrecy of the SCD used for signature creation.

T.SCD_Derive deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. **OT.SCD/SVD_Auth_Gen** counters this threat by implementing cryptographically secure generation of the SCD/SVD pair. **OT.Sig_Secure** ensures cryptographically secure electronic signatures.

T.Hack_Phys deals with physical attacks exploiting physical vulnerabilities of the TOE. **OT.SCD_Secrecy** preserves the secrecy of the SCD. **OT.EMSEC_Design** counters physical attacks through the TOE interfaces and observation of TOE emanations. **OT.Tamper_ID** and **OT.Tamper_Resistance** counter the threat **T.Hack_Phys** by detecting and by resisting tampering attacks.

T.SVD_Forgery deals with the forgery of the SVD exported by the TOE to the CGA for certificate generation. **T.SVD_Forge**ry is addressed by **OT.SCD_SVD_Corresp**, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and **OE.SVD_Auth** that ensures the integrity of the SVD exported by the TOE to the CGA.

T.SigF_Misuse addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create an electronic signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of Annex III. **OT.Lifecycle_Security** (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. **OT.Sigy_SigF** (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. **OE.DTBS_Intend** (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign. The combination of **OT.TOE_TC_DTBS_Imp** (Trusted channel of TOE for DTBS) and **OE.SCA_TC_DTBS_Exp** (Trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission form the SCA to the TOE. **OT.DTBS_Integrity_TOE** (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, **OE.HID_TC_VAD_Exp** (Trusted channel of HID for VAD) requires the HID to protect the confidentiality and the integrity of the VAD as needed by the authentication method employed. The HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to **OE.HID_TC_VAD_Exp** (Trusted channel of HID for VAD) and **OT.TOE_TC_VAD_Imp** (Trusted channel of TOE for VAD). **OE.Signatory** (Security obligation of the signatory) ensures that the signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD.

OE.Signatory (Security obligation of the signatory) ensures also that the signatory keeps their VAD confidential.

T.DTBS_Forgery addresses the threat arising from modifications of the DTBS/R sent to the TOE for signing which than does not correspond to the DTBS/R corresponding to the DTBS the signatory intends to sign. The threat **T.DTBS_Forgery** is addressed by the security objectives **OT.TOE_TC_DTBS_Imp** (Trusted channel of TOE for DTBS) and **OE.SCA_TC_DTBS_Exp** (Trusted channel of SCA for DTBS), which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE. The TOE counters internally this threat by the means of **OT.DTBS_Integrity_TOE** (DTBS/R integrity inside the TOE) ensuring the integrity of the DTBS/R inside the TOE. The TOE IT environment also addresses **T.DTBS_Forgery** by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE.

T.Sig_Forgery deals with non-detectable forgery of the electronic signature. **OT.Sig_Secure**, **OT.SCD_Unique** and **OE.CGA_QCert** address this threat in general. **OT.Sig_Secure** (Cryptographic security of the electronic signature) ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. **OT.SCD_Unique** and ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. **OE.CGA_QCert** prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

7.4.2 Organisational Security Policies

P.CSP_QCert establishes the CSP generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by

- the TOE security objective **OT.Lifecycle_Security**, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- the TOE security objective **OT.SCD_SVD_Corresp**, which requires to ensure the correspondence between the SVD and the SCD during their generation,
- the security objective for the operational environment **OE.CGA_QCert** for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

P.QSign provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. **OT.Sigy_SigF** ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others. **OT.Sig_Secure** ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques. **OE.CGA_QCert** addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature.

OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

P.Sigy_SSCD requires the TOE to meet Annex III. This is ensured as follows:

- **OT.SCD_Unique** meets the paragraph 1(a) of Annex III, by the requirements that the SCD used for signature creation can practically occur only once;
- **OT.SCD_Unique, OT.SCD_Secrecy and OT.Sig_Secure** meet the requirement in paragraph 1(a) of Annex III by the requirements to ensure secrecy of the **SCD. OT.EMSEC_Design** and **OT.Tamper_Resistance** address specific objectives to ensure secrecy of the SCD against specific attacks;
- **OT.SCD_Secrecy** and **OT.Sig_Secure** meet the requirement in paragraph 1(b) of Annex III by the requiements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE;
- **OT.Sigy_SigF** meets the requirement in paragraph 1(c) of Annex III by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others;
- **OT.DTBS_Integrity_TOE** meets the requirements in paragraph 2 of Annex III as the TOE must not alter the DTBS/R.

Paragraph 2 of Annex III, requires that an SSCD does not prevent the data to be signed from being presented to the signatory prior to the signature process is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the signatory and send it to the SSCD for signing.

The usage of SCD under sole control of the signatory is ensured by

- **OT.Lifecycle_Security** requiring the TOE to detect flaws during the initialisation, personalisation and operational usage,
- **OT.SCD/SVD_Auth_Gen**, which limits invocation of the generation of the SCD and the SVD to authorised users only, and
- **OT.Sigy_SigF**, which requires the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.

OE.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, initialised and personalised SSCD from an SSCD-provisioning service.

P.Sig_Non-Repud deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures created with the TOE. **OE.SSCD_Prov_Service** ensures that the signatory obtains an authentic copy of the TOE, initialised and personalised as SSCD from the SSCD-provisioning service. **OE.CGA_QCert** ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. **OE.SVD_Auth** and **OE.CGA_QCert** require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. **OT.SCD_SVD_Corresp** ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. **OT.SCD_Unique** provides that the signatory's SCD can practically occur just once.

OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). **OT.Sigy_SigF** provides that only the signatory may use the TOE for signature creation. As prerequisite **OE.Signatory** ensures that the signatory keeps their VAD confidential. **OE.DTBS_Intend**, **OE.DTBS_Protect** and **OT.DTBS_Integrity_TOE** ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS. The robust cryptographic techniques required by **OT.Sig_Secure** ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE **OT.Lifecycle_Security** (Lifecycle security), **OT.SCD_Secrecy** (Secrecy of the signature creation data), **OT.EMSEC_Design** (Provide physical emanations security), **OT.Tamper_ID** (Tamper detection) and **OT.Tamper_Resistance** (Tamper resistance) protect the SCD against any compromise.

7.4.3 Assumptions

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

A.SCA establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by **OE.DTBS_Intend** (Data intended to be signed) which ensures that the SCA generates the DTBS/R of the data that have been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

A.APPLET This assumption is upheld by the security objective for the operational environment OE.APPLET which ensures that no applet loaded post-issuance shall contain native methods.

A.VERIFICATION This assumption is upheld by the security objective on the operational environment OE.VERIFICATION which guarantees that all the bytecodes shall be verified at least once, before the loading, before the installation or before the execution in order to ensure that each bytecode is valid at execution time.
This assumption is also upheld by the security objective of the environment OE.CODE-EVIDENCE which ensures that evidences exist that the application code has been verified and not changed after verification.

7.4.4 Compatibility between Security Objectives of [ST-Belpic] and [ST-PLTF]

7.4.4.1 Compatibility between objectives for the TOE

The following table lists the relevant security objectives of the Platform MultiApp V4.1 and provides the link to the security objectives related to the composite product, showing that there is no contradiction between the two.

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
O.CIPHER	The TOE shall provide a means to cipher sensitive data for applications in a secure way	OT.Sig_Secure OT.Sigy_SigF OT.TOE_TC_VAD_Imp TOE_TC_DTBS_Imp
O.KEY-MNGT	The TOE shall provide a means to securely manage cryptographic keys. This concerns the correct generation, distribution, access and destruction of cryptographic keys.	OT.SCD_SVD_Corresp, OT.SCD_Secrecy
O.REALLOCATION	The TOE shall ensure that the re-allocation of a memory block for the runtime areas of the Java Card VM does not disclose any information that was previously stored in that block.	OT.Lifecycle_Security, OT.SCD_Secrecy
OT.AC_pers	Access Control for Personalisation of TOE and Applicative data	No direct link with the composite product security objectives, but this platform security objective is used to endure the security of the composite TOE.
O.GLOBAL_ARRAYS_CONFID	The TOE shall ensure that the APDU buffer that is shared by all applications is always cleaned upon applet selection. The TOE shall ensure that the global byte array used for the invocation of the install method of the selected applet is always cleaned after the return from the install method.	
O.TRANSACTION	The TOE must provide a means to execute a set of operations atomically	
O.PIN-MNGT	The TOE shall provide a means to securely manage PIN objects.	OT.SCD/SVD_Gen, OT.TOE_TC_VAD_Imp
O.OPERATE	The TOE must ensure continued correct operation of its security functions.	OT.Lifecycle_Security, OT.Tamper_ID,
O.DELETION	The TOE shall ensure that both applet and package deletion perform as expected.	No direct link with the composite product security objectives, but this platform security objective is used to endure the security of the composite TOE.
O.RESOURCES	The TOE shall control the availability of resources for the applications.	
O.ALARM	The TOE shall provide appropriate feedback information upon detection of a potential security violation	OT.Lifecycle_Security, OT.Tamper_ID
O.OBJ-DELETION	The TOE shall ensure the object deletion shall not break references to objects.	

Platform objective label	Platform objective short description (refer to [ST-PLTF] for the full description)	Link to the composite-product
O.SCP.SUPPORT	The SCP shall support the TSFs of the TOE.	No direct link with the composite product security objectives, but this platform security objective is used to endure the security of the composite TOE.
O.SCP.IC	The SCP shall provide all IC security features against physical attacks	OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance
O.SpecificAPI	The TOE shall provide to application a specific API means to optimize control on sensitive operations performed by application. TOE shall provide services for secure array management and to detect loss of data integrity and inconsistent execution flow and react against tearing or fault induction.	No direct link with the composite product security objectives, but this platform security objective is used to endure the security of the composite TOE.

The other objectives of the platform are not relevant for this composite TOE.

We can therefore conclude that the objectives for the TOE of [ST- Belpic] and [ST-PLTF] are consistent.

7.4.4.2 Compatibility between objectives for the environment

OE.SVD_Auth, OE.CGA_QCert, OE.SSCD_Prov_Service, OE.HID_VAD, OE.DTBS_Intend, OE.DTBS_Protect, OE.Signatory, OE.HID_TC_VAD_Exp, OE.SCA_TC_DTBS_Exp are objectives specific to [ST-Belpic] and they do no conflict with the objectives of [ST-PLTF].

The PACE objectives for the Environment of the platform, OE.Prot_Logical_Data, OE.Personalisation, OE.Terminal, OE.User_Obligations are not relevant for this application

We can therefore conclude that the objectives for the environment of [ST- Belpic] and [ST-PLTF] are consistent.

8 Extended Requirements

8.1 Extended Families

8.1.1 Extended Family FPT_EMS - TOE Emanation

8.1.1.1 Description

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

8.1.1.2 Extended Components

Extended Component FPT_EMS.1

Description

This family defines requirements to mitigate intelligible emanations.

FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Definition

FPT_EMS.1 TOE Emanation

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

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

Dependencies: No dependencies.

9 Security Requirements

9.1 Security Functional Requirements

This section describes the requirements imposed on the TOE as specified in [PP SSCD2] and [PP SSCD5] in order to achieve the security objectives laid down in the previous chapter.

[ST-PLTF] deals with the security functional requirements of [PP-JCS-Open].

Note: The assignments of the SFR appear in BOLD in the description text of each SFR.

The SFR with a refinement are declared with **[Editorially Refined]**

9.1.1 Cryptographic support (FCS)

FCS_CKM.1/ECC Cryptographic key generation

FCS_CKM.1.1/ECDSA [Editorially Refined] The TSF shall generate ***SCD/SVD pair*** in accordance with a specified cryptographic key generation algorithm **ECC Key Pair Generation** and specified cryptographic key sizes **256, 384, 512 and 521 bits** that meet the following: **[NIST FIPS 186-4]**.

Refinement:

Substitution of cryptographic keys by SCD/SVD pairs

FCS_CKM.1/AES Session Key generation

FCS_CKM.1.1/AES [Editorially Refined] The TSF shall generate ***AES Session Keys*** in accordance with a specified cryptographic key generation algorithm **ECDH** and specified cryptographic key sizes **256 bits** that meet the following: **[NIST SP 800-56A]**.

Refinement:

Substitution of cryptographic keys by AES Session Keys

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwrite the keys** that meets the following: **no standard**.

Application Note:

The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 [Editorially Refined] The TSF shall perform **[cryptographic operations]** in accordance with a specified cryptographic algorithm **[cryptographic algotithm]** and cryptographic key sizes **[key sizes]** that meet the following: **[Norms]**.

Refinement:

The assignment of the cryptographic operation are described in the table below:

Iteration	Cryptographic operation	Algorithms	Key size (bits)	Norms
/RSA	Digital signature verification	RSA	2048	RSASSA-PSS with SHA 2: RSA PKCS#1 2.1 (June 2002)
/ECC-SIGN	Digital signature verification	ECC	256, 384, 512, 521	ECDSA NIST FIPS 186-4 with with SHA 2
	Digital signature creation	ECC	256, 384, 512, 521	ECDSA NIST FIPS 186-4 With SHA (offcard): SHA 2 NIST FIPS 180-4 and SHA 3 NIST FIPS 202
	Key establishment	ECC	256, 384, 512, 521	ECDH NIST SP800-56A
/AES-CIPHER	Mutual Authentication Encryption	AES-CBC (Secure mode)	256	ISO/IEC 10116
	Secure Messaging Encryption	AES-CBC (Fast mode)	256	ISO/IEC 10116
	Secure Messaging Authentication	AES-CMAC (Fast mode)	256	NIST SP800-38B

9.1.2 User data protection (FDP)

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

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin: S.User acts as S.Admin, R.Sigy: S.User acts as S.Sigy
S.User	SCD/SVD Management	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value

FDP_ACC.1/SCD/SVD_Generation Subset access control

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

1. **subjects: S.User,**
2. **objects: SCD, SVD,**
3. **operations: generation of SCD/SVD pair**.

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

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

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

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

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

FDP_ACC.1/SVD_Transfer Subset access control

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

1. **subjects: S.User,**
2. **objects: SVD,**
3. **operations: export**.

FDP_ACF.1/SVD_Transfer Security attribute based access control

FDP_ACF.1.1/SVD_Transfer The TSF shall enforce the **SVD Transfer SFP** to objects based on the following:

1. **the S.User is associated with the security attribute Role,**
2. **the SVD**.

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

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

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

Application Note:

FDP_ACF.1/SVD Transfer SFP will be required only, if the TOE holds the SVD and the SVD is exported to the CGA for certification.

FDP_ACC.1/Signature_Creation Subset access control

FDP_ACC.1.1/Signature_Creation [Editorially Refined] The TSF shall enforce the **Signature Creation SFP** on creation_SFP**:**

1. **subjects: S.User,**
2. **objects: DTBS/R, SCD,**
3. **operations: signature creation**.

FDP_ACF.1/Signature_Creation Security attribute based access control

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

1. **the** user **S.User is associated with the security attribute "Role" and**
2. **the SCD with the security attribute "SCD Operational"**.

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

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

FDP_ACF.1.4/Signature_Creation The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no"**.

FDP_RIP.1 Subset residual information protection

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

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

1. **SCD**.
2. **SVD (if persistenly stored by the TOE)**

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

FDP_SDI.2/Persistent Stored data integrity monitoring and action

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

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

1. **prohibit the use of the altered data**
2. **inform the S.Sigy about integrity error**.

FDP_SDI.2/DTBS Stored data integrity monitoring and action

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

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

1. **prohibit the use of the altered data**
2. **inform the S.Sigy about integrity error**.

Application Note:

The integrity of TSF data like RAD shall be protected to ensure the effectiveness of the user authentication. This protection is a specific aspect of the security architecture (cf. ADV_ARC.1).

FDP_UIT.1/DTBS Data exchange integrity

FDP_UIT.1.1/DTBS The TSF shall enforce the **Signature Creation SFP** to **receive** user data in a manner protected from **modification, insertion** errors.

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

9.1.3 Identification and authentication (FIA)

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

1. **Self-test according to FPT_TST.1,**
2. **none**

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

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

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

1. **Self-test according to FPT_TST.1,**
2. **Identification of the user by means of TSF required by FIA_UID.1,**
3. **establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD**
4. **[none]**

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

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

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **three** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.

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

9.1.4 Security management (FMT)

FMT_SMR.1 Security roles

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

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

FMT_SMF.1 Specification of Management Functions

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

1. **Creation and modification of RAD,**
2. **Enabling the signature creation function,**
3. **Modification of the security attribute SCD/SVD management, SCD operational,**
4. **Change the default value of the security attribute SCD Identifier,**

5. **none**.

FMT_MOF.1 Management of security functions behaviour

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

FMT_MSA.1/Admin Management of security attributes

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

FMT_MSA.1/Signatory Management of security attributes

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

FMT_MSA.2 Secure security attributes

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

FMT_MSA.3 Static attribute initialisation

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

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

FMT_MSA.4 Security attribute value inheritance

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

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

FMT_MTD.1/Admin Management of TSF data

FMT_MTD.1.1/Admin [Editorially Refined] The TSF shall restrict the ability to **create** the **RAD** to **R.Admin**.

Application Note:

RAD being the PIN code, RAD and VAD are the same data.

FMT_MTD.1/Signatory Management of TSF data

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

Application Note:

RAD being the PIN code, RAD and VAD are the same data.

9.1.5 Protection of the TSF (FPT)

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **Side channel current, electromagnetic and timing** in excess of **State of the art limits** enabling access to **SCD** and **RAD**.

FPT_EMS.1.2 The TSF shall ensure **that unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to **RAD** and **SCD**.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

1. self-test according to FPT_TST fails
2. [none]

Application Note:

The assignment (1) addresses failures detected by a failed self-test and requiring appropriate action to prevent security violation.

When the TOE is in a secure state the TSF shall not perform any cryptographic operations and all data output interfaces shall be inhibited by the TSF.

FPT_PHP.1 Passive detection of physical attack

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

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

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **voltage, clock frequency and temperature out of bounds as well as penetration attacks** to the **integrated circuit** by responding automatically such that the SFRs are always enforced.

Application Note:

The TOE will implement appropriate measures to continuously counter physical tampering which may compromise the SCD. The "automatic response" in the element FPT_PHP.3.1 means (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time. Due to the nature of these attacks the TOE can by no means detect attacks on all of its elements (e.g. the TOE is destroyed). But physical tampering must not reveal information of the SCD. E.g. the TOE may be physically tampered in power-off state of the TOE (e.g. a smart card), which does not allow TSF for overwriting the SCD but leads to physical destruction of the memory and all information therein about the SCD. In case of physical tampering the TFS may not provide the intended functions for SCD/SVD pair generation or signature creation but ensures the confidentiality of the SCD by blocking these functions. The SFR FPT_PHP.1 requires the TSF to react on physical tampering in a way that the signatory is able to determine whether the TOE was physical tampered or not. E.g. the TSF may provide an appropriate message during start-up or the guidance documentation may describe a failure of TOE start-up as indication of physical tampering.

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up and at runtime execution for TSF data** to demonstrate the correct operation of the TSF.

Refinement:

Those TSF data are verified in integrity at the runtime execution. The executable code integrity is guarantee by the MPU of the IC

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **the file data, PIN and keys of the TSF**.

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

FTP_ITC.1/VAD Inter-TSF trusted channel – TC Human Interface Device

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

FTP_ITC.1.2/VAD The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/VAD The TSF or the HID shall initiate communication via the trusted channel for

1. User authentication according to FIA_UAU.1
2. [**none**]

Application note:

The component FTP_ITC.1/VAD requires the TSF to support a trusted channel established by the HID to send the VAD.

FTP_ITC.1/DTBS Inter-TSF trusted channel – Signature Creation Application

FTP_ITC.1./DTBS The TSF shall provide a communication channel between itself and another trusted IT product SCA that is logically distinct from other communication channelsand provides assured identification of its end points and protection of the channel data from modification or disclosure.

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

FTP_ITC.1.3/DTBS The TSF or the SCA shall initiate communication via the trusted channel for

1. Signature creation
2. [**none**]

Application note:

The component FTP_ITC.1/DTBS requires the TSF to support a trusted channel established by the SCA to send the DTBS.

9.2 Security Assurance Requirements

The security assurance requirement level is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

9.3 Security Requirements Rationale

9.3.1 Rationale tables of Security Objectives and SFRs

Requirements	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Auth_Gen	OT.SCD_SVD_Corresp	OT.SCD_Unique	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FCS_CKM.1/AES	X	X									X		
FCS_CKM.1/ECC	X	X								X			
FCS_CKM.4	X	X											
FCS_COP.1	X		X										
FDP_ACC.1/SCD/SVD_Generation	X								X				
FDP_ACF.1/SCD/SVD_Generation	X								X				
FDP_ACC.1/SVD transfer	X												
FDP_ACF.1/SVD transfer	X												
FDP_ACC.1/Signature_Creation	X			X									
FDP_ACF.1/Signature_Creation	X			X									
FDP_RIP.1		X		X									
FDP_SDI.2/Persistent		X	X							X			
FDP_SDI.2/DTBS				X	X								
FIA_AFL.1				X									
FIA_UAU.1				X					X				
FIA_UID.1				X					X				
FMT_MOF.1	X			X									
FMT_MSA.1/Admin	X								X				
FMT_MSA.1/Signatory	X			X									
FMT_MSA.2	X			X					X				
FMT_MSA.3	X			X					X				
FMT_MSA.4	X			X					X	X			
FMT_MTD.1/Admin	X			X									
FMT_MTD.1/Signatory	X			X									
FMT_SMF.1	X			X						X			
FMT_SMR.1	X			X									
FPT_EMS.1		X				X							

Requirements	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Auth_Gen	OT.SCD_SVD_Corresp	OT.SCD_Unique	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FPT_FLS.1		X											
FPT_PHP.1							X						
FPT_PHP.3		X						X					
FPT_TST.1	X	X	X										
FDP_UIT.1/DTBS													X
FTP_ITC.1/VAD												X	
FTP_ITC.1/DTBS													X

Table 3 Security Objectives and SFRs - Coverage

OT.Lifecycle_Security is provided by the SFR for SCD/SVD generation FCS_CKM.1/AES, FCS_CKM.1/ECC, SCD usage FCS_COP.1 and SCD destruction FCS_CKM.4 which ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer. The SCD usage is ensured by access control FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMF.1 and FMT_SMR.1. The test functions FPT_TST.1 provides failure detection throughout the lifecycle.

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

OT.SCD_Unique implements the requirement of practically unique SCD as laid down in Annex III, paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1/ECC.

OT.SCD_SVD_Corresp addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1/ECC to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT_SMF.1 and by FMT_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

OT.SCD_Secrecy is provided by the security functions specified by the following SFR. FCS_CKM.1/ECC, FCS_CKM.1/AES ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).

SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Sig_Secure is provided by the cryptographic algorithms specified by FCS_COP.1, which ensures the cryptographic robustness of the signature algorithms. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensures self-tests ensuring correct signature creation.

OT.Sigy_SigF is provided by an SFR for identification authentication and access control.

FIA_UAU.1 and FIA_UID.1 ensure that no signature creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process).

The security functions specified by FDP_ACC.1/Signature_Creation and FDP_ACF.1/Signature_Creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory. FMT_MOF.1 restricts the ability to enable the signature creation function to the signatory. FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

OT.DTBS_Integrity_TOE ensures that the DTBS/R is not altered by the TOE. The integrity functions specified by FDP_SDI.2/DTBS require that the DTBS/R has not been altered by the TOE.

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

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

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

OT.TOE_VAD_Imp is provided by FTP_ITC.1/VAD to provide a trusted channel to protect the VAD provided by the HID to the TOE.

OT. TOE_DTBS_Imp is provided by FTP_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by FDP_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS.

9.3.2 Compatibility between SFR of [ST-Belpic] and [ST-PLTF]

The PACE SFR are Irrelevant for the BELPIC application. All the SFR listed in the §10.1.2 TOE security finctions rationake for PACE MODULE of the [ST_PLTF] are by default in the group IP_SFR.

Requirements	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
FDP_ACC.2/FIREWALL			X
FDP_ACF.1/FIREWALL			X
FDP_IFC.1/JCVM			X
FDP_IFF.1/JCVM			X
FDP_RIP.1/OBJECTS		X	
FMT_MSA.1/JCRE	X		
FMT_MSA.1/JCVM	X		
FMT_MSA.2/FIREWALL_JCVM	X		
FMT_MSA.3/FIREWALL	X		
FMT_MSA.3/JCVM	X		
FMT_SMR.1/JCRE	X		
FMT_SMF.1/CORE_LC	X		
FCS_CKM.1/RSA std	X		
FCS_CKM.1/RSA CRT	X		
FCS_CKM.1/GP		X	
FCS_CKM.1/ECFP		X	
FCS_CKM.1/ECDH		X	
FCS_CKM.1/DHGen	X		
FCS_CKM.1/DH	X		
FCS_CKM.2/RSA	X		
FCS_CKM.2/TDES	X		
FCS_CKM.2/AES	X		
FCS_CKM.2/ECFP	X		
FCS_CKM.2/DH	X		
FCS_CKM.3	X		
FCS_CKM.4		X	

Requirements	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
FCS_COP.1/RSA-SIGN		X	
FCS_COP.1/RSA-CIPHER	X		
FCS_COP.1/ECC-SIGN		X	
FCS_COP.1/TDES-CIPHER	X		
FCS_COP.1/AES-CIPHER		X	
FCS_COP.1/AES-CIPHER FAST		X	
FCS_COP.1/TDES-CIPHER FAST	X		
FCS_COP.1/TDES-MAC	X		
FCS_COP.1/TDES-MAC FAST	X		
FCS_COP.1/AES-MAC	X		
FCS_COP.1/AES-MAC FAST	X		
FCS_COP.1/AES-CMAC FAST		X	
FCS_COP.1/SHA		X	
FCS_COP.1/DH-PACE	X		
FCS_COP.1/ECC-PACE	X		
FCS_COP.1/HMAC	X		
FCS_COP.1/OBKO		X	
FDP_RIP.1/ABORT		X	
FDP_RIP.1/APDU		X	
FDP_RIP.1/bArray		X	
FDP_RIP.1/KEYS		X	
FDP_RIP.1/TRANSIENT		X	
FDP_ROL.1/FIREWALL	X		
FAU_ARP.1			X
FDP_SDI.2		X	
FPR_UNO.1			X
FPT_FLS.1/JCS			X
FPT_TDC.1	X		
FIA_ATD.1/AID	X		
FIA_UID.2/AID	X		

Requirements	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
FIA_USB.1/AID	X		
FMT_MTD.1/JCRE	X		
FMT_MTD.3/JCRE	X		
FDP_ITC.2/Installer	X		
FMT_SMR.1/Installer	X		
FPT_FLS.1/Installer	X		
FPT_RCV.3/Installer	X		
FDP_ACC.2/ADEL	X		
FDP_ACF.1/ADEL	X		
FDP_RIP.1/ADEL	X		
FMT_MSA.1/ADEL	X		
FMT_MSA.3/ADEL	X		
FMT_SMF.1/ADEL	X		
FMT_SMR.1/ADEL	X		
FMT_SMF.1/ADEL	X		
FPT_FLS.1/ADEL	X		
FDP_RIP.1/ODEL		X	
FPT_FLS.1/ODEL		X	
FCO_NRO.2/CM	X		
FDP_IFC.2/CM	X		
FDP_IFF.1/CM	X		
FDP_UIT.1/CM	X		
FIA_UAU.1/CM	X		
FIA_UID.1/CM	X		
FMT_MSA.1/CM	X		
FMT_MSA.3/CM	X		
FMT_SMF.1/CM	X		
FMT_SMR.1/CM	X		
FTP_ITC.1/CM	X		
FPT_TST.1/SCP		X	

Requirements	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
FPT_PHP.3/SCP		X	
FPT_RCV.4/SCP			X
FDP_ACC.1/CMGR	X		
FDP_ACF.1/CMGR	X		
FMT_MSA.1/CMGR	X		
FMT_MSA.3/CMGR	X		
FPT_FLS.1/SpecificAPI		X	
FPT_ITT.1/SpecificAPI			X
FPR_UNO.1/SpecificAPI.			X
FCS_RND.1			X

Table 4 SFRs Dependencies

(*) RP_SFR-SERV group definition:

The SFR FDP_RIP.1 of the BELPIC applet is directly supporting with no incompatibilities, the SFR of the platform:

- FDP_RIP.1/OBJECTS
- FDP_RIP.1/ABORT
- FDP_RIP.1/APDU
- FDP_RIP.1/bArray
- FDP_RIP.1/KEYS
- FDP_RIP.1/TRANSIENT
- FDP_RIP.1.1/ODEL

The SFR FCS_CKM.1/ECC of the BELPIC applet is supported with no incompatibilities the Platform SFR:

- FCS_CKM.1/ECFP for the ECC key Generation (used for the command Internal Auth for the Key Agreement)
- FCS_CKM.1/ECFP for the ECC key generation
- FCS_CKM.1/ECDH for the Internal Authentification of the key agreement

The SFR FCS_CKM.1/AES of the BELPIC applet is supported with no incompatibilities the Platform SFR:

- SFR FCS_CKM.1/GP for the SCP03 (prepersonalisation)

The FCS_CKM.4 of the BELPIC Applet is directly supported with no incompatibilities the SFR of the platform: FCS_CMK.4 and there is no incompatibility

The FCS_COP.1 of the BELPIC Applet is directly supported with no incompatibilities the SFR of the platform:

- FCS_COP.1/ECC-SIGN for the ECC signature feature
- FCS_COP.1/AES-CIPHER for the key generation (used by the Internal Authentification and the external authentification)

- FCS_COP.1/AES-CIPHER FAST and FCS_COP.1/AES-CMAC FAST for the Secure Messaging
- FCS_COP.1/OBKO for the ECC key generation
- FCS_COP.1/RSA-SIGN only for the RSA signature feature. The RSA signature is Irrelevant

The FDP_SDI.2/Persistent, and FDP_SDI.2/DTBS of the Belpic Applet are directly supported with no incompatibilities the SFR of the platform FDP_SDI.2

The FPT_FLS.1/SpecificAPI of the Belpic Applet is directly supported with no incompatibilities the SFR of the platform FPT_FLS.1/ODEL

The FPT_TST.1 of the Belpic Applet is directly supported with no incompatibilities the SFR of the platform FPT_TST.1/SCP

The FPT_PHP.3 of the Belpic Applet is directly supported with no incompatibilities the SFR of the platform FPT_PHP.3/SCP

FPT_FLS.1 of the Belpic Applet is directly supported with no incompatibilities the SFR of the platform FPT_FLS.1/SpecificAPI

9.3.3 Dependencies

9.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCS_CKM.1/ECC	(FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1
FCS_CKM.1/AES	(FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/ECC, FCS_CKM.1/AES
FCS_COP.1	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/ECC, FCS_CKM.1/AES
FDP_ACC.1/SCD/SVD_Generation	(FDP_ACF.1)	FDP_ACF.1/SCD/SVD_Generation
FDP_ACF.1/SCD/SVD_Generation	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACC.1/SVD_Transfer	(FDP_ACF.1)	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SVD_Transfer	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
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, FMT_MSA.3
FDP_RIP.1	No Dependencies	
FDP_SDI.2/Persistent	No Dependencies	
FDP_SDI.2/DTBS	No Dependencies	
FIA_UID.1	No Dependencies	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FIA_AFL.1	(FIA_UAU.1)	FIA_UAU.1
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FMT_SMF.1	No Dependencies	
FMT_MOF.1	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1

Requirements	CC Dependencies	Satisfied Dependencies
FMT_MSA.1/Admin	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1
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, FMT_SMF.1
FMT_MSA.2	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.4	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FPT_EMS.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_PHP.1	No Dependencies	
FPT_PHP.3	No Dependencies	
FPT_TST.1	No Dependencies	
FDP_UIT.1/DTBS	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FTP_ITC.1/VAD	No Dependencies	
FTP_ITC.1/DTBS	No Dependencies	

Table 5 SFRs Dependencies

9.3.3.2 SARs Dependencies

EAL5+ SAR	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	(ADV_IMP.1) and (ADV_TDS.1)	ADV_IMP.1, ADV_TDS.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4, ALC_TAT.2
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	(ADV_FSP.5)	ADV_FSP.5
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.5
AGD_PRE.1	No dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2,) ALC_LCD.1
ALC_CMS.5	No dependencies	
ALC_DEL.1	No dependencies	
ALC_DVS.2	No dependencies	
ALC_LCD.1	No dependencies	
ALC_TAT.2	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependencies	
ASE_INT.1	No dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	(ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3

Table 6 SARs Dependencies

9.3.4 Rationale for the Security Assurance Requirements

EAL5 is required for this type of TOE and product since it is intended to defend against sophisticated attacks. This evaluation assurance level allows a developer to gain maximum assurance from positive security engineering based on good practices. EAL5 represents the highest practical level of assurance expected for a commercial grade product. In order to provide a meaningful level of assurance that the TOE and its embedding product provide an adequate level of defense against such attacks the evaluators should have access to the low level design and source code. The lowest for which such access is required is EAL5.

The assurance level EAL5 is achievable, since it requires no specialist techniques on the part of the developer.

Additional assurance requirements are also required due to the definition of the TOE and the intended security level to assure.

9.3.4.1 AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to operate in hostile environments. AVA_VAN.5 "Advanced methodical vulnerability analysis" is considered as the expected level for Java Card technology-based products hosting sensitive applications, in particular in payment and identity areas. AVA_VAN.5 has dependencies on ADV_ARC.1, ADV_FSP.1, ADV_TDS.3, ADV_IMP.1, AGD_PRE.1 and AGD_OPE.1. All of them are satisfied by EAL5.

9.3.4.2 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE and the embedding product. The standard ALC_DVS.1 requirement mandated by EAL5 is not enough.

Due to the nature of the TOE and embedding product, it is necessary to justify the sufficiency of these procedures to protect their confidentiality and integrity. ALC_DVS.2 has no dependencies.

10 TOE Summary Specification

10.1 TOE Summary Specification

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

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

10.1.1 TOE SECURITY FUNCTIONALITIES PROVIDED BY PLATFORM

Hardware Physical Protection

This security functionality protects the electronic signature application data RAD and SCD against physical tampering and physical probing. The security functionality ensures that:

1. The TOE shall resist physical reverse engineering.
2. The TOE shall ensure that the S.Attacker is not able to physically access to RAD and SCD storage location in memory.

This security function is supported by the IC security function SFR3 as described in [ST-IC]. SFR3 is implemented by countermeasures such as IC layout scrambling and active shield.

Hardware Emanation Protection

This security functionality protects the electronic signature application data RAD and SCD against snooping. The security functionality ensures that:

1. The TOE shall not emit electromagnetic radiation in excess of unintelligible emission enabling access to RAD and SCD.
2. The TOE shall ensure that the S.Attacker is not able to use I/O, VCC or Ground interface to gain access to RAD and SCD.

This security function is supported by the IC security function SFR14 as described in [ST-IC]. SFR14 consists of emanation protections in the IC such as data bus encryption, memory encryption and de-synchronization.

Logical Protection

The MultiApp platform provide the following security functions related to logical card operations from [ST-PLTF]:

Security Function	Name	Description
SF_FW	Firewall	Provides applet isolation
SF_API	Application Programming Interface	Provides access to cryptography library
SF.CSM	Card Security Management	Provides resource allocation/deallocation, exception handling and integrity checks on key and data
SF.AID	AID Management	Provides Applet ID management
SF.INST	Installer	Provides Applet management
SF.ADEL	Applet Deletion	Provides Applet management
SF.ODEL	Object Deletion	Provides object deallocation
SF.CAR	Secure Carrier	Provides evidence of origin for application packages
SF.SCP	Smart Card Platform	Provides integrity checks on applets, PIN and keys. Checks the physical attack sensors
SF.CMG	Card Manager	Provides security attribute integrity
SF.APIS	Specific API	Provides application control flow
SF.RND	RNG	Provides AIS31 Random Number Generator

Table 7 MultiApp V4.1 Security Functions

10.1.2 TOE SECURITY FUNCTIONALITIES PROVIDED BY BELPIC APPLET

Authentication management

This security functionality manages the authentication mechanisms such as:

1. Authentication operations for role management (i.e. PIN verification)
2. External Authentication to authenticate the external application to get access to the autorized data and functions during the operational phase

This security function:

3. Manages authentication failure: when the three unsuccessful authentication attempts has been met or surpassed, the TSF shall block RAD.
4. Manage the RAD.

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

5. Identification of the user

Cryptography management

This security functionality manages the cryptographic operations of the electronic signature application:

1. Key generation for ECC
2. Key destruction / Key erase
3. Perform cryptographic operations

Cryptographic algorithms ECC, RSA and RNG and provided by the platform and ensures that SCD information is made unavailable after use (key erase).

1. ECC algorithm supports key 256, 384, 512 and 521 bits. The ECC algorithm is provided by the platform. The platform supports ECDSA and ECDH protocols based on ECC.
2. RSA algorithm supports 2048 bits key. The RSA algorithm is provided by the platform. The platform supports RSA mode. The RSA is used to verify the signature only (public key).
3. Random generator uses the certified Hardware Random Generator that fulfils the requirements of AIS31 (see [ST-PLTF]).
4. SHA 256, 384 and 512 hash algorithms

This security function controls all the operations relative to the card keys management (provided also by the platform)

5. Key generation: The TOE provides the following:

- ECDSA key generation for 256, 384, 512 and 521 bits keys.

6. Key destruction/key erase: the TOE provides a specified cryptographic key destruction method that makes Key unavailable.

This security functionality ensures the confidentiality of keys during manipulation and ensures the de-allocation of memory after use. It is supported by the platform security function SF.RND (Random Number Generator), see [ST-PLTF].

Integrity monitoring

The integrity of persistently stored data such as SCD, RAD and SVD is monitored using the platform features.

This TSF also monitors the integrity of the access conditions of created data objects and also ensures that no residual information is available after a PIN update or clearance.

In case of integrity error this TSF will

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

Operation Management and Access Control

This security functionality provides application operation management and access control.

Operation management This security functionality manages the electronic signature application during its initialization and operation. This SF manages the security environment of the application and:

1. Maintains the roles S.Signatory, S.Admin.
2. Controls if the authentication required for a specific operation has been performed with success.
3. Manages restriction to security function access and to security attribute modification.
4. Ensures that only secure values are accepted for security attributes.

This security functionality restricts the ability to perform the function Signature-creation SFP to S.Signatory. This security functionality ensures that only S.Admin is authorized to

1. Modify Initialization SFP and Signature-creation SFP attributes
2. Specify alternative default values

Access control This security functionality provides the electronic signature application with access control and ensures that the following operations are executed by authorized roles:

1. Generation of SCD/SVD pair by S.User
2. Creation of RAD by S.Admin
3. Signing of DTBS-representation by S.Signatory

This security functionality provides access control to data objects.

This security functionality enforces the security policy on the export of user data on:

1. SVD Transfer SFP: SVD shall be sent to an authenticated CGA.
2. Signature-creation SFP: DTBS/R shall be sent by an authenticated SCA.

Trusted Channel/Secure Messaging

The TOE implements trusted channel using its secure messaging feature. The secure messaging is based on ECDH protocol and AES symmetric algorithm. During mutual authentication with an external application, the TOE shared the elliptic curve parameters to the application. The ECDH key establishment generates a mutually-known 256-bit random value. This random bits is then used as AES session key to secure the subsequent communication between the TOE and the application in the particular session.

Index