THALES
Building a future we can all trust

IAS Classic v5.2.1 with MOC Server v3.1.1 on MultiApp V5.1
Security Target Lite
Version 1.2p

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

© Copyright Thales

CONTENT

© Copyright Thales

FIGURES

TABLES

© Copyright Thales

1. SECURITY TARGET INTRODUCTION

1.1 SECURITY TARGET REFERENCE

Title :	IAS Classic v5.2.1 with MOC Server v3.1.1 on MultiApp v5.1 Security Target Lite
Version :	1.2p
ST Reference :	D1569576
Origin :	THALES
IT Security Evaluation scheme :	LETI
IT Security Certification scheme :	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

1.2 TOE REFERENCE

The product is available in a combination of 4 configurations:

- Configuration 1: TOE based on the IC AQUARIUS_BA_09- AQUARIUS_v1 called "revision B"
  - FULL configuration
  - COMPACT configuration
- Configuration 2: TOE based on the IC AQUARIUS_CA_09- AQUARIUS_v2 called "revision C"
  - FULL configuration
  - COMPACT configuration

Product Name :	IAS Classic v5.2.1
Product Commercial Names:	IAS Classic v5.2.1 on MultiApp V5.1
Security Controllers :	For the configuration 1 (Revision B): AQUARIUS_BA_09 (Thales DIS France SAS) For the configuration 2 (Revision C): AQUARIUS_CA_09 (Thales DIS France SAS)
TOE Name :	IAS Classic V5.2.1 on MultiApp V5.1
TOE Version :	For configuration 1 (Revision B): **IAS Classic version 5.2.1.A.C** for FULL configuration **IAS Classic version 5.2.1.A.O** for COMPACT configuration For configuration 2 (Revision C): **IAS Classic version 5.2.1.A.C Revision C** for FULL configuration **IAS Classic version 5.2.1.A.O Revision C** for COMPACT configuration
TOE Marketing Product Reference*	M1016970
TOE Technical Product Reference*	T1038534
Product Guidance :	Guidance [AGD]
Composition elements:	
Platform Identifier:	MultiApp V5.1 Platform
Platform Version:	5.1

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

The TOE will be delivered in two configurations of the IAS applet

1. IAS Classic V5.2.1 - Full configuration on MultiApp V5.1
2. IAS Classic V5.2.1 - Compact configuration on MultiApp V5.1

The Platform MAV5.1 [ST-PLTF] is covering the both configurations.

© Copyright Thales

1.3 TOE IDENTIFICATION

The TOE identification is provided by the Card Production Life Cycle Data (CPLC Data) of the TOE. These data are available by executing a dedicated command.

The TOE identification is provided by a dedicated command GET CARD DATA with the next TAG:

	P1	P2
CPLC data	'9F'	'7F'
Software version	'7F'	'30'
Applet version	'DF'	'30'

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

1.3.1 IAS Full configuration

With TAG "7F30": Software version (Applet Label + Applet version)

When requiring the software version (P1P2='7F30') the applet returns, embedded in a BERTLV '7F30', 'C0' and 'C1' as described in next table:

Tag	Length	Value	Subject	Value
'C0'	'0E'	"IAS Classic v5"	Applet label	"IAS Classic v5" (ascii) Or '49:41:53:20:43:6C:61:73:73:69:63:20:76:35' (hexa)
'C1'	'09'	"5.2.1.A.C"	Applet version	IAS ClassicV5.2.1 on MultiAppV5.1 "5.2.1.A.C" (ascii) or '35:2E:32:2E:31:2E:41:2E:43' (hexa)

With TAG "DF30": Applet version (identical to Applet version with tag "7F30")

When requiring the applet version (P1P2='DF30') the applet returns the applet version embedded in a BERTLV 'DF30':

Value	Subject	Value
"5.2.1.A.C"	Applet version	5.2.1.A.C '352E322E312E412E43'

1.3.2 IAS Compact configuration

With TAG "7F30": Software version (Applet Label + Applet version)

When requiring the software version (P1P2='7F30') the applet returns, embedded in a BERTLV '7F30', 'C0' and 'C1' as described in next table:

Tag	Length	Value	Subject	Value
'C0'	'0E'	"IAS Classic v5"	Applet label	"IAS Classic v5" (ascii) Or '49:41:53:20:43:6C:61:73:73:69:63:20:76:35' (hexa)
'C1'	'09'	"5.2.1.A.O"	Applet version	IAS CompactV5.2.1 on MultiAppV5.1 "5.2.1.A.O" (ascii) or '35:2E:32:2E:31:2E:41:2E:4F' (hexa)

With TAG "DF30": Applet version (identical to Applet version with tag "7F30")

When requiring the applet version (P1P2='DF30') the applet returns the applet version embedded in a BERTLV 'DF30':

Value	Subject	Value
"5.2.1.A.O"	Applet version	5.2.1.A.O '352E322E312E412E4F'

© Copyright Thales

1.3.3 IAS Common to all configurations

With TAG "9F7F"

When requiring the CPLC data (P1P2='9F7F'), the applet returns the following data:

DTHR data		
Tag	**Length**	**Subject**
'9F7F'	'2A'	CPLC Data is defined in below

Name	Length in bytes	Value
IC fabricator	2	1290h
IC type	2	0013h
Operating system identifier	2	1981h
Operating system release date	2	3055h
Operating system release level	2	0510h
IC fabrication date	2	
IC serial number	4	
IC batch ID	2	
IC module fabricator	2	
IC module packaging data	2	
ICC manufacturer	2	
IC embedding date	2	
IC pre-personalizer	2	
IC pre-personalization date	2	
IC pre-personalization equipment ID	4	
IC personalizer	2	
IC personalization date	2	
IC personalization equipment ID	4	

The TOE and the product differ, as further explained in §2 TOE boundaries:

- The TOE is the IAS Classic v5.2.1 application, with MOCA Server, on the JCS open platform MultiApp V5.1
- The MultiApp V5.1 product also includes other applets.

Note: The identification of the IC type is provided by the Platform.
To read this information, it is needed to make a PACE authentication, a Select ISD and read the tag 010B as describe in the [ST-PLTF].

With TAG "010B"

The identification of the IC type is provided by the Platform.

To read this information, it is needed to make a Select ISD and to read the tag 010B as describe in the [STs-Platform]. The command GET CARD DATA can be found in the [AGD-Platform].

Index	Description	IC Revision B Value (Previous)	IC Revision C Value	Part of TOE the identification
0	PRODUCT	0x09	0x09	No
1	HW_REV	0x42	0x43	Yes
2	Not relevant for identification			No
…				No
15				No

1.3.4 MOC Server v3.1.1

The MOC Server v3.1.1 identification is provided by a dedicated command GET VERSION with the following format:

Field	Value
CLA	00h
INS	5Ah
P1	00h
P2	00h
Le	25h

The response of the GET VERSION is described below:

Field	Value
Data	Identification of MOC Server is detailed in the below
SW1-SW2	Status Bytes

The data are structured with two BER coded data objects as follow:

- Tag ‘A0’ contains the product reference.
- Tag ‘A1’ contains the product version.
- Tag ‘A2’ contains the Fingerprint Algo version (under hexadecimal form).
- Tag ‘A3’ contains the Face Algo Version (under decimal form).
- Tag ‘A4’ contains the Iris Algo Version (under decimal form).

Details are given in the table below:

Tag	Length	Value	Subject	Value
A0h	0Fh	“MOCA SERVER 3.1”	Applet label	4D:4F:43:41:20:53:45:52:56:45:52:20:33:2E:31
A1h	07h	3.1.1.A	Applet version (“M.m.ny”) M: Major m: minor n: sub version y: release (A-Z)	33:2E:31:2E:31:2E:41
A2h	02h	2.0.6	Fingerprint Algo version	00:CE
A3h	02h	5.2	Face Algo Version	05:02
A4h	02h	3.0	Iris Algo Version	03:00

The TOE and the product differ, as further explained in §2 TOE boundaries:

- The TOE is the IAS application, with MOC server, on the JCS open platform MultiApp V5.1
- The MultiApp V5.1 product also includes other applets (see section 2.2).

© Copyright Thales

1.4 SECURITY TARGET OVERVIEW

The Target of Evaluation (TOE) is composed of the MultiApp V5.1 platform and the electronic signature application IAS Classic V5.2.1 with MOC Server V3.1.1.

The platform includes the hardware and the operating system.

The IC is evaluated in conformance with [PP-IC-0084].

The Platform is evaluated in conformance with [PP-JCS-Open].

The IAS application is evaluated in conformance with [PP-SSCD-KG TCCGA TCSCA] and [PP-SSCD-KI TCSCA],

The main objectives of this ST are:

- To introduce TOE and the IAS application,
- To define the scope of the TOE and its security features,
- To describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- To describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.
- To specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functions.

© Copyright Thales

1.5 REFERENCES

1.5.1 External References

[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-2012-04-003, version 3.1 rev 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation Evaluation Methodology CCMB-2017-04-004, version 3.1 rev 5, April 2017
[ICAO]	**ICAO references**
[ICAO-TR-SAC]	Technical Guideline – TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26.02.2015
[ISO]	**ISO references**
[ISO7816]	*ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange*, FDIS2004
[ISO9796-2]	*ISO/IEC 9796-2:2010: Information technology – Security techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorization based mechanisms,* *Third edition 2010-12-15*
[ISO9797-1]	*ISO/IEC 9797-1:2011: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, Second edition 2011-03-01*
[PKCS#3]	*PKCS #3: Diffie-Hellman Key-Agreement Standard,* An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[PP]	**Protection profiles**
[PP-SSCD]	[EN-419211] supersedes former EN 14169
[PP-SSCD-KG]	[EN-419211-2]
[PP-SSCD-KI]	[EN-419211-3]
[EN-419211]	Protection profiles for secure signature creation device – EN version
[PP-SSCD-KG TCCGA TCSCA]	[EN-419211-2] & [EN-419211-4] & [EN-419211-5]
[PP-SSCD-KI TCSCA]	[EN-419211-3] & [EN-419211-6]
[EN-419211-2]	Protection profiles for secure signature creation device – Part2 : Device with key generation BSI-CC-PP-0059-2009-MA-02, 30 June 2016
[EN-419211-3]	Protection profiles for secure signature creation device – Part3: Device with key import BSI-CC-PP-0075-2012-MA-01, 30 June 2016
[EN-419211-4]	Protection profiles for secure signature creation device – Part4: Extension for device with key generation and trusted communication with certificate generation application BSI-CC-PP-0071-2012-MA-01, 30 June 2016

© Copyright Thales

[EN-419211-5]	Protection profiles for secure signature creation device – Part5: Extension for device with key generation and trusted communication with signature-creation application BSI-CC-PP-0072-2012-MA-01, 30 June 2016
[EN-419211-6]	Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application BSI-CC-PP-0076-2013-MA-01, 30 June 2016
[PP-JCS-Open]	Java Card System Protection Profile – Open Configuration BSI-CC-PP-0099-V2-2020, Version 3.1, April 2020
[PP-IC-0084]	Security IC Platform Protection Profile with augmentation Packages– BSI-CC-PP-0084-2014

1.5.2 Internal References

[ASE]	**TOE Security Target**
[ST-PLTF]	MultiApp V5.1: JCS Security Target Ref: D1569436
[AGD]	**TOE Guidance documentation**
[AGD-USR]	IAS Classic v5.2.1, Reference Manual Ref: D1542053C
[AGD-USR-BIO]	BioPIN Manager V3 Reference Manual Ref: D1481720E
[AGD-OPE-PRE]	MultiApp V5.1: AGD OPE and PRE – IAS Classic v5.2.1 Ref: D1588538
[AGD-PERSPEC]	IAS Classic v5.2.1, Personalization Profiles Guide Ref: D1546633B
[AGD-COMP]	**TOE Guidance documentation – Composition**
[AGD-COMP-USR]	MultiApp ID Operating System –Reference Manual Ref: D1525385C
[AGD-Ref]	MultiApp Guidance Document - Guidance document for secure development for MultiApp products Ref: D1539156

© Copyright Thales

1.6 ACRONYMS AND GLOSSARY

Acr.	Term	Definition
	Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [SS]
	IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
	IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
	Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [SS]
	Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification l (IC identification data).
IC	Integrated circuit	Electronic component(s) designed to perform processing and/or memory functions. The MultiApp's chip is a integrated circuit.
	Personalization	The process by which the portrait, signature and biographical data are applied to the document. [SS]
	Personalization Agent	The agent acting on the behalf of the issuing State or organization to personalize the TOE for the holder.
	Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
	Pre- personalization Data	Any data that is injected into the non-volatile memory of the TOE by the TOE Manufacturer (Phase 2) for traceability of non-personalized TOE's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair.
	Pre –personalized TOE's chip	TOE's chip equipped with pre-personalization data.
	TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [1]).
	User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [1]).
CGA	Certification Generation Application	Application with the purpose to generate certificate
CSP	Certification Service Provider	Provide certification service including CGA
DTBS or DTBS/R	Data to be signed or its unique Representation	Data to be signed, off-card hash value
HID	Human Interface Device	Human interface provided by the SCA for user authentication.
RAD	Reference Authentication Data	PIN stored in EID
SCA	Signature-Creation Application	application with a user interface to create an electronic signature
SCD	Signature-Creation Data	Private Key used to create electronic signature
SDO	Signed Data Object	Electronic data to which an electronic signature has been attached to or logically associated with as a method of authentication.

SSCD	Secure Signature Creation Device	Smartcard able to provide the services described in [PP-SSCD-KG TCCGA TCSCA] and [PP-SSCD-KI TCSCA]
SVD	Signature-Verification Data	Public Key used to verify electronic signature
VAD	Verification Authentication Data	PIN given by end user

© Copyright Thales

2. TOE OVERVIEW

2.1 TOE DESCRIPTION

IAS is a Java Card application that provides a Secure Signature Creation Device [SSCD] as defined in the REGULATION N° 910/2014 of the European Parliament and of the Council of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[PP-SSCD] defines protection profiles for SSCD:

- [PP-SSCD-KG] is a protection profile for an SSCD with SCD/SVD key generation and signature creation.
- [PP-SSCD-KI] is a protection profile for an SSCD with SCD key import and signature creation.

[PP-SSCD] also defines possible extensions for the above protection profiles (included in this TOE):

- [EN-419211-4] defines extensions for [PP-SSCD-KG] with trusted communication between SSCD and CGA.
- [EN-419211-5] defines extensions for [PP-SSCD-KG] with trusted communication between SSCD and SCA.
- [EN-419211-6] defines extensions for [PP-SSCD-KI] with trusted communication between SSCD and SCA.

In this document the terminology of [PP-SSCD] is used. In particular, the Signatory's Reference Authentication Data (RAD) is the PIN stored in the card and the Signatory's Verification Authentication Data (VAD) is the PIN provided by the user.

The IAS application can be used in contact (T=0 and T=1) or contactless (T=CL) mode.

The IAS application supports:

- The import of the SCD via a trusted channel
- The (on-board) generation of SCD/SVD pairs
- The generation of electronic signatures
- The export of the SVD to the certification generation application (CGA)
- PIN Policy features: PIN Length, Char set used, overall quality checking, PIN change before first used, PIN history

IAS is aimed to create legal valid signatures and therefore provides mechanisms to ensure the secure signature creation as:

- Authentication of the signatory by PIN or BioPIN,
- Authentication of the administrator (mutual authentication):

Mutual Authentication	**Configurations**	
	IAS Full	***IAS Compact***
Symmetric scheme with TDES or AES	Present	Present
Asymmetric scheme with Diffie-Hellman based on RSA or elliptic curves	Present	Not Supported

- Integrity of access conditions to protected data (SCD, RAD),
- Integrity of the data to be signed (DTBS),
- External communication protection against disclosure and corruption (secure messaging),
- Access control to commands and data by authorized users.

The functionalities of IAS Classic 5.2.1 other than the ones from SSCD are out of scope of the TOE perimeter. For BioPIN (MOC Server v3.1.1 application) provides biometry recognition with fingerprint, facial and Iris matchers.

© Copyright Thales

2.2 TOE BOUNDARIES

The Target of Evaluation (TOE) is the Secure Signature Creation Device (SSCD) IAS defined by:

- The underlying Integrated Circuit
- The MultiApp V5.1 platform (JavaCard platform)
- The IAS Classic Application V5.2.1.
- The BioPin application (MOC Server Application V3.1.1).

The figure below gives a description of the TOE and its boundaries (red dash line).

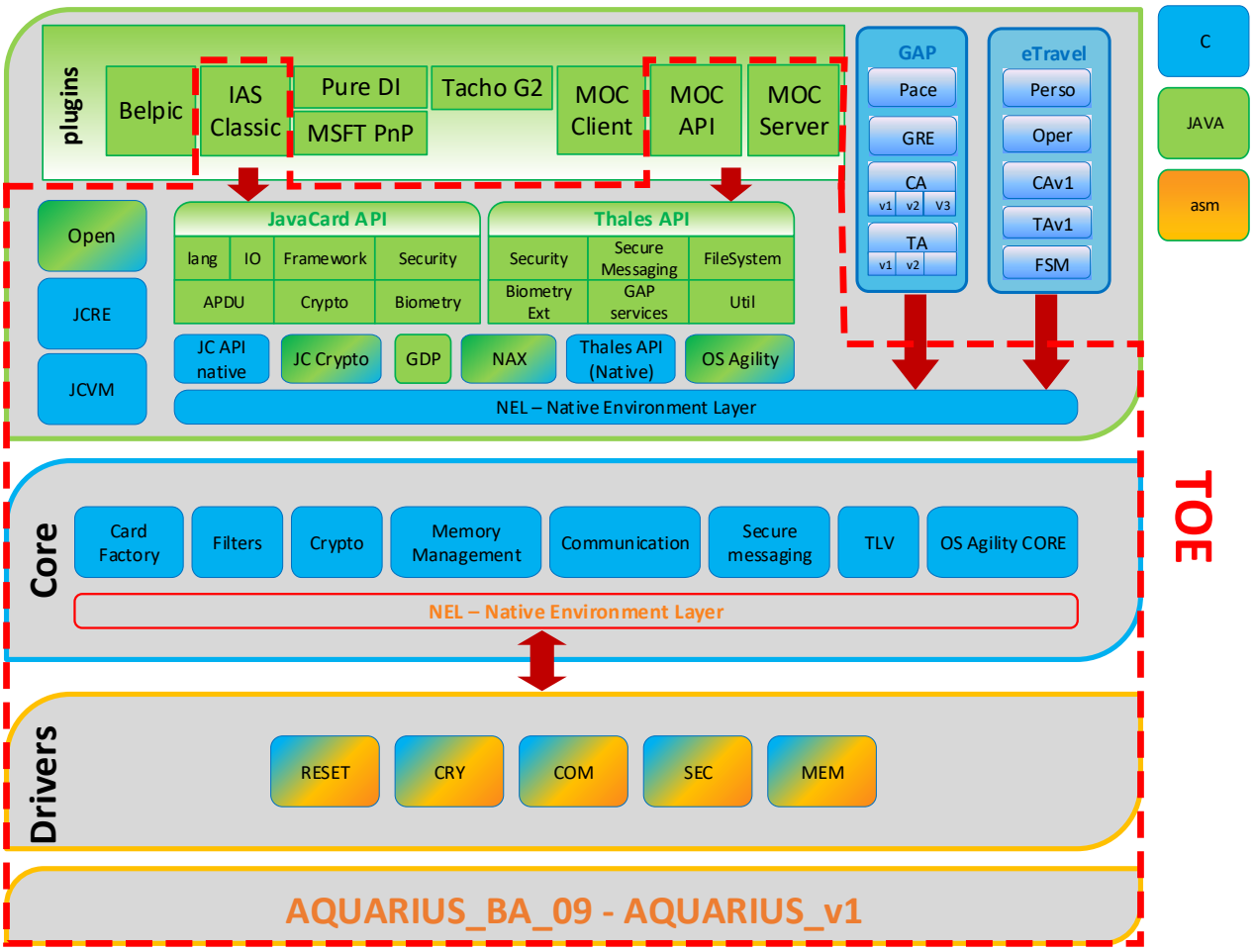


Figure 1: TOE Boundaries

2.3 TOE LIFE-CYCLE

2.3.1 Actors

Actors	Identification
Integrated Circuit (IC) Developer	THALES Design Services
Embedded Software Developer	THALES
Integrated Circuit (IC) Manufacturer	THALES Design Services
Module manufacturer	THALES Design Services
Initializer/Pre-personalizer	THALES
Administrator or Personalization Agent	The agent who personalizes the SSCD for the holder.
Signatory or SSCD Holder	The rightful holder of the TOE for whom the Administrator personalizes the SSCD.

Table 1: Identification of the actors

2.3.2 Four phases

The TOE life cycle is described in terms of the four life cycle phases:

Phase 1 “Development”:
The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.
The Embedded Software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the SSCD application and the guidance documentation associated with these TOE components. As a result the flashmask is generated (HEX file) with initialisation and pre-personalisation scripts.

Phase 2 “Manufacturing”:
In a first step the IC is produced by the IC manufacturer including the THALES flash loader and protected by a dedicated transport key. The creation of the Module can be done by Thales.
Then the module is put on a dedicated form factor (Card, Inlay, other) by Thales or a Form factor manufacturer.
The SSCD manufacturer (Thales) has the following tasks:

- **Initialization:** Load the Thales software (flash mask including the platform and the applications) in the flash memory
- **Pre-personalization:** initialization of the SSCD application.

© Copyright Thales

Phase 3 Personalization of the TOE:

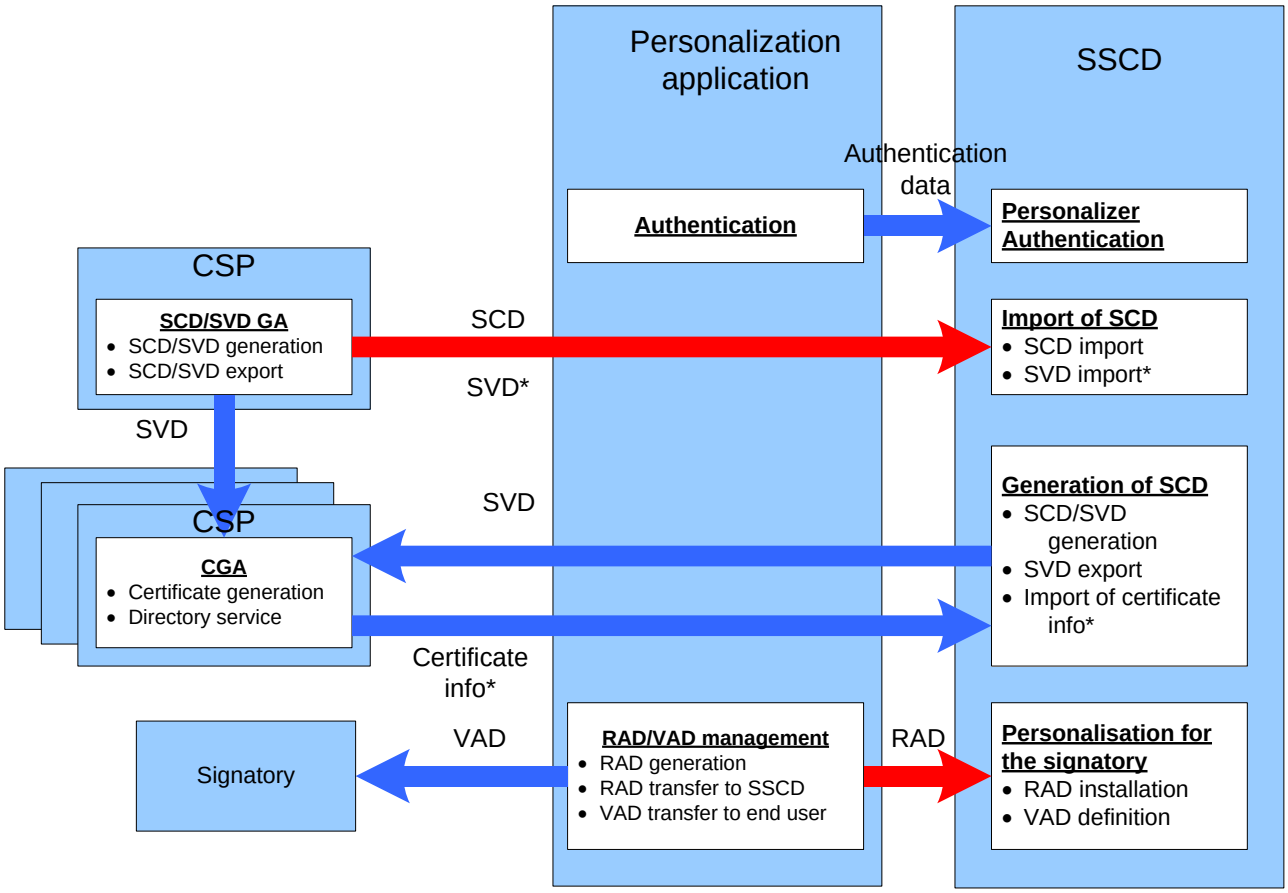


Figure 2: TOE Personalization

RAD Import in the Personalization phase,

- The Personalizor (Administrator) authenticates himself to the TOE.
- The Personalizor (Administrator) sends the RAD to the TOE.
- The RAD shall also be securely sent to the Signatory.

SCD Import in the Personalization phase,

- The Personalizor (Administrator) authenticates himself to the TOE.
- The Personalizor (Administrator) requests the generation of a SCD/SVD key pair on the CSP.
- The SCD / SVD pair is generated.
- The SCD is sent to the TOE.
- The SVD is sent to the CGA.
- The CGA generates the certificate.
- The certificate info is imported into the TOE.

SCD/SVD generation in the Personalization phase,

- The Personalizor (Administrator) authenticates himself to the TOE.
- The Personalizor (Administrator) requests the generation of a SCD/SVD key pair on the SSCD.
- The SCD / SVD pair is generated in the TOE.
- The SVD is sent to the CGA.
- The CGA generates the certificate.
- The certificate info is imported into the TOE.

© Copyright Thales

Phase 4 “Operational Use”

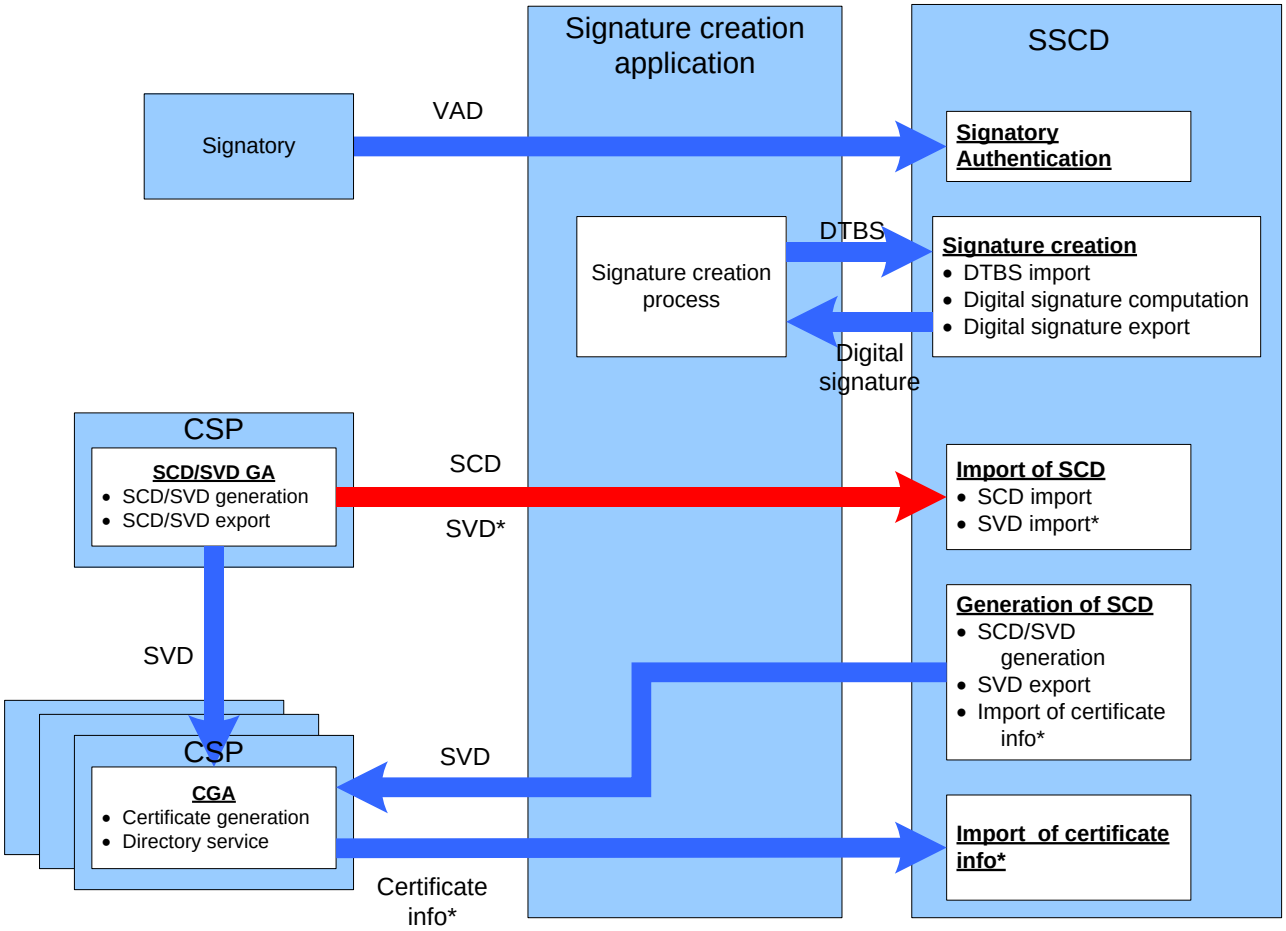


Figure 3: TOE Operational Use

SCD/SVD generation in the usage phase,

- The signatory enters his PIN code (VAD) to authenticate himself to the TOE.
- The signatory requests the generation of a SCD/SVD key pair on the SSCD.
- The SCD / SVD pair is generated in the TOE.
- The SVD is sent to the CGA.
- The CGA generates the certificate.
- The certificate info is imported into the TOE.

SCD Import in the usage phase,

- The signatory authenticates himself to the TOE.
- The signatory requests the generation of a SCD/SVD key pair on the CSP.
- The SCD / SVD pair is generated.
- The SCD is sent to the TOE.
- The SVD is sent to the CGA.
- The CGA generates the certificate.
- The certificate info is imported into the TOE.
-

Signature Creation in the usage phase,

- The signatory enters his PIN code (VAD) to authenticate himself to the TOE.
- The signatory sends the DTBS or DTBS representation to the TOE.
- The TOE computes the Signature.
- The TOE sends the Signature to the SCA

As a summary description of how the parts of the TOE are delivered to the final customer, the IAS Classic v5.2.1 application is delivered conjointly with the MultiApp platform in form of a smart card, inlay or module form factor. The form factor is packaged on Thales’s manufacturing facility and sent to final customer premises.

© Copyright Thales

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 Thales's Technical representative.

2.3.3 Involved Thales-DIS sites

- **Development and Project Managment**
  - La Ciotat (France)
    - CC project management
  - Singapore & Meudon (France)
    - Platform & eTravel & IAS development

- **Manufacturing**
  - Gémenos, Singapore, Vantaa, Tczew, Curitiba, Chanhassen

- **IT activities**
  - Gémenos, Calamba, Les Clayes, Marcoussis, Pune

2.3.4 TOE Delivery

The TOE is delivered as a whole package with the Platform (MultiApp v5.1). There is no distinction between the delivery of the platform MultiApp v5.1 and this TOE. Please refer to section 2.6.2.2 on the platform Security Target [ST-PLTF].

Regarding the documentation to be delivered, a part from the one described on section 2.5.4 of the platform Security Target [ST-PLTF], the documentation found on [AGD] accompanies this TOE. The documentation is delivered in form of electronic documents (*.pdf) by Thales's Technical representative via a secure file sharing platform download action.

Item type	Item	Reference/Version	Form of delivery
Document	IAS Classic v5.2.1, Reference Manual	D1542053C October 26, 2022	Electronic document via secure file download
Document	IAS Classic v5.2.1, Personalization Profiles Guide	D1546633B September 20, 2022	Electronic document via secure file download
Document	AGD OPE - PRE document – IAS Classic v5.2.1	D1588538, Rev 1.4 03/05/2023	Electronic document via secure file download
Document	BioPIN Manager V3.0 Reference Manual	D1481720E June 25th, 2021	Electronic document via secure file download
Document	MultiApp Guidance Document - Guidance document for secure development for MultiApp products	D1539156, Rev 1.2 2023-03-24	Electronic document via secure file download

© Copyright Thales

3. CONFORMANCE CLAIMS

3.1 CC CONFORMANCE CLAIM

This security target claims conformance to

- [CC-1]
- [CC-2]
- [CC-3]

as follows

- Part 2 extended,
- Part 3 conformant.

The [CEM] has to be taken into account.

The evaluation of the TOE uses the result of the CC evaluation of the platform MultiApp V5.1 claiming conformance to [PP-JCS-Open].

3.2 PP CLAIM

This MultiApp V5.1 IAS security target claims strict conformance to the following Protection Profiles:

- [PP-SSCD-KG TCCGA TCSCA] including [PP-SSCD-KG], which defines security requirements for an SSCD with SCD/SVD key generation and signature creation, with extension [EN-419211-4] related to trusted communication between SSCD and CGA and extension [EN-419211-5] related to trusted communication between SSCD and SCA.
- [PP-SSCD-KI TCSCA] including [PP-SSCD-KI], which defines security requirements for an SSCD with SCD key import and signature creation with extension [EN-419211-6] related to trusted communication between SSCD and SCA.

The evaluation is a composite evaluation and uses the results of the CC evaluation of the MultiApp V5.1 platform. The platform embedded software has been evaluated at level EAL 5+.
The security problem definition, the objectives, and the SFR of the platform are not described in this document but in [ST-PLTF].

The MultiApp V5.1 JCS security target [ST-PLTF], claims demonstrable conformance to the Protection Profile “JavaCard System – Open configuration”, Version 3.1 ([PP-JCS-Open]).

3.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [CC-3].

© Copyright Thales

4. SECURITY PROBLEM DEFINITION

4.1 GENERAL

The assets, threats, OSP, and assumptions of the TOE are those defined in [PP-SSCD-KG], [PP-SSCD-KI] (no additional assets, threats, OSP, and assumptions in extension [EN 419211-4], [EN 419211-5], [EN 419211-6]). The present Security Target deals with the assets, threats, OSP, and assumptions of [PP-SSCD-KG] and [PP-SSCD-KI].
The assets of [PP-JCS-Open] are studied in [ST-PLTF].

The Common Criteria define assets as entities that the owner of the TOE presumably places value upon. The term “asset” is used to describe the threats in the operational environment of the TOE.

Assets and objects:

1. SCD: 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.

2. SVD: 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.

3. DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.

User and subjects acting for users:

1. 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.

2. Administrator: 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.

3. Signatory: User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.

Threat agents:

1. Attacker: human or process acting on his 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.

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

© Copyright Thales

T.SVD_Forgery *Forgery of 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-representation*

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.

4.3 ORGANIZATIONAL SECURITY POLICIES

The Secure Signature Creation Device usage is for advanced electronic signature. So it is mandatory to follow the organisational security policy proposed by [PP-SSCD-KG] and [PP-SSCD-KI].

P.CSP_QCert *Qualified certificate*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (see previous directive 1999/93 article 2, clause 9, and Annex I or new [Regulation EU], article 3, clause 14, 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. previous directive 1999/93 article 1, clause 2 or new [Regulation EU],, Article 3, clause 11), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the previous directive 1999/93 Annex I or new [Regulation EU], Annex I)[1].
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 his sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

P.Sigy_SSCD *TOE as secure signature-creation device*

The TOE meets the requirements for an SSCD laid down in Annex III of the previous directive 1999/93 or in Annex II of the new [Regulation EU]]. This implies the SCD is used for signature creation under sole control of the signatory and the SCD can practically occur only once.

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

© Copyright Thales

P.Sig_Non-Repud *Non-repudiation of signatures*

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

P.Pre-perso_authentication *Strong authentication in pre-personalisation*

During pre-personalisation, The TOE protects itself with strong authentication.

4.4 ASSUMPTIONS

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

A.CGA *Trustworthy certification-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 the data the signatory wishes to sign in a form appropriate for signing by the TOE.

A.CSP *Secure SCD/SVD management by CSP*

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

Assumptions coming from the platform:

A.CAP_FILE

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.

A.Insp_Sys Inspection Systems for global interoperability

The Extended Inspection System (EIS) for global interoperability (i) implements at least the terminal part of PACE [ICAO-TR-SAC]. If several protocols are supported by the EIS, PACE secure channel must be established and applicative data (e.g. the logical travel document) must be transferred under PACE. Other operations may be done when additional protocols are supported by the terminal.

4.5 JUSTIFICATIONS FOR ADDING ASSUMPTIONS ON THE ENVIRONMENT

4.5.1.1 Additions coming from the Platform

The only additional assumptions on the environment are A.CAP_FILE, A.VERIFICATION and A.Insp_Sys. These assumptions deal with the assumptions linked to application loading on the Open Platform of the TOE. The others assumptions from the Platform are not relevant in this composite TOE. Therefore, the added assumption does not weaken the TOE.

© Copyright Thales

5. SECURITY OBJECTIVES

5.1 GENERALS

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.
The security objectives of the TOE are those defined in [PP-SSCD-KG], [PP-SSCD-KI] and updated regarding related extension [EN-419211-4], [EN 419211-5], [EN 419211-6]
The present Security Target deals with security objectives of [PP-SSCD-KG] and [PP-SSCD-KI] and updated regarding related extension [EN-419211-4], [EN 419211-5], [EN 419211-6]
.
The security objectives stated in [PP-JCS-Open] can be found in [ST-PLTF].

5.2 SECURITY OBJECTIVES FOR THE TOE

5.2.1 Common to [EN-419211-2] Part 2 and [EN-419211-3] Part 3

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.

OT.SCD_Secrecy *Secrecy of signature-creation data*

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

OT.Sig_Secure *Cryptographic security of the electronic signature*

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

OT.Sigy_SigF *Signature generation 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 resists physical tampering with specified system devices and components.

© Copyright Thales

5.2.2 [EN-419211-2] Part 2 specific

OT.SCD/SVD_Auth_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 can 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 a digital signature creation with the SCD.

5.2.3 [EN-419211-3] Part 3 specific

OT.SCD_Auth_Imp *Authorised SCD import*

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

5.2.4 [EN-419211-4] Part 4 specific (additional security objectives related to part 2)

OT.TOE_SSCD_Auth *Authentication proof as SSCD*

The TOE shall hold unique identity and authentication data as SSCD and provide security mechanisms to identify and to authenticate itself as SSCD.

OT.TOE_TC_SVD_Exp *TOE trusted channel for SVD export*

The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the TOE.

5.2.5 [EN-419211-5] Part 5 and [EN-419211-6] part 6 extension (additional security objectives related to [EN-419211-2] part 2 & [EN-419211-3] part 3)

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.

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.

5.2.6 Extensions

OT.Pre-perso_authentication *Strong authentication in pre-personalisation*

During pre-personalisation, The TOE protects itself with strong authentication.

5.3 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

5.3.1 Common to [EN-419211-2] Part 2 and [EN-419211-3] Part 3

OE.SVD_Auth *Authenticity of the SVD*

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

OE.CGA_Qcert *Generation of qualified certificates*

The CGA shall generate a qualified certificate that includes,(amongst others)
(a) the name of the signatory controlling the TOE,
(b) the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
(c) the advanced signature of the CSP.
The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a SSCD.

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

The signatory shall use a trustworthy SCA that
(a) 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,
(b) sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
(c) attaches the signature produced by the TOE to the data or provides it separately.

OE.Signatory *Security obligation of the Signatory*

The Signatory checks that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The Signatory keeps their VAD confidential.

5.3.2 [EN-419211-3] Part 3 specific

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.
Remark : This Objective is specific to part 3 due to the adding of part 4.

OE.SCD/SVD_Auth_Gen *Authorized SCD/SVD generation*

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

OE.SCD_Secrecy *SCD Secrecy*

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

OE.SCD_Unique *Uniqueness of the signature-creation data*

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

OE.SCD_SVD_Corresp *Correspondence between SVD and SCD*

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

5.3.3 [EN-419211-4] Part 4 specific (additional security objectives related to part 2)

Part 4 substitutes OE.SSCD_Prov_Service from the core PP(part 2) by OE.Dev_Prov_Service and adds security objectives for the operational environment OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp in order to address the additional method of use as SCD/SVD pair generation after delivery to the signatory and outside the secure preparation environment.

OE.Dev_Prov_Service *Authentic SSCD provided by SSCD Provisioning Service*

The SSCD Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, personalises the TOE for the legitimate user as signatory, links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the signatory. Note: This objective replaces OE.SSCD_Prov_Service from the core PP, which is possible as it does not imply any additional requirements for the operational environment when compared to OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_Service).

OE.CGA_SSCD_Auth *Pre-initialisation of the TOE for SSCD authentication*

The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSCD, successfully proved this identity as SSCD to the CGA, and whether this identity is linked to the legitimate holder of the device as applicant for the certificate.

OE.CGA_TC_SVD_Imp *CGA trusted channel for SVD import*

The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the SSCD.

The developer prepares the TOE by pre-initialisation for the delivery to the customer (i.e. the SSCD provisioning service) in the development phase not addressed by a security objective for the operational environment. The SSCD Provisioning Service performs initialisation and personalisation as TOE for the legitimate user (i.e. the Device holder). If the TOE is delivered to the Device holder with SCD the TOE is a SSCD. This situation is addressed by OE.SSCD_Prov_Service except the additional initialisation of the TOE for proof as SSCD and trusted channel to the CGA. If the TOE is delivered to the Device holder without a SCD the TOE will be a SSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the signatory in the operational use stage the TOE provides additional security functionality addressed by OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp. But this security functionality must be initialised by the SSCD Provisioning Service as described in OE.Dev_Prov_Service. Therefore this PP (part4) substitutes OE.SSCD_Prov_Service by OE.Dev_Prov_Service allowing generation of the first SCD/SVD pair after delivery of the TOE to the Device holder and requiring initialisation of security functionality of the TOE. Nevertheless the additional security functionality must be used by the operational environment as described in OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp. This approach does not weaken the security objectives of and requirements to the TOE but enforce more security functionality of the TOE for additional method of use. Therefore it does not conflict with the CC conformance claim to the core [PP_SSCD_KG]

5.3.4 [EN-419211-5] Part 5 and [EN-419211-6] part 6 extension (additional security objectives related to [EN-419211-2] part 2 & [EN-419211-3] part 3)

Part 5 and part 6 substitute OE.HID_VAD from the core PP by OE.HID_TC_VAD_Exp and OE.DTBS_Protect from the core PP by OE.SCA_TC_DTBS_Exp

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.

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.

© Copyright Thales

5.3.5 Objectives of Environments coming From MultiApp V5.1 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.CAP_FILE

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.
For application code loaded post-issuance and partially or entirely verified on-card, technical measures must ensure that the verification required in OE.VERIFICATION are performed. On-card bytecode verifier is out of the scope of this Protection Profile.

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.

OE.Prot_Logical_Data Protection of TOE and applicative data

The inspection system of the applicative entity (e.g. receiving State or Organisation) ensures the confidentiality and integrity of the data read from the TOE and applicative data (e.g. logical travel document). The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established.

OE.Personalisation Personalisation of TOE and application data requiring PACE usage

The Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the applicative user (e.g. travel document holder) and create the accurate applicative data* and write them in TOE.

Note: in the specific case of MRTD, accurate applicative data are biographical data for the travel document), (ii) biometric reference data of the travel document holder, the initial TSF data, (the Document Security Object defined in [ICAO-9303] (in the role of a DS).

OE.Terminal Terminal operating
The terminal operators must operate their terminals as follows:

1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in as defined in [ICAO-9303].

2.) The related terminals implement the terminal parts of the PACE protocol [ICAO-TR-SAC], of the Passive Authentication [ICAO-TR-SAC] (by verification of the signature of the Document Security Object) and use them in this order (This order is commensurate with [ICAO-TR-SAC]. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

© Copyright Thales

3.) The related terminals need not to use any own credentials.

4.) The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [ICAO-9303]).

5.) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

OE.User_Obligations User Obligations

The application user (e.g. travel document holder) may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

Other security objectives for Operational environment from [PP_EAC2] are specific to travel document and are not copied here.

5.4 SECURITY OBJECTIVE RATIONALE

Threats – Assumption – Policies / Security Objectives	OT.Lifestyle_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-Unique	OT.SCD_SVD_Corresp	OT.SCD_Auth_Imp	OT.Pre-perso_authentication	OT.TOE_SSCD_Auth (part 4)	OT.TOE_TC_SVD_Exp (part 4)	OT.TOE_TC_VAD_Imp (part 5&6)	OT.TOE_TC_DTBS_Imp (part 5&6)	OE.SVD_Auth	OE.CGA_QCert	OE.DTBS_Intend	OE.Signatory	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.Dev_Prov_Service (part 4) replace	OE.SSCD_Prov_Service (part 2)	OE.CGA_SSCD_Auth (part 4)	OE.CGA_TC_SVD_Imp (part 4)	OE.HID_TC_VAD_Exp (part 5 & 6) replace	OE.SCA_TC_DTBS_Exp (part 5&6) replace	OE.DTBS_Protect	OE.CAP_FILE	OE.VERIFICATION	OE.Prot_Logical_Data	OE.CODE-EVIDENCE	OE.Personalisation	OE.Terminal	OE.User_Obligations
T.SCD_Divulg		X										X										X	X															
T.SCD_Derive			X						X															X														
T.Hack_Phys		X				X	X	X																														
T.SVD_Forgery											X				X			X							X				X									
T.SigF_Misuse	X			X	X											X	X			X	X								X	X	X						
T.DTBS_Forgery					X												X			X											X	X			X	X	X
T.Sig_Forgery			X							X									X					X													
P.CSP_Qcert	X										X	X		X					X			X			X				X								
P.Qsign			X	X															X	X																	

P.Sigy_SSCD	X	X	X	X	X	X		X	X	X		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	X	X	X			X									
P.Pre-perso_authentication													X																													
A.SCA																				X																						
A.CGA																		X	X																							
A.CSP																						X	X	X	X																	
A.CAP_FILE																																									
A.VERIFICATION																																									
A.Insp_Sys																																									

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

5.4.1 Threats

T.SCD_Divulg (*Storing, copying and releasing of the signature creation data***)** addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in recital (18) of the previous directive 1999/93 or in Annex II of [Regulation EU], . This threat is countered by:

- OT.SCD_Secrecy, which assures the secrecy of the SCD during use by the TOE for signature creation,
- OE.SCD_Secrecy, which assures the secrecy of the SCD in the CSP environment (when SCD is generated off-TOE),

Furthermore, generation and/or import of SCD known by an attacker is countered by:

- OE.SCD/SVD_Auth_Gen, which ensures that only authorized SCD generation in the environment is possible (when SCD is generated off-TOE), and
- OT.SCD_Auth_Imp, which ensures that only authorised SCD import is possible (when SCD is generated off-TOE).

T.SCD_Derive (*Derive the signature creation data***)** 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 (when SCD is generated on-TOE).
OE.SCD_Unique counters this threat by implementing cryptographically secure generation of the SCD/SVD pair (when SCD is generated off-TOE).
OT.Sig_Secure ensures cryptographically secure electronic signatures.

T.Hack_Phys (*Exploitation of physical vulnerabilities***)** deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. OT.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 (*Forgery of the signature verification data***)** deals with the forgery of the SVD exported by the TOE to the CGA for certificate generation. T.SVD_Forgery 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 (when SCD is generated on-TOE),
- OE.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 (when SCD is generated off-TOE), and
- OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA and verification of the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

- (This is specific to [PP SSCD KG] extended with part 4.) Additionally T.SVD_Forgery is addressed by OT.TOE_TC_SVD_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA_TC_SVD_Imp, which provides verification of SVD authenticity by the CGA.

T.SigF_Misuse (*Misuse of the signature creation function of the TOE*) addresses the threat of misuse of the TOE signature creation function to create 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

© Copyright Thales

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 (*Forgery of the DTBS/R*) 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. In addition, OE.Personalisation, OE.Terminal and OE.User_Obligations contribute to secure exchange between the TOE and the terminal.

T.Sig_Forgery (*Forgery of the electronic signature***)** 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 (when SCD is generated on-TOE) or OE.SCD_Unique (when SCD is generated off-TOE) 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.

5.4.2 Organisational security policies

P.CSP_QCert (*CSP generates qualified certificates*)
Dedicated to [PP SSCD KI]
establishes the CSP generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD under sole control of his signatory. P.CSP_QCert is addressed by

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- OT.SCD_SVD_Corresp (when SCD is generated on-TOE) or OE.SCD_SVD_Corresp (when SCD is generated off-TOE), which requires to ensure the correspondence between the SVD and the SCD during their generation,
- 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.
- OE.SCD/SVD_Auth_Gen, which ensures that the SCD/SVD generation can be invoked by authorized users only (when SCD is generated off-TOE),
- OT.SCD_Auth_Imp which ensures that authorised users only may invoke the import of the SCD (when SCD is generated off-TOE).

Dedicated to [PP SSCD KG] extended with part 4
provides that the TOE and the SCA may be employed to sign data with (qualified) electronic signatures, as defined by previous directive 1999/93 (article 5, paragraph 1) or in the new [Regulation EU], (article 25) refers to SSCDs to ensure the functionality of advanced signatures. The OE.CGA_QCert addresses the requirement of qualified (or advanced) electronic signatures as being based on qualified (or non-qualified) certificates. According to OT.TOE_SSCD_Auth the copies of the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD to prove this identity as SSCD to the CGA. The OE.CGA_SSCD_Auth ensures that the SP checks the proof of the device presented of the applicant that it is a SSCD. The OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE to the CGA corresponds to the SCD stored in the TOE and used by the signatory. The OT.Lifecycle_Security ensures that the TOE detects flaws during the initialisation, personalisation and operational usage.

P.QSign (*Qualified electronic signatures*) 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

© Copyright Thales

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 (*TOE as secure signature creation device*) requires the TOE to meet Annex III of the previous directive 1999/93 or Annex II of the new [Regulation EU],
Dedicated to [PP SSCD KI]
This is ensured as follows

- OE.SCD_Unique meets the paragraph 1(a), Annex III of the previous directive 1999/93 or paragraph 1(b) of the new [Regulation EU], Annex II, by the requirements
that the SCD used for signature creation can practically occur only once.
- OE.SCD_Unique, OT.SCD_Secrecy and OE.SCD_Secrecy meet the paragraph 1(a), Annex III of previous directive 1999/93 ot the paragraph 1(a) of the new [Regulation EU],, Annex II, by the requirements to ensure the secrecy of the SCD.
OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of SCD against specific attacks.
OT.SCD_Secrecy and OT.Sig_Secure meet the paragraph 1(b), Annex III of the previous directive 1999/93 or paragraph 1(c) of the new [Regulation EU], Annex II, by
the requirements to ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE.
- OT.Sigy_SigF and OE.SCD_Secrecy meet the paragraph 1(c), Annex III of the previous directive 1999/93 or paragraph 1(d) of the new [Regulation EU],], Annex II, 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 the paragraph 2, Annex III of **the** previous directive 1999/93 or paragraph 2 of the new [Regulation EU], Annex II,
The TOE must not alter the DTBS/R.

Please take note, the requirements of previous directive 1999/93 Annex III, 2 or the new [Regulation EU], Annex II, 2., that the 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 them to the SSCD for signing.

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

- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialisation, personalisation and operational usage
- OE.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only,
- OT.SCD_Auth_Imp, which limits SCD import to authorised users only,
- OE.SCD_Secrecy, which ensures the confidentiality of the SCD during generation and export to the TOE, and deletes the SCD after export to the TOE. The CSP does not use the SCD for signature creation.
- 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 as SSCD from the SSCD-provisioning service.

Dedicated to [PP SSCD KG] extended with part 4
The paragraph 1(a) of Annex III is ensured by OT.SCD_Unique requiring that the SCD used for signature creation can practically occurs only once. The OT.SCD_Secrecy OT.Sig_Secure and OT.EMSEC_Design and OT.Tamper_Resistance address the secrecy of the SCD (cf. paragraph 1(a) of Annex III). OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III by the requirements 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. The usage of SCD under sole control of the signatory is ensured by OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen and OT.Sigy_SigF.

OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised TOE from an SSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the

TOE as SSCD. If the TOE is delivered to the legitimate user without SCD In the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA_SSCD_Auth and the received SVD is sent by this SSCD as required by OE.CGA_TC_SVD_Imp. Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

P.Sig_Non-Repud (*Non-repudiation of signatures***)**
[PP SSCD KI] & [PP SSCD KG] extended with part 5 and part 6
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 (when SCD is generated on-TOE) or OE.SCD_SVD_Corresp (when SCD is generated off-TOE) ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. OT.SCD_Unique (when SCD is generated on-TOE) or OE.SCD_Unique (when SCD is generated off-TOE) 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). The TOE security feature addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp supported by OE.Dev_Prov_Service enables the verification whether the device presented by the applicant is a SSCD as required by OE.CGA_SSCD_Auth and the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA_TC_SVD_Imp. 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 generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may generate 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.

Dedicated to [PP SSCD KG] extended with part 4
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, that ensure the aspects of signatory's sole control over and responsibility for the electronic signatures generated with the TOE. OE.Dev_Prov_Service ensures that the signatory uses an authentic TOE, initialised and personalised for the signatory. 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). The TOE security feature addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp supported by OE.Dev_Prov_Service enables the verification whether the device presented by the applicant is a SSCD as required by OE.CGA_SSCD_Auth and the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA_TC_SVD_Imp. 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 generates

electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may generate 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.

P.Pre-perso_authentication **(***Strong authentication in pre-personalisation)* requests a strong authentication before accessing the SSCD. This is directly addressed by OT.Pre-perso_authentication.

5.4.3 Assumptions

A.SCA *(Trustworthy signature creation application)* 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.CGA *(Trustworthy certificate generation application)* establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert (Generation of qualified certificates), which ensures the generation of qualified certificates, and by OE.SVD_Auth (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.CSP (*Secure SCD/SVD management by CSP*) establishes several security aspects concerning handling of SCD and SVD by the CSP. That the SCD/SVD generation device can only be used by authorized users is addressed by OE.SCD/SVD_Auth_Gen (Authorized SCD/SVD Generation), that the generated SCD is unique and cannot be derived by the SVD is addressed by OE.SCD_Unique (Uniqueness of the signature creation data), that SCD and SVD correspond to each other is addressed by OE.SCD_SVD_Corresp (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are deleted in the environment once exported to the TOE is addressed by OE.SCD_Secrecy (SCD Secrecy).
This assumption is only applicable when SCD is generated off-card.

Assumptions coming from the Platform

A.CAP_FILE This assumption is upheld by the security objective for the operational environment OE.CAP_FILE 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.

A.Insp_Sys This assumption is upheld by the security objective for the environment OE.Prot_Logical_Data which ensures that the data read from the TOE and the applicative data are protected in confidentiality and integrity thanks to the establishment of secure messaging.

5.4.4 Compatibility between objectives of [ST-IAS] and [ST-PLTF]

5.4.4.1 Compatibility between objectives for the TOE

The following table lists the relevant security objectives of the platform 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.SID	The TOE shall uniquely identify every subject (applet, or package) before granting it access to any service.	OT.SCD/SVD_Auth_Gen, OT.SCD_Auth_Imp, OT.TOE_SSCD_Auth
O.CIPHER	The TOE shall provide a means to cipher sensitive data for applications in a secure way	OT.TOE_TC_SVD_Exp, 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.Lifecycle_Security, OT.SCD/SVD_Auth_Gen, OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.SCD_Auth_Imp 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
O.GLOBAL_ARRAYS_INTEG	The TOE shall ensure that no application can store a reference to the APDU buffer, a global byte array created by the user through makeGlobalArray method and the byte array used for invocation of the install method of the selected applet	No direct link with the composite product security objectives, but these platform security objectives are 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.ARRAY_VIEWS_CONFID	The TOE shall ensure that no application can read elements of an array view not having array view security attribute ATTR_READABLE_VIEW. The TOE shall ensure that an application can only read the elements of the array view within the bounds of the array view.	
O. ARRAY_VIEWS_INTEG	The TOE shall ensure that no application can write to an array view not having array view security attribute ATTR_WRITABLE_VIEW. The TOE shall ensure that an application can only write within the bounds of the array view.	
O.PIN-MNGT	The TOE shall provide a means to securely manage PIN objects.	OT.SCD/SVD_Auth_Gen, OT.SCD_Auth_Imp, OT.TOE_TC_VAD_Imp
O.OPERATE	The TOE must ensure continued correct operation of its security functions.	OT.Lifecycle_Security, OT.Tamper_ID, OT.Tamper_rsistance
O.ALARM	The TOE shall provide appropriate feedback information upon detection of a potential security violation	OT.Lifecycle_Security, OT.Tamper_ID, OT.Tamper_rsistance
O.OBJ-DELETION	The TOE shall ensure the object deletion shall not break references to objects.	OT.Lifecycle_Security
O.SCP. RECOVERY	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.Tamper_ID, OT.Tamper_Resistance
O.SCP.SUPPORT	The SCP shall support the TSFs of the TOE	OT.TOE_TC_VAD_Imp, OT.TOE_TC_DTBS_Imp, OE.SCD_Secrecy, OE.HID_TC_VAD_Exp, OE.SCA_TC_DTBS_Exp
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.
O.SECURE_LOAD_ACODE		Not relevant for this composite product security objectives. The OS agility mechanism is fully managed by the platform.
O.SECURE_AC_ACTIVATION		
O.TOE_IDENTIFICATION		
O.CONFID-OS-UPDATE.LOAD		

Table 3: Compatibility with platform Security objectives

The other objectives (O.FIREWALL, O.NATIVE, O.RNG, O.LOAD, O.INSTALL, O.DELETION, O.TRANSACTION, O.RESOURCES, O.CARD-MANAGEMENT) of the platform are not relevant for this composite TOE or are directly handle by the Platform itself.

Platform PACE Module objective label	**PACE Module Platform objective short description (refer to [ST-PLTF] for the full description)**	**Link to the composite-product**
OT.Data_Integrity	The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying).The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected	OT.DTBS_Integruty_TOE, OT.TOE_TC_SVD_Exp, OT.TOE_TC_VAD_Imp, OT.TOE_TC_DTBS_Imp, OE.HID_TC_VAD_Exp, OE.SCA_TC_DTBS_Exp
OT.Data_Authenticity	The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side .The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected	OE.HID_TC_VAD_Exp, OT.TOE_SSCD_Auth, OT.TOE_TC_VAD_Imp
OT.Data_Confidentiality	The TOE must ensure confidentiality of the User Data and the TSF data by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected	OE.HID_TC_VAD_Exp, OT.TOE_TC_VAD_Imp
OT.Identification	The TOE must provide means to store Initialisation and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the application data requiring PACE usage	No direct link with the composite product security objectives, but this platform security objective is used to endure the security of the composite TOE.
OT.AC_pers	Access Control for Personalisation of TOE and Applicative data	OT.Pre-perso_authentication
OT.Prot_Abuse_Func	The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE	OT.Lifecycle_Security
OT.Prot_Inf_Leak	The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the TOE	OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, OT.Sig_Secure

© Copyright Thales

OT.Prot_Phys_Tamper	The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the TOE's Embedded Software	OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance
OT.Prot_Malfunction	The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE	OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance

Table 4: Compatibility with platform PACE Security objectives

The other patch loading objectives (O.SECURE_LOAD_ACODE, O.SECURE_AC_ACTIVATION, O.TOE_IDENTIFICATION, O.CONFID-OS-UPDATE.LOAD) of the platform are not relevant for this composite TOE or are directly handle by the Platform itself.

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

5.4.4.2 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.SCD/SCD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OE.Dev_Prov_Service,, OE.CGA_SSCD_Auth, OE.CGA_TC_SVD_Imp and OE.SCD_SVD_Corresp, OE.HID_TC_VAD_Exp, OE.SCA_TC_DTBS_Exp are objectives specific to [ST-IAS] and they do no conflict with the objectives of [ST-PLTF].

OE.SCP.SUPPORT, OE.SCP.RECOVERY, OE.CARD-MANAGEMENT, OE.PERSONALISATION, OE.TERMINAL OE.USER_OBLIGATIONS, OE.VERIFICATION, OE.CODE-EVIDENCE and OE.CAP_FILE are objectives specific to the Java Card platform and they do no conflict with the objectives of [IFX-IC].

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

5.4.5 Justifications for adding & substitution objectives on the environment

5.4.5.1 Additions from the platform

Additional objectives on the environment coming from the platform are: OE.VERIFICATION, OE.CAP_FILE, OE.CODE-EVIDENCE and OE.PROT_LOGICAL_DATA, OE.PERSONALISATION, OE.TERMINAL and OE.USER_OBLIGATIONS are linked to trust the application installation and execution in the Open platform of the TOE.
Therefore the added objectives on the environment do not weaken the TOE.

5.4.5.2 Substitution

Part 5 and part 6 substitute OE.HID_VAD from the core PP by OE.HID_TC_VAD_Exp and OE.DTBS_Protect from the core PP by OE.SCA_TC_DTBS_Exp. These do not weaken the TOE.

6. EXTENDED COMPONENTS DEFINITION

This ST uses two components defined as extensions to CC part 2:

- FPT_EMS.1 which is defined in [PP-SSCD-KG] and [PP-SSCD-KI].
- FIA_API.1 which is defined in [EN-419211-4].

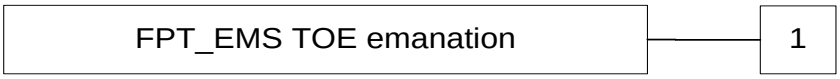
6.1 DEFINITION OF THE FAMILY FPT_EMS

The sensitive 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 TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [CC-2].

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

Family behaviour
This family defines requirements to mitigate intelligible emanations.

Component levelling:



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.

Management: FPT_EMS.1
There are no management activities foreseen.

Audit: FPT_EMS.1
There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components
Dependencies: No dependencies.

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*].

© Copyright Thales

6.2 DEFINITION OF THE FAMILY FIA_API

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

FIA_API Authentication Proof of Identity

Family behaviour

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component levelling:

FIA_API.1 Authentication Proof of Identity:

Management: FIA_API.1
The following actions could be considered for the management functions in FMT:
Management of authentication information used to prove the claimed identity.
activities foreseen.

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components
Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

7. SECURITY REQUIREMENTS

7.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

This chapter defines the security functional requirements for the TOE using functional requirements components as specified in [PP-SSCD-KI], [PP-SSCD-KG]
and [EN-419211-4] adding an operation of FIA_UAU.1 and adding SFRs: FIA_API.1, FDP_DAU.2/SVD, FTP_ITC.1/SVD.
and [EN-419211-5] & [EN-419211-6] adding an operation of FIA_UAU.1 and adding SFRs: FDP_UIT.1/DTBS, FTP_ITC.1/VAD and FTP_ITC.1/DTBS

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

Refinements in this section are underlined when they are PP refinements and in bold characters when they are additional ones.

For this section, a presentation choice has been selected. Each SFR present a table with different type of algorithms treated. For each case, there is no distinction regarding the technical objectives fulfilled by each row on the table (thus algorithm family). The technical objectives are the same disregarding this differentiation.

7.1.1 Class Cryptographic Support (FCS)

FCS_CKM.1/SCD Cryptographic key generation for SCD/SVD pair

Hierarchical to:	No other components
Dependencies:	[FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 /SCD	The TSF shall generate SCD/SVD pair in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [*assignment: list of standards*].

Algorithm type	algorithm	Key size	standards
/RSA	**RSA CRT key generation**	**1024, 1536, 2048,3072,4096**	**ANSI X9.31**
/ECC	**ECC key generation**	**160, 224, 256, 384, 512, 521**	**ANSI X9.62**

Table 5: FCS_CKM.1/SCD iteration explanation

Application note: part 2 only [PP-SSCD-KG].
Application note:
FCS_CKM.1/SCD is named FCS_CKM.1 in [PP-SSCD-KG]. This naming clarified the purpose of the SFR and allows for the introduction of FCS_CKM.1/SCD.

FCS_CKM.1/Session Cryptographic key generation for session keys

Hierarchical to:	No other components
Dependencies:	[FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 /Session: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [*assignment: list of standards*].

Algorithm type	algorithm	Key size	standards
/TDES	**TDES session key generation**	**112**	**[ISO7816], [PKCS#3] DH.**
/AES	**AES session key generation**	**128, 192, 256**	**[ISO7816], [PKCS#3] DH, [IEEE-P1363] ECDH, [IEEE-P1363] ECDHC**

Table 6: FCS_CKM.1/Session iteration explanation

FCS_CKM.4/SCD Cryptographic key destruction

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

FCS_CKM.4.1 /SCD: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: **method from the underlying platform** that meets the following: **No standard**

Algorithm type	when
/RSA	new SCD generation or import /signer's will
/ECC	new SCD generation or import /signer's will

Table 7: FCS_CKM.4 iteration explanation

Application note: part 2 only [PP-SSCD-KG].
Application note:
FCS_CKM.4/SCD is named FCS_CKM.4 in [PP-SSCD-KG]. This naming clarified the purpose of the SFR and allows for the introduction of FCS_CKM.4/SCD.

FCS_CKM.4/Session Cryptographic key destruction

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

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

Algorithm type	when
/TDES	End of session
/AES	End of session

Table 8: FCS_CKM.4/Session iteration explanation

FCS_COP.1/DSC Cryptographic operation – Digital Signature Creation

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

FCS_COP.1.1 /DSC The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [*assignment: list of standards*].

Algorithm type	operation	algorithm	key size	standards
/DSC-RSA	signature	**RSA CRT**	**1024, 1536, 2048, 3072, and 4096**	**[ISO9796-2]** **RSA SHA PKCS#1 v1.5** **RSA PSS SHA PKCS#1**
/DSC-ECC	signature	**ECC**	**224, 256, 384, 512, and 521**	**[TR-03111] ECDSA SHA**

Table 9: FCS_COP.1/DSC iteration explanation

Application note: part 2 only [PP-SSCD-KG].
Application note:
FCS_COP.1/DSC is named FCS_COP.1 in [PP-SSCD-KG]. This naming clarified the purpose of the SFR and allows for the introduction of FCS_COP.1/DSC.

FCS_COP.1/Session Cryptographic operation – Other operations

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

FCS_COP.1.1 The TSF shall perform [*assignment: cryptographic operations*] in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [*assignment: list of standards*].

Algorithm type	operation	algorithm	key size	standards
/ENC-TDES	**Encryption & decryption**	**TDES**	**112**	**[SP800-67]**
/ENC-AES	**Encryption & decryption**	**AES**	**128, 192, 256**	**[FIPS197] AES 128 NOPAD**
/MAC-TDES	**MAC computation & Verification**	**TDES**	**112**	**[SP800-67] [ISO9797-1]** **DES MAC ISO9797-1 M2**
/MAC-AES	**MAC computation & Verification**	**AES**	**128,192, 256**	**[FIPS197] AES 128 NOPAD**

Table 10: FCS_COP.1/Session 'Other operations' iteration explanation

7.1.2 Class FDP User Data Protection

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
SVD	No security attribute	NA

Table 11: Subjects and security attributes for access control

FDP_ACC.1/Signature_Creation Subset access control

Hierarchical to: No other components
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 /Signature_Creation: The TSF shall enforce the Signature Creation SFP to objects based on the following:
1. Subjects: S.User,
2. Objects: DTBS/R, SCD
3. Operations: signature creation.

FDP_ACF.1/Signature_Creation Security attribute based access control

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

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

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

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

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

FDP_ACC.1/SCD/SVD_Generation Subset access control

Hierarchical to: No other components
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 /SCD/SVD_Generation: The TSF shall enforce the SCD/SVD Generation SFP to objects based on the following:
1. Subjects: S.User,
2. Objects: SCD, SVD
3. Operations: generation of SCD/SVD pair.

Application note: part 2 only [PP-SSCD-KG].

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

Hierarchical to: No other components

Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 /SCD/SVD_Generation	The TSF shall enforce the SCD/SVD Generation SFP to objects based on the following: the user S.User is associated with the security attribute “SCD/SVD Management“.
FDP_ACF.1.2 /SCD/SVD_Generation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute “SCD/SVD Management” set to “authorized” is allowed to generate SCD/SVD pair,
FDP_ACF.1.3 /SCD/SVD_Generation	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4 /SCD/SVD_Generation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute “SCD/SVD management” set to “not authorised” is not allowed to generate SCD/SVD pair.

Application note: part 2 only [PP-SSCD-KG].

FDP_ACC.1/SVD_Transfer Subset access control

Hierarchical to:	No other components
Dependencies:	FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 /SVD_Transfer	The TSF shall enforce the SVD Transfer SFP to objects based on the following: 1. Subjects: S.User, 2. Objects: SVD 3. Operations: export.

Application note: part 2 only [PP-SSCD-KG].

FDP_ACF.1/SVD_Transfer Security attribute based access control

Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 /SVD_Transfer	The TSF shall enforce the SVD Transfer SFP to objects based on the following: 1. the S.User is associated with the security attribute Role 2. the SVD .
FDP_ACF.1.2 /SVD_Transfer	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Admin or R.Sigy is allowed to export SVD,
FDP_ACF.1.3 /SVD_Transfer	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4 /SVD_Transfer	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none

Application note: part 2 only [PP-SSCD-KG].

FDP_ACC.1/SCD_Import Subset access control

Hierarchical to:	No other components
Dependencies:	FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 /SCD_Import	The TSF shall enforce the SCD Import SFP to objects based on the following: 1. Subjects: S.User, 2. Objects: SCD 3. Operations: import of SCD.

Application note: part 3 only [PP-SSCD-KI].

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1)” as specified below (Common Criteria Part 2).

FDP_ACF.1/SCD_Import Security attribute based access control

Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 /SCD_Import	The TSF shall enforce the SCD Import SFP to objects based on the following: the S.User is associated with the security attribute “SCD/SVD Management”.
FDP_ACF.1.2 /SCD_Import	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute “SCD/SVD Management” set to “authorised” is allowed to import SCD,
FDP_ACF.1.3 /SCD_Import	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4 /SCD_Import	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute “SCD/SVD management” set to “not authorised” is not allowed to import SCD.

Application note: part 3 only [PP-SSCD-KI].

FDP_DAU.2/SVD Data Authentication with Identity of Guarantor

Hierarchical to:	FDP_DAU.1 Basic Data Authentication
Dependencies:	FIA_UID.1 Timing of identification

FDP_DAU.2.1 /SVD	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of SVD.
FDP_DAU.2.2 /SVD	The TSF shall provide CGA with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

Application note: Part 4 extension [EN-419211-4] related to core PP key generation [PP-SSCD-KG]..

FDP_ITC.1/SCD Import of user data without security attributes

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control,] FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1 /SCD	The TSF shall enforce the SCD Import SFP when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2 /SCD	The TSF shall ignore any security attributes associated with the SCD when imported from outside the TOE.
FDP_ITC.1.3/SCD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

Application note: part 3 only [PP-SSCD-KI].

FDP_RIP.1 Subset residual information protection

Hierarchical to:	No other components
Dependencies:	No dependency

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

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

1. SCD
2. SVD (if persistent stored by TOE).

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

FDP_SDI.2/Persistent Stored data integrity monitoring and action

Hierarchical to:	FDP_SDI.1
Dependencies:	No dependency

FDP_SDI.2.1/Persistent	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked persistent stored data.
FDP_SDI.2.2/Persistent	Upon detection of a data integrity error, the TSF shall : 1. prohibit the use of the altered data 2. inform the S.Sigy about integrity error.

FDP_SDI.2/DTBS Stored data integrity monitoring and action

Hierarchical to:	FDP_SDI.1
Dependencies:	No dependency

FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored DTBS.
FDP_SDI.2.2/DTBS	Upon detection of a data integrity error, the TSF shall : 1. prohibit the use of the altered data 2. inform the S.Sigy about integrity error.

FDP_UCT.1/SCD Basic data exchange confidentiality

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

FDP_UCT.1.1/SCD	The TSF shall enforce the SCD Import SFP to receive **SCD** in a manner protected from unauthorized disclosure.

Application note: part 3 only [PP-SSCD-KI].

FDP_UIT.1/DTBS Inter-TSF trusted channel – TC Human Interface Device

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

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

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

Application note: Part 5 extension [EN-419211-5] related to core PP key generation [PP-SSCD-KG] and Part 6 extension [EN-419211-6] related to core PP key importation [PP-SSCD-KI].

7.1.3 Class FIA Identification and Authentication

FIA_AFL.1/SIG Authentication failure handling

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

FIA_AFL.1.1/SIG The TSF shall detect when **[3]** unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

FIA_AFL.1.2/SIG When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD.

Note: PIN or BioPIN could be used for user authentication.

FIA_AFL.1/PERSO Authentication failure handling during pre-personalization and personalization phases

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

FIA_AFL.1.1/PERSO The TSF shall detect when [**Number in Table 12**] unsuccessful authentication attempts occurs related to **authentication attempts**.

FIA_AFL.1.2/PERSO When the defined number of unsuccessful authentication attempts has been met, the TSF shall block key.

Auth type	Number	Actions
GP	**3**	**Block GP authentication**.

Table 12: FIA_AFL.1/PERSO refinements

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components
Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a **mutual authentication** to prove the identity of the SSCD.

Application note: Part 4 extension [EN-419211-4] related to core PP key generation [PP-SSCD-KG]..

FIA_UAU.1/PERSO Timing of authentication

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

FIA_UAU.1.1/PERSO	The TSF shall allow 1. Identification of the user by means of TSF required by FIA_UID.1. 2. **No other action**. on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/PERSO	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:
In pre-personalisation, the TSF shall allow no action to be performed before user is authenticated.

FIA_UAU.1/SIG Timing of authentication

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

FIA_UAU.1.1 /SIG	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 CGA and the TOE by means of TSF required by FTP_ITC.1/SVD 4. establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD 5. **None**. on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 /SIG	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:
The TSF shall allow no Signature generation related action to be performed before user is authenticated. That means that other actions, not specifically related to the Signature creation, may be performed before user is authenticated.

Application note: Part 4 extension [EN-419211-4], Part 5 extension [EN-419211-5] and Part 6 extension [EN-419211-6] add operations on FIA-UAU.1/SIG.

FIA_UID.1/PERSO Timing of identification

Hierarchical to:	No other components
Dependencies:	No dependencies

FIA_UID.1.1/PERSO	The TSF shall allow 1. **No action**. on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/PERSO	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1/SIG Timing of identification

Hierarchical to:	No other components
Dependencies:	FDP_DAU.2/SVD Data **Authentication with Identity of Guarantor**

FIA_UID.1.1/SIG	The TSF shall allow 1. Self test according to FPT_TST.1. 2. **No other Signature generation related action**. on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/SIG	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.1.4 Class FMT Security Management

FMT_MOF.1 Management of security functions behaviour

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

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

FMT_MSA.1/Signatory Management of security attributes

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management functions

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

FMT_MSA.1/AdminKG Management of security attributes

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management functions

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

Application note: part 2 only [PP-SSCD-KG].

FMT_MSA.1/AdminKI Management of security attributes

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management functions

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

Application note: part 3 only [PP-SSCD-KI].

FMT_MSA.2 Secure security attributes

Hierarchical to:	No other components

Dependencies: [FDP_ACC.1 Subset access control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

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

FMT_MSA.3/Keygen Static attribute initialization

Hierarchical to: No other components
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1/Keygen 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/Keygen The TSF shall allow the R.Admin to specify alternative initial values to override the default values when an object or information is created.

Application note: part 2 only [PP-SSCD-KG].

FMT_MSA.3/KeyImport Static attribute initialization

Hierarchical to: No other components
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1/KeyImport The TSF shall enforce the SCD Import SFP and Signature-creation SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

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

Application note: part 3 only [PP-SSCD-KI].

FMT_MSA.4/Keygen Static attribute value inheritance

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control]

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

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. 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.

Application note: part 2 only [PP-SSCD-KG].

FMT_MSA.4/KeyImport Static attribute value inheritance

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control]

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

1. If S.Admin imports SCD while S.Sigy is not currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "no" after import of the SCD as a single operation.
2. If S.Admin imports SCD while the S.Sigy is currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "yes" after import of the SCD as a single operation.

Application note: part 3 only [PP-SSCD-KI].

FMT_MTD.1/Admin Management of TSF data

Hierarchical to: No other components
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

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

FMT_MTD.1/Signatory Management of TSF data

Hierarchical to: No other components
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MTD.1.1/Signatory The TSF shall restrict the ability to modify the RAD to S.Sigy.

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components
Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security 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. **No other security management function**.

FMT_SMR.1 Security roles

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

FMT_SMR.1.1 The TSF shall maintain the roles R.Admin and R.Sigy
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

© Copyright Thales

7.1.5 Class FPT Protection of the Security Functions

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components
Dependencies: No dependencies

FPT_EMS.1.1 The TOE shall not emit **[electromagnetic and current emissions]** in excess of **[intelligible threshold]** enabling access to RAD and SCD.
FPT_EMS.1.2 The TSF shall ensure **[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

Hierarchical to: No other components
Dependencies: No dependencies

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
1. self-test according to FPT_TST fails.
2. **[No other failure]**.

FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components
Dependencies: No dependencies

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components
Dependencies: No dependencies

FPT_PHP.3.1 The TSF shall resist **[clock frequency, voltage tampering and penetration of protection layer]** to the **[integrated circuit]** by responding automatically such that the SFRs are always enforced.

FPT_TST.1 TSF testing

Hierarchical to: No other components
Dependencies: No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests **[see Table 13: conditions triggering tests]** to demonstrate the correct operation of the TSF.
FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of TSF.

Conditions under which self test should occur	Description of the self test
During initial start-up	RNG live test, sensor test, FA detection, Integrity Check of NVM ES
Periodically	RNG monitoring, sensor test, FA detection
After cryptographic computation	FA detection
Before any use or update of TSF data	FA detection, Integrity Check of related TSF data

Table 13: conditions triggering tests

7.1.6 Class FTP Trusted Path/Channel

FTP_ITC.1/SCD_import Inter-TSF trusted Channel

Hierarchical to: No other components
Dependencies: No dependencies

FTP_ITC.1.1/SCD import	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/SCD import	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/SCD import	The TSF shall initiate communication via the trusted channel for 1. Data exchange integrity according to FDP_UCT.1/SCD. 2. **[None].**

Application note: part 3 only [PP-SSCD-KI].

FTP_ITC.1/SVD Inter-TSF trusted Channel

Hierarchical to: No other components
Dependencies: No dependencies

FTP_ITC.1.1/SVD	The TSF shall provide a communication channel between itself and another trusted IT product **CGA** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/SVD	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/SVD	The TSF **or the CGA** shall initiate communication via the trusted channel for 1. Data authentication with Identity of Guarantor according to FIA_API.1 and FDP_DAU.2/SVD, 2. [None].

Application note: Part 4 extension [EN-419211-4] related to core PP key generation [PP-SSCD-KG]..

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

Hierarchical to: No other components
Dependencies: No dependencies

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/SIG,, 2. **[None].**

Application note: Part 5 extension [EN-419211-5] related to core PP key generation [PP-SSCD-KG] and Part 6 extension [EN-419211-6] related to core PP key importation [PP-SSCD-KI].

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

Hierarchical to: No other components

Dependencies: No dependencies

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

FTP_ITC.1.2/DTBS 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: Part 5 extension [EN-419211-5] related to core PP key generation [PP-SSCD-KG] and Part 6 extension [EN-419211-6] related to core PP key importation [PP-SSCD-KI].

7.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

The SAR for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 5 (EAL5) and augmented by taking the following components: ALC_DVS.2, and AVA_VAN.5.

7.3 SECURITY REQUIREMENTS RATIONALE

7.3.1 SFR and PP

Requirements	[PP-SSCD-KG]	[PP-SSCD-KI]	additions	[EN-419211-4]	[EN-419211-5]	[EN-419211-6]
FCS_CKM.1/SCD	X					
FCS_CKM.1/Session			X			
FCS_CKM.4/SCD	X					
FCS_CKM.4/Session			X			
FCS_COP.1/DSC	X	X				
FCS_COP.1/Session			X			
FDP_ACC.1/Signature-creation	X	X				
FDP_ACF.1/Signature-creation	X	X				
FDP_ACC.1/SCD/SVD_Generation	X					
FDP_ACF.1/SCD/SVD_Generation	X					
FDP_ACC.1/SVD transfer SFP	X					
FDP_ACF.1/SVD transfer SFP	X					
FDP_ACC.1/SCD import SFP		X				
FDP_ACF.1/SCD import SFP		X				
FDP_ITC.1/SCD		X				
FDP_RIP.1	X	X				
FDP_SDI.2/Persistent	X	X				
FDP_SDI.2/DTBS	X	X				
FDP_UIT.1/DTBS					X	X
FDP_DAU.2/SVD				X		
FDP_UCT.1/SCD		X				
FIA_AFL.1/PERSO			X			

Requirements	[PP-SSCD-KG]	[PP-SSCD-KI]	additions	[EN-419211-4]	[EN-419211-5]	[EN-419211-6]
FIA_AFL.1/SIG	X	X				
FIA_API.1				X		
FIA_UAU.1/PERSO			X			
FIA_UAU.1/SIG	X	X		X	X	X
FIA_UID.1/PERSO			X			
FIA_UID.1/SIG	X	X				
FMT_MOF.1	X	X				
FMT_MSA.1/Signatory	X	X				
FMT_MSA.1/AdminKG	X					
FMT_MSA.1/AdminKI		X				
FMT_MSA.2	X	X				
FMT_MSA.3/Keygen	X					
FMT_MSA.3/KeyImport		X				
FMT_MSA.4/Keygen	X					
FMT_MSA.4/KeyImport		X				
FMT_MTD.1/Admin	X	X				
FMT_MTD.1/Signatory	X	X				
FMT_SMF.1	X	X				
FMT_SMR.1	X	X				
FPT_EMS.1	X	X				
FPT_FLS.1	X	X				
FPT_PHP.1	X	X				
FPT_PHP.3	X	X				
FPT_TST.1	X	X				
FTP_ITC.1/SCD_import		X				
FTP_ITC.1/SVD				X		
FTP_ITC.1/VAD					X	X
FTP_ITC.1/DTBS					X	X

Table 14: PP vs. SFR rationale

7.3.2 Security Functional Requirements Rationale

7.3.2.1 Security objectives for the TOE

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 (Part 2 only)	OT.SCD_Unique (Part 2 only)	OT.SCD_SVD_Corresp (Part 2 only)	OT.SCD_Auth_Imp (Part 3 only)	OT.Pre-perso_authentication	OT.TOE_SSCD_Auth (part 4)	OT.TOE_TC_SVD_Exp (part 4)	OT.TOE_TC_VAD_Imp (part 5&6)	OT.TOE_TC_DTBS_Imp (part 5&6)
FCS_CKM.1/SCD	X	X								X	X						
FCS_CKM.1/Session	X												X				
FCS_CKM.4/SCD	X	X															
FCS_CKM.4/Session	X												X				
FCS_COP.1/DSC	X		X														
FCS_COP.1/Session	X												X				
FDP_ACC.1/Signature-creation	X			X													
FDP_ACF.1/Signature-creation	X			X													
FDP_ACC.1/SCD/SVD_Generation	X								X						X		
FDP_ACF.1/SCD/SVD_Generation	X								X						X		
FDP_ACC.1/SVD transfer	X																
FDP_ACF.1/SVD transfer	X																
FDP_ACC.1/SCD import	X											X					
FDP_ACF.1/SCD import	X											X					
FDP_ITC.1/SCD	X																
FDP_RIP.1		X															
FDP_SDI.2/Persistent		X	X								X						
FDP_SDI.2/DTBS				X	X												
FDP_DAU.2/SVD															X		
FDP_UCT.1/SCD	X	X															
FDP_UIT.1/ DTBS																X	X
FIA_AFL.1/PERSO													X				
FIA_AFL.1/SIG				X													
FIA_API.1														X			
FIA_UAU.1/PERSO													X				
FIA_UAU.1/SIG				X					X					X			
FIA_UID.1/PERSO													X				
FIA_UID.1/SIG				X					X								
FMT_MOF.1	X			X													
FMT_MSA.1/AdminKG	X								X								
FMT_MSA.1/AdminKI	X																
FMT_MSA.1/Signatory	X			X													
FMT_MSA.2	X			X					X								
FMT_MSA.3/Keygen	X			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 (Part 2 only)	OT.SCD_Unique (Part 2 only)	OT.SCD_SVD_Corresp (Part 2 only)	OT.SCD_Auth_Imp (Part 3 only)	OT.Pre-perso_authentication	OT.TOE_SSCD_Auth (part 4)	OT.TOE_TC_SVD_Exp (part 4)	OT.TOE_TC_VAD_Imp (part 5&6)	OT.TOE_TC_DTBS_Imp (part 5&6)
FMT_MSA.3/KeyImport	X			X													
FMT_MSA.4/Keygen	X			X					X		X						
FMT_MSA.4/KeyImport	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											
FPT_FLS.1		X															
FPT_PHP.1							X										
FPT_PHP.3		X						X									
FPT_TST.1	X	X	X														
FTP_ITC.1/SCD_import	X	X															
FTP_ITC.1/SVD															X		
FTP_ITC.1/VAD																X	
FTP_ITC.1/DTBS																	X

Table 15: Objective vs. SFR rationale

OT.Lifecycle_Security (*Lifecycle security*) is provided by the SFR for SCD/SVD generation FCS_CKM.1/SCD,
SCD usage FCS_COP.1/DSC and SCD destruction FCS_CKM.4/SCD 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_AFC.1/Signature_Creation which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/AdminKG, FMT_MSA.1/AdminKI, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3/KeyGen, FMT_MSA.3/KeyImport, FMT_MSA.4/KeyGen, FMT_MSA.4/KeyImport, 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.
The SCD import is controlled by TSF according to FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import and FDP_ITC.1/SCD. The confidentiality of the SCD is protected during import according to FDP_UCT.1/SCD in the trusted channel FTP_ITC.1/SCD_import .
FCS_CKM.1/Session, FCS_CKM.4/Session and FCS_COP.1/Session ensure the secure channel mechanisms for the initialisation, personalisation and operational usage of the TOE.

OT.SCD_Secrecy (*Secrecy of signature creation data*) is provided by the security functions specified by the following SFR. FCS_CKM.1/SCD 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/SCD 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.
FDP_UCT.1/SCD and FTP_ITC.1/SCD_import ensures the confidentiality for SCD import.

OT.Sig_Secure (*Cryptographic security of the electronic signature*) is provided by the cryptographic algorithms specified by FCS_COP.1/DSC, 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 (*Signature creation function for the legitimate signatory only*) is provided by an SFR for identification authentication and access control. FIA_UAU.1/SIG and FIA_UID.1/SIG 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/SIG 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/KeyGen, FMT_MSA.3/KeyImport, FMT_MSA.4/KeyGen, and FMT_MSA.4/KeyImport. 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 (*DTBS/R integrity inside the 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 (*Provide physical emanations security*) covers that no intelligible information is emanated. This is provided by FPT_EMS.1.1.

OT.Tamper_ID (*Tamper detection*) is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

OT.Tamper_Resistance (*Tamper resistance*) is provided by FPT_PHP.3 to resist physical attacks.

SSCD Part 2 only

OT.SCD/SVD_Auth_Gen (*Authorized SCD/SVD generation*) addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1/SIG and FIA_UAU.1/SIG 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/AdminKG, FMT_MSA.2, and FMT_MSA.3/Keygen for static attribute initialisation. The SFR FMT_MSA.4/KeyGen defines rules for inheritance of the security attribute “SCD operational” of the SCD.

OT.SCD_Unique (*Uniqueness of the signature creation data*) 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/SCD.

OT.SCD_SVD_Corresp (*Correspondence between SVD and SCD*) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1/SCD 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

© Copyright Thales

by FMT_SMF.1 and by FMT_MSA.4/KeyGen allow R.Admin to modify the default value of the security attribute SCD Identifier.

SSCD Part 2 and part 4

OT.TOE_SSCD_Auth (Authentication proof as SSCD) requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by FIA_API.1 (Authentication Proof of Identity). The SFR FIA_UAU.1/SIG allows (additionally to the core PP SSCD KG) establishment of the trusted channel before (human) user is authenticated.

OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export) requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA, which is directly provided by

- The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer.

- FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor), which requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.

- FTP_ITC.1/SVD Inter-TSF trusted channel), which requires the TOE to provide a trusted channel to the CGA.

SSCD Part 3 only

OT.SCD_Auth_Imp (*Authorized SCD import***)** is provided by the security functions specified by the following SFR. FIA_UID.1/SIG and FIA_UAU.1/SIG ensure that the user is identified and authenticated before SCD can be imported. FDP_ACC.1/SCD_Import and FDP_ACF.1/SCD_Import ensure that only authorised users can import SCD.

SSCD part 5 and part 6 in addition with part 2 and part 3

OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import) 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_TC_DTBS_Imp (Trusted channel of TOE for DTBS) 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.

Extensions

OT.Pre-perso_authentication (*strong authentication in Pre-personalisation*) is provided by the security functions specified by the following SFR. FIA_AFL.1/PERSO, FIA_UAU.1/PERSO, FIA_UID.1/PERSO, FCS_CKM.1/Session, FCS_CKM.4/Session, FCS_COP.1/DSC and FCS_COP.1/Session.

© Copyright Thales

7.3.2.2 *Dependency Rationale*

Requirements	CC Dependencies	Satisfied Dependencies
FCS_CKM.1/SCD	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/DSC, FCS_CKM.4/SCD
FCS_CKM.1/Session	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/Session, FCS_CKM.4/Session
FCS_CKM.4/SCD	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/SCD, FDP_ITC.1/SCD
FCS_CKM.4/Session	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/Session
FCS_COP.1/DSC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/SCD, FCS_CKM.1/SCD
FCS_COP.1/Session	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/Session, FCS_CKM.4/Session, FDP_ITC.1/SCD,
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/KeyGen, FMT_MSA.3/KeyImport
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/KeyGen
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/KeyGen
FDP_ACC.1/SCD import	(FDP_ACF.1)	FDP_ACF.1/SCD import
FDP_ACF.1/SCD import	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SCD import, FMT_MSA.3/KeyImport
FDP_DAU.2/SVD	FIA_UID.1	FIA_UID.1/SIG
FDP_ITC.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1/SCD import, FMT_MSA.3/KeyImport
FDP_RIP.1	No dependencies	
FDP_SDI.2/Persistent	No dependencies	
FDP_SDI.2/DTBS	No dependencies	
FDP_UIT.1/DTBS	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FDP_UCT.1/SCD	(FTP_ITC.1 or FTP_TRP.1) (FDP_ACC.1 or FDP_IFC.1)	FTP_ITC.1/SCD_import, FDP_ACC.1/SCD import,
FIA_AFL.1/PERSO	(FIA_UAU.1)	FIA_UAU.1/PERSO
FIA_AFL.1/SIG	(FIA_UAU.1)	FIA_UAU.1/SIG
FIA_UAU.1/PERSO	(FIA_UID.1)	FIA_UID.1/PERSO
FIA_UAU.1/SIG	(FIA_UID.1)	FIA_UID.1/SIG
FIA_API.1	No dependencies	n/a
FIA_UID.1/PERSO	No dependencies	n/a
FIA_UID.1/SIG	No dependencies	n/a
FMT_MOF.1	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/AdminKG	(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/AdminKI	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/SCD Import, FMT_SMR.1, FMT_SMF.1

© Copyright Thales

Requirements	CC Dependencies	Satisfied Dependencies
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_MSA.1/AdminKG, FMT_MSA.1/AdminKI FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.3/KeyGen	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/AdminKG, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.3/KeyImport	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/AdminKI, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4/KeyGen	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.1/SCD/SVD_Generation FDP_ACC.1/Signature-creation
FMT_MSA.4/KeyImport	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.1/SCD Import, 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
FMT_SMF.1	No dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1/SIG
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	
FTP_ITC.1/SCD_import	No dependencies	
FTP_ITC.1/SVD	No dependencies	n/a
FTP_ITC.1/VAD	No dependencies	n/a
FTP_ITC.1/DTBS	No dependencies	n/a

Table 16: Dependency rationale

7.3.3 Security Assurance Requirements Rationale

EAL5 was chosen because it provides a high level of independently assured security in a planned development. It requires a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.
The selection of the component ALC_DVS.2 provides a higher assurance of the security of the SSCD's development and manufacturing especially for the secure handling of the SSCD's material.
The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential.

7.3.4 Compatibility between SFR of [ST-IAS] and [ST-PLTF]

We can therefore conclude that the SFR of [ST-IAS] and [ST-PLTF] are consistent.

Requirements	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
FDP_ACC.2/FIREWALL			X FDP_ACC.1/Signature_Creation FDP_ACC.1/SCD/SVD_Generation FDP_ACC.1/SVD_Transfer
FDP_ACF.1/FIREWALL			X FDP_ACF.1/Signature_Creation FDP_ACF.1/SCD/SVD_Generation FDP_ACF.1/SVD_Transfer
FDP_IFC.1/JCVM		X FMT_MSA.4/Keygen FDP_UCT.1/SCD FMT_MSA.4/KeyImport	
FDP_IFF.1/JCVM	X		
FDP_RIP.1/OBJECTS		X SFR FDP_RIP.1	
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		X FCS_CKM.1/SCD FCS_CKM.1/Session	
FCS_CKM.2	X		
FCS_CKM.3	X		
FCS_CKM.4		X FCS_CKM.4/SCD FCS_CKM.4/Session	
FCS_COP.1		X FCS_COP.1/DSC FCS_COP.1/Session	
FDP_RIP.1/ABORT		X FDP_RIP.1	
FDP_RIP.1/APDU		X FDP_RIP.1	
FDP_RIP.1/GlobalArray		X FDP_RIP.1	
FDP_RIP.1/bArray		X FDP_RIP.1	
FDP_RIP.1/KEYS		X FDP_RIP.1	

© Copyright Thales

Requirements	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
FDP_RIP.1/TRANSIENT		X FDP_RIP.1	
FDP_ROL.1/FIREWALL	X		
FAU_ARP.1	X		
FDP_SDI.2/DATA		X FDP_SDI.2/Persistent FDP_SDI.2/DTBS	
FPR_UNO.1	X		
FPT_FLS.1/JCS			X FPT_FLS.1
FPT_TDC.1	X		
FIA_ATD.1/AID	X		
FIA_UID.2/AID	X		
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		
FPT_FLS.1/ADEL	X		
FDP_RIP.1/ODEL		X FDP_RIP.1	
FPT_FLS.1/ODEL		X FPT_FLS.1	
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		

© Copyright Thales

Requirements	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
FMT_SMR.1/CM	X		
FTP_ITC.1/CM	X		
FPT_TST.1/SCP		X FPT_TST.1	
FPT_PHP.3/SCP		X FPT_PHP.3 FPT_PHP.1	
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_FLS.1	
FPT_ITT.1/SpecificAPI	X		
FPR_UNO.1/SpecificAPI	X		
FCS_RNG.1			X FCS_RNG.1
FDP_ACC.1/OS-UPDATE	X		
FDP_ACF.1/OS-UPDATE	X		
FIA_ATD.1/OS-UPDATE	X		
FMT_MSA.3/OS-UPDATE	X		
FMT_SMR.1/OS-UPDATE	X		
FMT_SMF.1/OS-UPDATE	X		
FTP_TRP.1/OS-UPDATE	X		
FCS_COP.1/OS-UPDATE-DEC	X		
FCS_COP.1/OS-UPDATE-VER	X		
FPT_FLS.1/OS-UPDATE	X		

Table 17: SFRs Dependencies from Platform

(*) RP_SFR-SERV group definition:

Requirements	IP_SFR	RP_SFR-SERV (*)	RP_SFR-MECH
FCS_CKM.1/DH_PACE		X	
FCS_CKM.1/PERSO		X	
FCS_CKM.4/PACE		X	
FCS_COP.1/PACE_ENC		X	
FCS_COP.1/PACE_MAC		X	
FCS_COP.1/PACE_CAM		X	
FCS_COP.1/PERSO		X	
FCS_RNG.1/PACE			X
FIA_AFL.1/PERSO			X
FIA_AFL.1/PACE			X
FIA_UID.1/PERSO		X	
FIA_UAU.1/PERSO		X	
FIA_UID.1/PACE		X	
FIA_UAU.1/PACE		X	
FIA_UAU.4/PACE		X	
FIA_UAU.5/PACE		X	
FIA_UAU.6/PACE		X	
FDP_RIP.1/PACE			X
FTP_ITC.1/PACE		X	
FMT_SMF.1/PACE	X		
FMT_SMF.1/PERSO	X		
FMT_SMR.1/PACE		X	
FMT_SMR.1/PERSO		X	
FMT_LIM.1/PERSO		X	
FMT_LIM.2/PERSO		X	
FMT_MTD.1/INI_ENA		X	
FMT_MTD.1/INI_DIS		X	
FMT_MTD.1/KEY_READ		X	
FMT_MTD.1/Initialize_PINPUK	X		
FMT_MTD.1/Resume_PINPUK	X		
FMT_MTD.1/Change_PIN	X		
FMT_MTD.1/Unblock_ PIN	X		
FPT_EMS.1			X
FPT_TST.1		X	
FPT_FLS.1			X
FPT_PHP.3		X	

Table 18: SFRs Dependencies from PACE

© Copyright Thales

8. TOE SUMMARY SPECIFICATION

8.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the IAS application with its OS, and by the chip.
The security functions provided by the platform are described in [ST-PLTF].

8.1.1 SF provided by IAS Application

This section presents the security functions provided by the IAS application.

Identification	Name
SF.AUTHENTICATION	Authentication management
SF.CRYPTO	Cryptography management
SF.INTEGRITY	Integrity monitoring
SF.MANAGEMENT	Operation management and access control
SF.SECURE_MESSAGING	Secure messaging management
SF.CSM	Card Security Management

Table 19: TOE security functions list

SF.AUTHENTICATION provides the authentication management on the TOE. It encompasses:

- Signatory authentication failure as defined in **FIA_AFL.1/SIG**,
- Timing of signatory identification and authentication as defined in **FIA_UID.1/SIG** and **FIA_UAU.1/SIG**,
- Authentication of proof of identity & identity guarantor **FIA_API.1** & **FDP_DAU.2/SVD**
- Pre-personaliser authentication failure as defined in **FIA_AFL.1/PERSO**,
- Timing of pre-personaliser identification and authentication as defined in **FIA_UID.1/PERSO** and **FIA_UAU.1/PERSO**.

SF.CRYPTO provides the crypto management on the TOE. It encompasses:

- The generation of SCD/SVD and session keys as defined in **FCS_CKM.1/SCD** and **FCS_CKM.1/Session**,
- The destruction of SCD and session keys as defined in **FCS_CKM.4/SCD** and **FCS_CKM.4/Session**,
- The usage of SCD and session keys as defined in **FCS_COP.1/DSC** and **FCS_COP.1/Session**

SF.INTEGRITY provides the integrity monitoring on the TOE. It encompasses:

- The integrity of sensitive data as defined in **FDP_SDI.2/Persistent** and **FDP_SDI.2/DTBS**, and also **FDP_UIT.1/DTBS**

SF.MANAGEMENT provides operation management and access control. It encompasses:

- Access management as defined in **FDP_ACC.1/Signature-creation, FDP_ACF.1/Signature-creation, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FDP_ACC.1/SVD transfer, FDP_ACF.1/SVD transfer, FDP_ACC.1/SCD import, FDP_ACF.1/SCD import** SFR,
- Data input and output as defined in **FDP_ITC.1/SCD**,
- Management of functions as defined in **FMT_MOF.1** and **FMT_SMF.1**,
- Management of security attributes **FMT_MSA.1/AdminKG**, **FMT_MSA.1/AdminKI**, **FMT_MSA.1/Signatory**, **FMT_MSA.2**, **FMT_MSA.3/KeyImport**, **FMT_MSA.3/KeyGen**, **FMT_MSA.4/KeyImport**, **FMT_MSA.4/KeyGen**,
- Management of TSF data as defined in **FMT_MTD.1/Admin** and **FMT_MTD.1/Signatory**,
- Management of roles as defined in **FMT_SMR.1**,

SF.SECURE_MESSAGING provides secure messaging for the TOE. It encompasses:

- Data exchange integrity and confidentiality as defined in **FDP_UCT.1/SCD**,
- Secure channel and secure path as defined in **FTP_ITC.1/SCD_import**, in **FTP_ITC.1/SVD,** in **FTP_ITC.1/VAD,** in **FTP_ITC.1/DTBS,**

SF.CSM provides cards security protection. It encompasses:

- Protection against physical attacks as defined in **FPT_EMS.1**, **FPT_FLS.1**, **FPT_PHP.1**, and **FPT_PHP.3**,

- Testing of the card as defined in **FPT_TST.1**,
- Secure unavailability of sensitive data as defined in **FDP_RIP.1**.

8.1.2 TSFs provided by the platform

The evaluation is a composite evaluation and uses the results of the Platform CC.

SF	Description
SF_FW	Firewall
SF_API	Application Programming Interface
SF.CSM	Card Security Management
SF.AID	AID Management
SF.INST	Installer
SF.ADEL	Applet Deletion
SF.ODEL	Object Deletion
SF.CAR	Secure Carrier
SF.SCP	Smart Card Platform
SF.CMG	Card Manager
SF.APIS	Specific API
SF.RND	RNG
SF.OSAGILITY	OS Agility Management

Table 20: Security Functions provided by the MultiApp V5.1 Platform

These SF are described in [ST-PLTF].

8.2 TOE SUMMARY SPECIFICATION RATIONALE

8.2.1 TOE security functions rationale

Requirements	SF.Authentication	SF.Crypto	SF.Integrity	SF.Management	SF.Secure_Messaging	SF.CSM
FCS_CKM.1/SCD		X				
FCS_CKM.1/Session		X				
FCS_CKM.4/SCD		X				
FCS_CKM.4/Session		X				
FCS_COP.1/DSC		X				
FCS_COP.1/Session		X				
FDP_ACC.1/Signature-creation				X		
FDP_ACF.1/Signature-creation				X		
FDP_ACC.1/SCD/SVD_Generation				X		
FDP_ACF.1/SCD/SVD_Generation				X		
FDP_ACC.1/SVD transfer				X		
FDP_ACF.1/SVD transfer				X		
FDP_ACC.1/SCD import				X		
FDP_ACF.1/SCD import				X		
FDP_ITC.1/SCD				X		
FDP_RIP.1						X
FDP_SDI.2/Persistent			X			
FDP_SDI.2/DTBS			X			
FDP_UIT.1/DTBS			X			

© Copyright Thales

Requirements	SF.Authentication	SF.Crypto	SF.Integrity	SF.Management	SF.Secure_Messaging	SF.CSM
FDP_DAU.2/SVD	X					
FDP_UCT.1/SCD					X	
FIA_AFL.1/SIG	X					
FIA_API.1	X					
FIA_UAU.1/SIG	X					
FIA_UID.1/SIG	X					
FIA_AFL.1/PERSO	X					
FIA_UID.1/PERSO	X					
FIA_UAU.1/PERSO	X					
FMT_MOF.1				X		
FMT_MSA.1/AdminKG				X		
FMT_MSA.1/AdminKI				X		
FMT_MSA.1/Signatory				X		
FMT_MSA.2				X		
FMT_MSA.3/KeyImport				X		
FMT_MSA.3/KeyGen				X		
FMT_MSA.4/KeyImport				X		
FMT_MSA.4/KeyGen				X		
FMT_MTD.1/Admin				X		
FMT_MTD.1/Signatory				X		
FMT_SMF.1				X		
FMT_SMR.1				X		
FPT_EMS.1						X
FPT_FLS.1						X
FPT_PHP.1						X
FPT_PHP.3						X
FPT_TST.1						X
FTP_ITC.1/SCD_import					X	
FTP_ITC.1/SVD					X	
FTP_ITC.1/VAD					X	
FTP_ITC.1/DTBS					X	

Table 21: Rationale table of functional requirements and security functions

FCS-CKM.1/SCD requires the generation of the SCD/SVD pair. This requirement is fulfilled by SF.CRYPTO “Cryptography management” that manages the cryptographic operations the TOE.

FCS-CKM.1/Session requires the generation of the session keys. This requirement is fulfilled by SF.CRYPTO “Cryptography management” that manages the cryptographic operations the TOE.

FCS-CKM.4/SCD requires the destruction of the previous SCD/SVD pair in case of re-generation or import of SCD. This requirement is fulfilled by SF.CRYPTO “Cryptography management” that manages the cryptographic operations the TOE.
FCS-CKM.4/Session requires the destruction of the session keys. This requirement is fulfilled by SF.CRYPTO “Cryptography management” that manages the cryptographic operations the TOE.

© Copyright Thales

FCS_COP.1/DSC requires the availability of cryptographic operations to support the electronic signature application. This requirement is fulfilled by SF.CRYPTO “Cryptography management” that manages the cryptographic operations the TOE.

FCS_COP.1/Session requires the availability of cryptographic operations for secure messaging. This requirement is fulfilled by SF.CRYPTO “Cryptography management” that manages the cryptographic operations the TOE.

FDP_ACC.1 and **FDP_ACF** require access control on operations covered by the SFP. These requirements are fulfilled by SF.MANAGEMENT “Operation management and access control”.

FDP_ITC.1/SCD controls transfer of SCD into the TSF. This requirement is fulfilled by SF.MANAGEMENT “Operation management and access control”.

FDP_RIP.1 requires that any residual information content of a resource is made unavailable upon de-allocation of this resource. This requirement is fulfilled by SF.CSM “Card Security Management”.

FDP_SDI.2/Persistent FDP_SDI.2/DTBS and **FDP_UIT.1/DTBS** require the integrity of stored sensitive data. These requirements are fulfilled by SF.Integrity “Integrity monitoring”.

FDP_UCT.1/SCD requires the confidentiality and integrity of the SCD during its transfer into the TSF. This requirement is fulfilled by SF.SECURE_MESSAGING “Secure messaging management”.

FIA_AFL.1/PERSO, FIA_UAU.1/PERSO, FIA_UID.1/PERSO, FIA_AFL.1/SIG, **FIA_UAU.1/SIG**, **FIA_UID.1/SIG**,**FIA_API.1** and **FDP_DAU.2/SVD** require authentication management. These requirements are fulfilled by SF_AUTHENTICATION “Authentication management“.

FMT_MOF.1, **FMT_MSA.1**, **FMT_MSA.2**, **FMT_MSA.3**, **FMT_MSA.4**, **FMT_MTD.1**, **FMT_SMF.1**, and **FMT_SMR.1** require several functions for the management of TSF data. These requirements are fulfilled by SF_MANAGEMENT” Operation management and access control”.

FPT_EMS.1 requires counter-measures to avoid access via emanations using TOE interfaces. This requirement is fulfilled by SF.CSM “Card Security Management”.

FPT_FLS.1, **FPT_PHP.1**, and **FPT_PHP.3** require physical protection of the TOE. These requirements are fulfilled by SF.CSM “Card Security Management”.

FPT_TST.1 requires testing the TSF. This requirement is fulfilled by SF.CSM “Card Security Management”.

FTP_ITC.1/SCD_import requires trusted channel between SCA and the TOE. This requirement is fulfilled by SF.SECURE_MESSAGING “Secure messaging management”.

FTP_ITC.1/SVD requires trusted channel between CGA and the TOE. This requirement is fulfilled by SF.SECURE_MESSAGING “Secure messaging management”.

FTP_ITC.1/VAD requires trusted channel between HID of CGA and the TOE. This requirement is fulfilled by SF.SECURE_MESSAGING “Secure messaging management”.

FTP_ITC.1/DTBS requires trusted channel between HID of CGA and the TOE. This requirement is fulfilled by SF.SECURE_MESSAGING “Secure messaging management”.

END OF DOCUMENT

© Copyright Thales