MultiApp V3
IAS CWA
Security Target

UPDATES

Date	Author	Modification
23 Jan 14	Gemalto	Creating from evaluated ST (V1.0)

CONTENT

FIGURES

TABLES

1. ST INTRODUCTION

1.1 ST IDENTIFICATION

Title:	MultiApp V3 IAS CWA Security Target
Version:	1.0p
ST reference:	ST_D1261752
Origin:	Gemalto
Product identification:	IAS on MultiApp V3
Security Controllers:	M7820 A11
TOE identification:	IAS on MultiApp V3
TOE documentation:	Guidance document [GUIDE]

The TOE identification is provided by the Card Production Life Cycle Data (CPLCD) of the TOE, located in OTP and in EEPROM. These data are available by executing a dedicated command.

The TOE and the product differ, as further explained in §1.7 TOE boundaries:

- The TOE is the IAS application, with MOCserver, on MultiApp V3
- The MultiApp V3 product also includes 2 applications in ROM.

CPLC field	Length	Value
IC Fabricator	2	IFX
IC Type	2	M7820 A11, M7801 A12
Operating System Identifier	2	n.a.
Operating System release date	2	n.a.
Operating System release level	2	n.a.
IC Fabrication Date	2	n.a.
IC Serial Number	4	Unique identification of the chip written by the ICC Manufacturer
IC Batch Identifier	2	n.a.
IC Module Fabricator	2	n.a.
IC Module Packaging Date	2	n.a.
ICC Manufacturer	2	‘Gemalto’
IC Embedding Date	2	n.a.
IC Pre-personalizer	2	‘Gemalto’
IC Pre-personalization Date	2	n.a.

CPLC field	Length	Value
IC Pre-personalization Equipment Identifier	4	n.a.
IC Personalizer	2	n.a.
IC Personalization Date	2	n.a.
IC Personalization Equipment Identifier	4	n.a.

Table 1: Card Production Life Cycle Data

IT Security Evaluation scheme	Serma Technologies
IT Security Certification scheme	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

1.2 ST OVERVIEW

The Target of Evaluation (TOE) is composed of the MultiApp V3 platform and the electronic signature application IAS with MOCserver.
The platform includes the hardware and the operating system.

The IC is evaluated in conformance with [PP-IC-0035].
The Platform is evaluated in conformance with [PP-JCS-Open].
The IAS application is evaluated in conformance with [EN-14169-2] and [EN-14169-3],

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.

1.3 REFERENCES

1.3.1 External References

[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2012-09-001, version 3.1 rev 4, September 2012
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2012-09-002, version 3.1 rev 4, September 2012
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2012-09-003, version 3.1 rev 4, September 2012
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology CCMB-2012-09-004, version 3.1 rev 4, September 2012
[ST-IC]	[ST-IC-M7820]
[ST-IC-M7820]	ST of M7820 A11 SLE78CLX1600P - Rev. 0.6 - 15 April 2011
[CR-IC]	[CR-IC-M7820]
[CR-IC-M7820]	Certification Report, BSI-DSZ-CC-0695-2011 (11-05-2011)
[FIPS180-2]	*Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+Change Notice to include SHA-224),* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1
[FIPS46-3]	*Federal Information Processing Standards Publication FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES),* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, Reaffirmed 1999 October 25
[ISO15946-1]	*ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General,* 2002
[ISO15946-2]	*ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures,* 2002
[ISO15946-3]	*ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment,* 2002
[ISO7816]	*ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange*, FDIS2004
[ISO9796-2]	*ISO/IEC 9797: Information technology – Security techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms,* 2002
[ISO9797-1]	*ISO/IEC 9797: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher,* 1999
[PKCS#3]	*PKCS #3: Diffie-Hellman Key-Agreement Standard,* An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993

[PP-IC-0035]	*Smartcard IC Platform protection Profile* BSI-PP-0035
[CWA-14169]	Protection profiles for secure signature creation device – CWA version
[PP-SSCD-KG]	[CWA-14169-3]
[PP-SSCD-KI]	[CWA-14169-2]
[CWA-14169-2]	Protection Profile – Secure Signature-Creation Device Type2 BSI-PP-0005, Version 1.04, 25th July 2001
[CWA-14169-3]	Protection Profile – Secure Signature-Creation Device Type3 BSI-PP-0006, Version 1.05, 25th July 2001
[PP-JCS-Open]	Java Card System Protection Profile – Open Configuration ANSSI-PP-2010- 03, Version 2.6, April, 19th 2010
[GP211]	Global Platform Card Specification v 2.1.1 - March 2003
[DirectiveEC]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures
[EN-14168-2]	Protection profiles for secure signature creation device – Part2 : Device with key generation BSI-CC-PP-0059-2009-MA-01, Version 2.01, January 2012
[EN-14168-3]	Protection profiles for secure signature creation device – Part3: Device with key import BSI-CC-PP-0075-2012, Version 1.02, July 2012
[CR-IC-M7820]	*Certification Report, SLE78CLX1600P* / M7820 A11 & M11 *BSI-DSZ-CC-0829-2012*
[CR-IC-M7801]	*Certification Report SLE78CX1600P / M7801 A12 BSI-DSZ-CC-0727-2011*

1.3.2 Internal References

[ST-PLTF]	D1184308 JCS Security Target - MultiApp V3
[GUIDE]	IAS V4 user guidance Multiapp V3 platform User Guidance

1.4 ACRONYMS

CC	Common Criteria
CGA	Certificate generation application
DTBS	Data to be signed
DTBS/R	Data to be signed or its unique representation
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IT	Information Technology
OS	Operating System
PP	Protection Profile
RAD	Reference Authentication Data
SAR	Security Assurance Requirements
SCA	Signature-creation application
SCD	Signature-creation data
SCS	Signature-creation system

SDO	Signed data object
SF	Security Function
SFR	Security functional requirements
SSCD	Secure signature-creation device
ST	Security Target
SVD	Signature-verification data
TOE	Target Of Evaluation
TSF	TOE Security Functionality
VAD	Verification authentication data

1.5 GLOSSARY

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).
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]).

1.6 TOE OVERVIEW

1.6.1 TOE description

IAS is a Java Card application that provides a Secure Signature Creation Device – SSCD - as defined in the DIRECTIVE 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures.

[CWA-14169] defines protection profiles for SSCD:

- [PP-SSCD-KI] is a protection profile for an SSCD Type 2 with SCD key import and signature creation.
- [PP-SSCD-KG] is a protection profile for an SSCD Type 3 with SCD/SVD key generation and signature creation.

In this document the terminology of [CWA-14169] 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 or contactless 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)

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):
  - Symmetric scheme with TDES or AES
  - Asymmetric scheme with Diffie-Hellman based on RSA or elliptic curves
- 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.

1.7 TOE BOUNDARIES

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

- The underlying Integrated Circuit
- The MultiApp V3 platform (JavaCard platform)
- The IAS Application.

Figure 1: TOE Boundaries gives a description of the TOE and its boundaries.

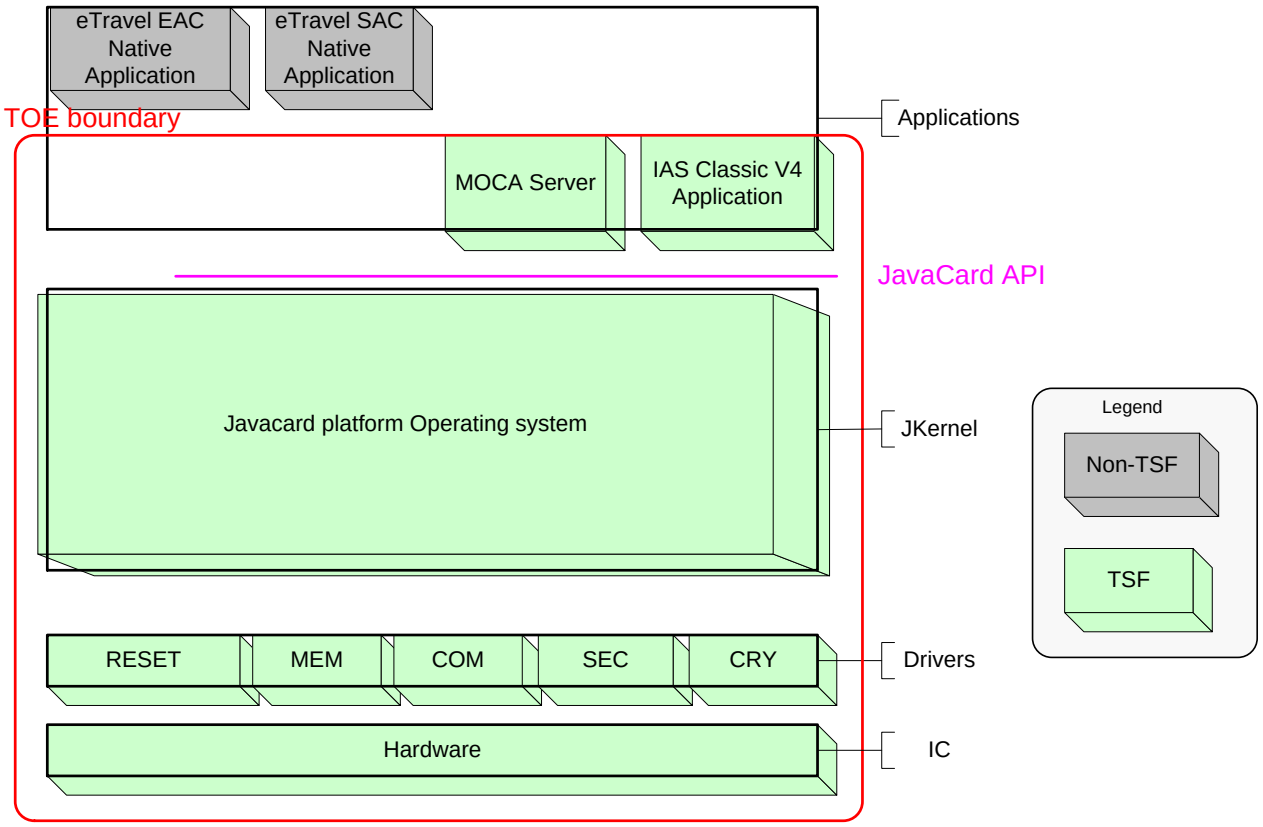


Figure 1: TOE Boundaries

1.8 TOE LIFE-CYCLE

1.8.1 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.

Phase 2 “Manufacturing”:
In a first step the TOE integrated circuit is produced containing the chip Dedicated Software and the parts of the chip Embedded Software in the nonvolatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as SSCD material during the IC manufacturing and the delivery process to the SSCD manufacturer. The IC is securely delivered from the IC manufacturer to the SSCD manufacturer.
The SSCD manufacturer has the following tasks:

- **Initialization:** adding the parts of the IC Embedded Software (NVM ES) to the EEPROM,
- **Pre-personalization:** initialization of the SSCD application,

Phase 3 Personalization of the TOE:

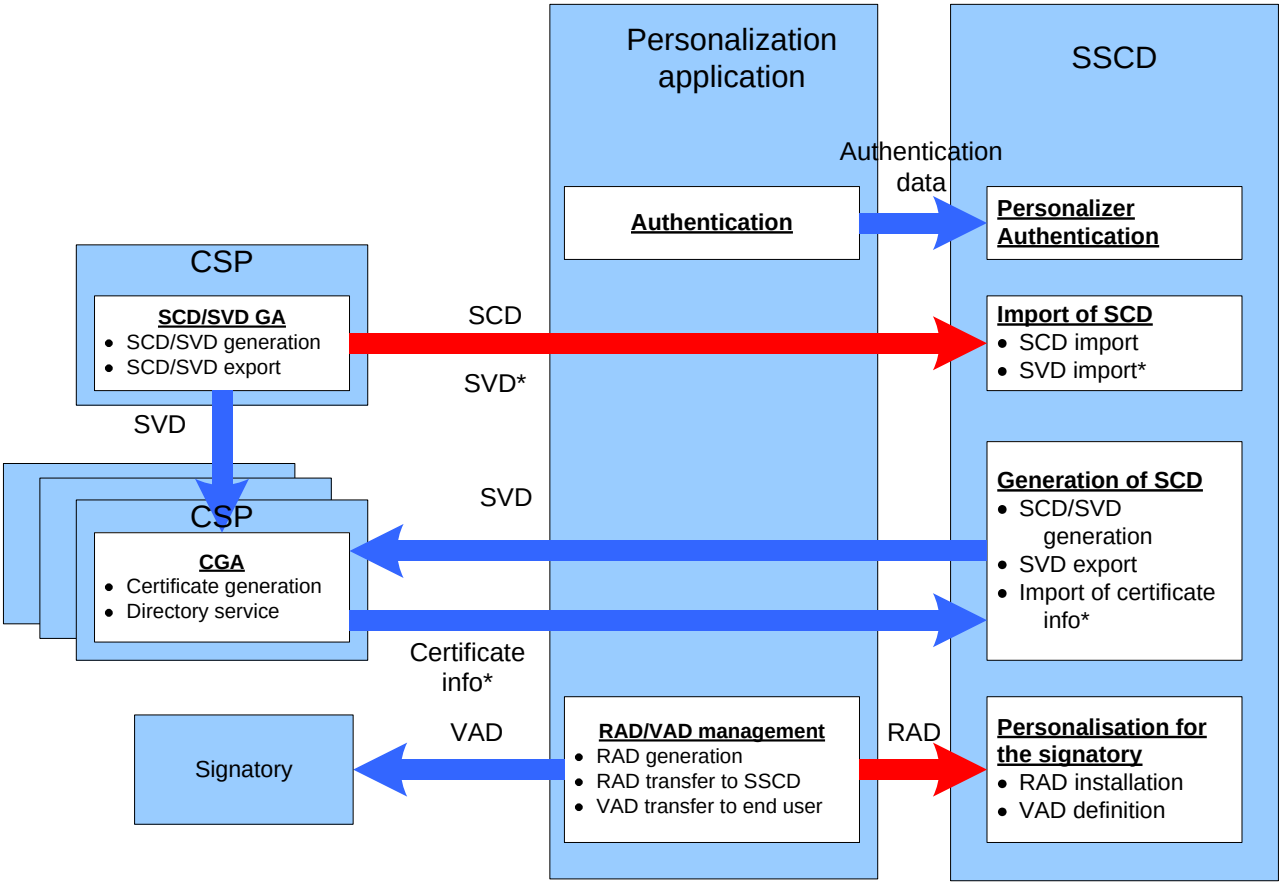


Figure 2: TOE Personalization

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.

Phase 4 “Operational Use”

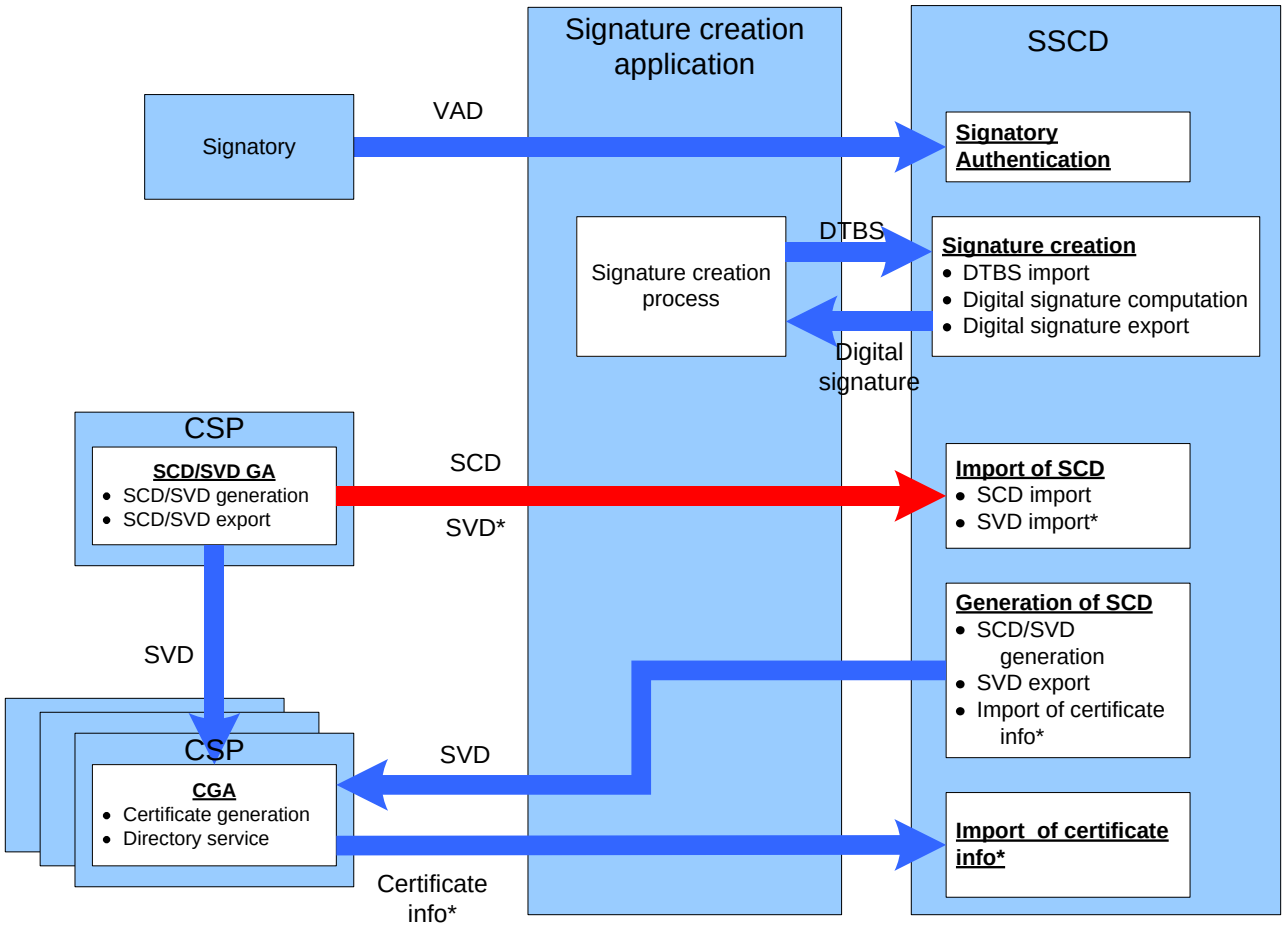


Figure 3: TOE Operational Use

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.

1.8.2 Actors

Actors	Identification
Integrated Circuit (IC) Developer	IFX
Embedded Software Developer	Gemalto
Integrated Circuit (IC) Manufacturer	IFX
Initializer	Gemalto or IFX
Pre-personalizer	Gemalto or IFX
Inlay manufacturer (optional)	Gemalto or another Inlay manufacturer
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 2: Identification of the actors

1.8.3 Involved sites

Life cycle phase	Involved sites
Embedded software development (Phase 1)	**Gemalto Meudon** site (R&D IAS Team) **Gemalto Vantaa** site (R&D OS Team) **Gemalto La Ciotat** site (MKS servers) **Gemalto Gémenos** site (Component team[1])
IC development (Phase 2)	Infineon development site(s) mentioned in [CR-IC-M7820] and [CR-IC-M7801]
IC Manufacturing & Testing (Phase 3)	Infineon production site(s) mentioned in [CR-IC-M7820] and [CR-IC-M7801]
IC initialization, packaging & testing (Phase 4)	Scenario LC1/LC3: **Gemalto Gémenos** site **Gemalto Singapore** site **Gemalto Pont-Audemer** site
Prepersonalization & testing (Phase 5)	Scenario LC1/LC3: **Gemalto Gémenos** site **Gemalto Singapore** site **Gemalto Tczew** site

[1] The Component team is in charge of the delivery of the smartcard embedded software to Infineon (Mask launch)

1.8.4 Pre-personalization on module at Gemalto site

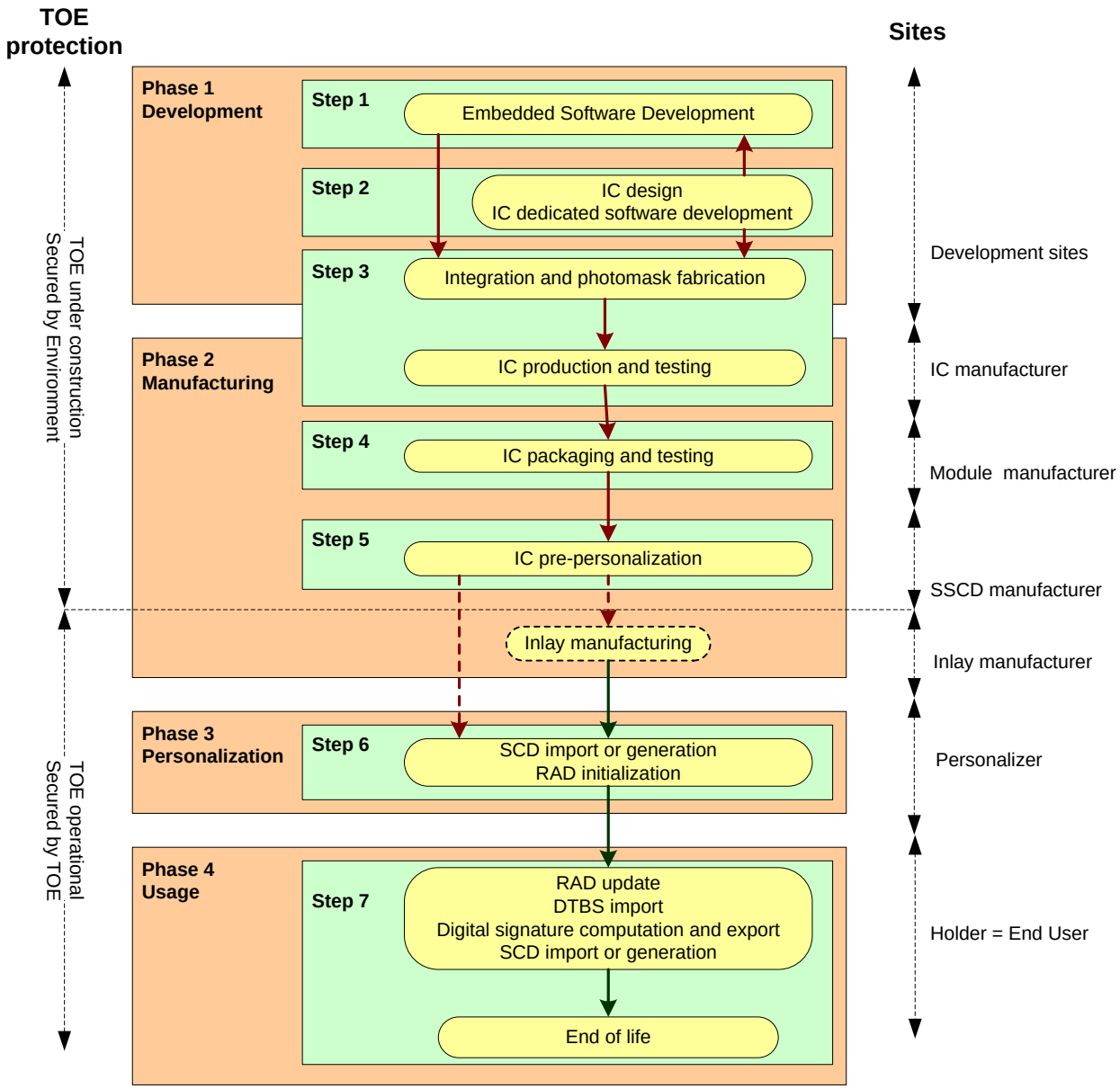


Figure 4: LC1: Pre-personalization on module at Gemalto site

Figure 4: LC1: Pre-personalization on module at Gemalto site describes the standard Life Cycle. The module is manufactured at the founder site. It is then shipped, as wafers or modules, to Gemalto site where it is pre-personalized and then shipped to the Personalizer directly or through an Inlay manufacturer.
During the shipment from Gemalto to the Personalizer, the module is protected by a diversified key.

1.8.5 Pre-personalization on inlay at Gemalto site

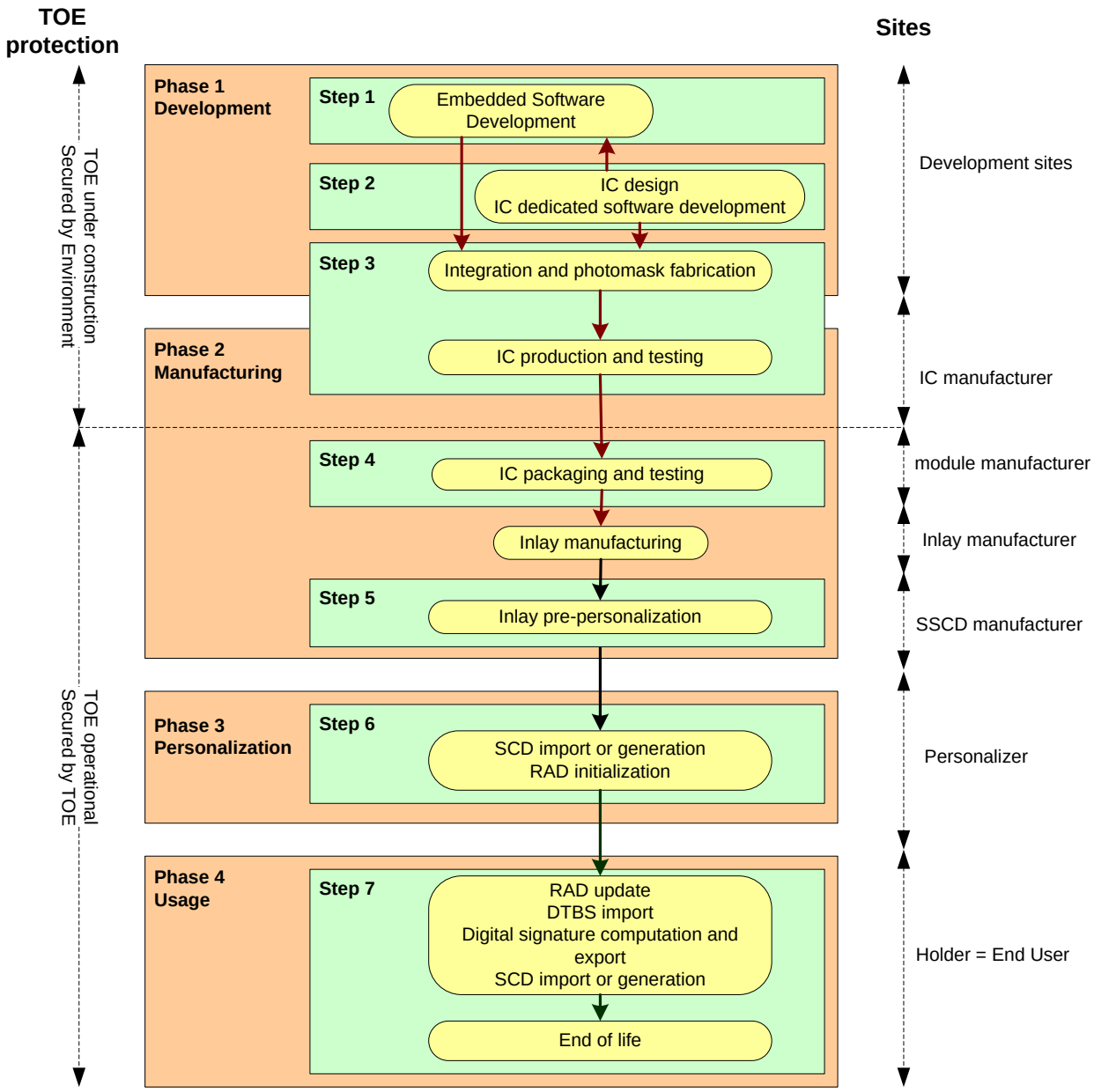


Figure 5: LC3: Pre-personalization on inlay at Gemalto site

LC3 is another alternative to LC1. *Figure 5: LC3: Pre-personalization on inlay at Gemalto site* describes the Life Cycle when Gemalto wishes to receive inlays instead of modules from the founder. In this case, the founder ships the module to the Inlay manufacturer.
During the shipment from the founder to Gemalto, the module is protected by a diversified key.

2. CONFORMANCE CLAIMS

2.1 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 V3 claiming conformance to [PP-JCS-Open].

2.2 PP CLAIM,

This MultiApp v3 IAS security target claims strict conformance to the following Protection Profiles:

- [PP-SSCD-KI], which defines security requirements for an SSCD Type 2 with SCD key import and signature creation.
- [PP-SSCD-KG], which defines security requirements for an SSCD Type 3 with SCD/SVD key generation and signature creation.

The evaluation is a composite evaluation and uses the results of the platform CC evaluation evaluated at level EAL 5+.

The TOE also claims conformance to other Protection Profiles. This is described in other Security Targets:

2.3 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].

3. SECURITY PROBLEM DEFINITION

3.1 INTRODUCTION

3.1.1 Assets

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

D.SCD
SCD: private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).

D.SVD
SVD: public key linked to the SCD and used to perform an electronic signature verification (integrity of the SVD when it is exported must be maintained).

D.DTBS
DTBS and DTBS-representation: set of data, or its representation which is intended to be signed (Their integrity must be maintained).

D.VAD
VAD: PIN code entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed are required)

D.SSCD
Signature-creation function of the SSCD using the SCD: (The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures)

D.RAD
RAD: Reference PIN code used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)

D.SIG
Electronic signature: (Unforgeability of electronic signatures must be assured).

3.1.2 Subjects

Subject	Definition
S.User	End user of the TOE which can be identified as S.Admin or S.Signatory
S.Admin	User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions.
S.Signatory or S.Sigy	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.

3.1.3 Threat agent

Subject	Definition
S.OFFCARD	Attacker. A human or a process acting on his behalf being located outside the TOE. The

	main goal of the S.OFFCARD attacker is to access Application sensitive information. The attacker has a **high level potential attack** and **knows no secret**.

3.2 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 and the SVD in the qualified certificate by an advanced signature of the CSP.

A.SCA
Trustworthy signature-creation application
The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

A.SCD_Generate
Trustworthy SCD/SVD generation
If a party other than the signatory generates the SCD/SVD-pair of a signatory, then
(a) this party will use a SSCD for SCD/SVD-generation,
(b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and
(c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory.
(d) The generation of the SCD/SVD is invoked by authorized users only
(e) The SSCD Type1 ensures the authenticity of the SVD it has created an exported

3.3 THREATS

The TOE is required to counter the threats described hereafter.
A threat agent wishes to abuse the assets either by functional attacks or by environmental manipulation, by specific hardware manipulation, by a combination of hardware and software manipulations or by any other type of attacks.
The threats of the TOE are those defined in [PP-SSCD-KI], [PP-SSCD-KG].The present Security Target deals with the threats of [PP-SSCD-KI] and [PP-SSCD-KG].
The assets of [PP-JCS-Open] are studied in [ST-PLTF].

T.Hack_Phys
Physical attacks through the TOE interfaces
An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat addresses all the assets.

T.SCD_Divulg
Storing ,copying, and releasing of the signature-creation data
An attacker can store, copy, the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE.

T.SCD_Derive
Derive the signature-creation data
An attacker derives the SCD from public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.

T.Sig_Forgery
Forgery of the electronic signature
An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

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

T.SVD_Forgery
Forgery of signature-verification data
An attacker forges the SVD presented by the TOE to the CGA. This result in loss of SVD integrity in the certificate of the signatory.

T.DTBS_Forgery
Forgery of the DTBS-representation
An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intended to sign.

T.SigF_Misuse
Misuse of the signature creation function of the TOE
An attacker misuses the signature-creation function of the TOE to create 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.

3.4 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-KI] and [PP-SSCD-KG].

P.CSP_QCert
Qualified certificate
The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.

P.Qsign
Qualified electronic signatures
The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate and is created by a SSCD.

P.Sigy_SSCD
TOE as secure signature-creation device

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

P.Pre-personalisation *Strong authentication in pre-personalisation*
During pre-personalisation, The TOE protects itself with strong authentication.

3.5 COMPATIBILITY BETWEEN SECURITY ENVIRONMENTS OF [ST-IAS] AND [ST-PLTF]

3.5.1 Compatibility between threats of [ST-IAS] and [ST-PLTF]

T.Hack_Phys and T.SCD_Divulg are included in T.Physical
T.SCD_Derive, T.Sig_Forgery, T.DTBS_Forgery, T.Sig_Repud, T.SVD_Forgery, and T.SigF_Misuse are threats specific to [ST-IAS] and they do not conflict with the threats of [ST-PLTF].
We can therefore conclude that the threats of [ST-IAS] and [ST-PLTF] are consistent.

3.5.2 Compatibility between OSP of [ST-IAS] and [ST-PLTF]

P.CSP_QCert, P.Qsign, and P.Sigy_SSCD and P.Pre-personalisation are OSP specific to [ST-IAS] and they do not conflict with the OSP of [ST-PLTF].
We can therefore conclude that the OSP of [ST-IAS] and [ST-PLTF] are consistent.

3.5.3 Compatibility between assumptions of [ST-IAS] and [ST-PLTF]

A.CGA, A.SCA, and A.SCD_Generate are assumptions specific to [ST-IAS] and they do no conflict with the assumptions of [ST-PLTF].
We can therefore conclude that the assumptions of [ST-IAS] and [ST-PLTF] are consistent.

3.6 JUSTIFICATIONS FOR ADDING ASSUMPTIONS ON THE ENVIRONMENT

3.6.1.1 Additions to [PP-SSCD-KG]

The only additional assumption on the environment is A.SCD_Generate. This assumption deals with the SCD generation when the SCD is generated off-TOE and imported afterwards. These two operations are outside the scope of [PP-SSCD-KG]. Therefore the added assumption does not weaken the TOE.

4. SECURITY OBJECTIVES

The security objectives in this Security Target are those named and described in [PP-SSCD-KI] and [PP-SSCD-KG].
They cover the following aspects:

- The security objectives for the TOE,
- The security objectives for the environment.

The security objectives stated in [PP-JCS-Open] can be found in [ST-PLTF].

4.1 SECURITY OBJECTIVES FOR THE TOE

4.1.1 Common to Type 2 and Type 3

OT.Lifecycle_Security
Lifecycle security
The TOE shall detect flaws during the initialization, personalization and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-generation or re-import.

OT.SCD_Secrecy
Secrecy of signature-creation data
The secrecy of the SCD (used for signature generation) is reasonably assured against attacks with a high attack potential.

OT.Sig_Secure
Cryptographic security of the electronic signature
The TOE generates electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the electronic signatures. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.
OT.EMSEC_Design
Provide physical emanations security
Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.

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

OT.Tamper_Resistance
Tamper resistance
The TOE prevents or resists physical tampering with specified system devices and components.

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

OT.Sigy_SigF
Signature generation function for the legitimate signatory only

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

OT.SCD_SVD_Corresp

Correspondence between SVD and SCD

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

OT.SVD_Auth_TOE

TOE ensures authenticity of the SVD

The TOE provides means to enable the CGA to verify the authenticity of the SVD that has been exported by that TOE.

4.1.2 Type 2 specific

OT.SCD_Transfer

Secure transfer of SCD between SSCD

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

4.1.3 Type 3 specific

OT.Init

SCD/SVD generation

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

OT.SCD_Unique

Uniqueness of the signature-creation data

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

4.1.4 Extensions

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

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

4.2 Security Objectives for the Operational Environment

This section describes the security objectives for the environment.

The IT environment of the TOE is composed of the Certification Generation Application (CGA) and the Signature Creation Application (SCA).

4.2.1 Common to Type 2 and Type 3

OE.CGA_Qcert
Generation of qualified certificates
The CGA generates qualified certificates which include inter alia
(a) the name of the signatory controlling the TOE,
(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,
(c) the advanced signature of the CSP.

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

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

OE.SCA_Data_Intend
Data intended to be signed
The SCA
(a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,
(b) sends the DTBS-representation to the TOE and enables verification of the integrity of DTBS-representation by the TOE,
(c) attaches the signature produced by the TOE to the data or provides it separately.

4.2.2 Specific to Type 2

OE.SCD_SVD_Corresp
Correspondence between SVD and SCD
The SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSVD Type1 shall prove the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.

OE.SCD_Transfer
Secure transfer of SCD between SSCD
The SSCD Type1 shall ensure the confidentiality of the SCD transferred to the TOE. The SSCD Type1 shall prevent the export of a SCD that already has been used for signature generation by the SSCD Type 2. The SCD shall be deleted from the SSCD Type1 whenever it is exported into the TOE.

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

5. EXTENDED COMPONENTS DEFINITION

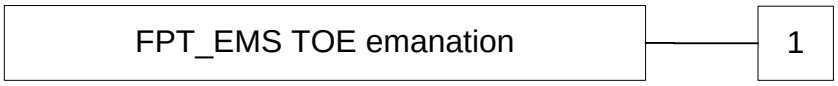
This ST uses one component defined as extensions to CC part 2: FPT_EMS.1 which is defined as FPT_EMSEC.1 in protection profile [PP-SSCD-KI] and [PP-SSCD-KG].

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the 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 behavior
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 other components.

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].

6. SECURITY REQUIREMENTS

6.1 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] and [PP-SSCD-KG].

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

Definition of security attributes:

The security attributes for the subjects, TOE components and related status are:

Groups of security attributes [USER, SUBJECT OR OBJECT THE ATTRIBUTE IS ASSOCIATED WITH]	**ATTRIBUTES**	**ATTRIBUTES STATUS**
GENERAL ATTRIBUTE GROUP		
[User]	ROLE	ADMINISTRATOR, SIGNATORY
INITIALISATION ATTRIBUTE GROUP		
[USER]	SCD/SVD MANAGEMENT	AUTHORISED / NOT AUTHORISED
[SCD]	SECURE SCD IMPORT ALLOWED	NO/YES
SIGNATURE-CREATION ATTRIBUTE GROUP		
[SCD]	SCD OPERATIONAL	NO/YES
[DTBS]	SENT BY AN AUTHORISED SCA	NO/YES

6.1.1 Class Cryptographic Support (FCS)

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

Hierarchical to: No other components
Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 /SCD 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*].

iteration	algorithm	Key size	standards
/RSA	**RSA CRT key generation**	**1024, 1536, 2048**	**none (generation of random numbers and Miller- Rabin primality testing)**
/ECC	**ECC key generation**	**160, 224, 256, 384, 512, 521**	**None**

Table 3: FCS_CKM.1/SCD refinement

Application note: Type 3 only
Application note:

FCS_CKM.1/SCD is named FCS_CKM.1 in [PP-SSCD-KI] and [PP-SSCD-KG]. The new naming clarifies 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_CKM.2 Cryptographic key distribution or
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*].

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

Table 4: FCS_CKM.1/Session refinement

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 **Secure erasing of the value** that meets the following: **None**.

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

Table 5: FCS_CKM.4 refinement

Application note:
FCS_CKM.4/SCD is named FCS_CKM.4 in [PP-SSCD-KI] and [PP-SSCD-KG]. The new naming clarifies 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 /Session | The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Secure erasing of the value** that meets the following: **None**.

iteration	when
/TDES	End of session
/AES	End of session

Table 6: FCS_CKM.4 refinement

FCS_COP.1/CORRESP Cryptographic operation – SCD/SVD correspondence verification

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 /CORRESP | The TSF shall perform SCD/SVD correspondence verification 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*].

iteration	algorithm	key size	standards
/CORRESP-RSA	**RSA CRT key generation**	**1024, 1536, 2048**	**none (generation of random numbers and Miller-Rabin primality testing)**
/CORRESP-ECC	**ECC key generation**	**160, 224, 256, 384, 512, 521**	**None**

Table 7: FCS_COP.1/CORRESP refinement

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*].

iteration	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,**	**[TR-03111] ECDSA SHA**

iteration	operation	algorithm	key size	standards
			and 521	

Table 8: FCS_COP.1/DSC refinement

Application note:
FCS_COP.1/DSC is named in FCS_COP.1/SIGNING [PP-SSCD-KI] and [PP-SSCD-KG].

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 /Session 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*].

iteration	operation	algorithm	key size	standards
/ENC-TDES	**Encryption & decryption**	**TDES**	**112**	**[SP800-67]**
/ENC-AES	**Encryption & decryption**	**AES**	**128**	**[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**	**[FIPS197] AES 128 NOPAD**

Table 9: FCS_COP.1/Other refinement

6.1.2 Class FDP User Data Protection

FDP_ACC.1 Subset access control

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

FDP_ACC.1 /Initialisation SFP The TSF shall enforce the Initialisation SFP on Generation of SCD/SCD pair by User.

Application note: Type 3 only

FDP_ACC.1 /SVD transfer SFP The TSF shall enforce the SVD transfer SFP on import and on export of SVD by User.

Application note:
When SCD is imported into the TOE, FDP_ACC.1/SVD Transfer SFP will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification. This is not the case in this TOE. (Type 2)

When SCD is generated in the TOE, FDP_ACC.1/SVD Transfer SFP will be required to export the SVD to the CGA for certification. (Type 3).

FDP_ACC.1.1 /SCD Import SFP	The TSF shall enforce the SCD Import SFP on Import of SCD by User.

Application note: Type 2 only.

FDP_ACC.1.1 /Personalisation SFP	The TSF shall enforce the Personalisation SFP on Creation of RAD by Administrator.
FDP_ACC.1.1 /Signature-creation SFP	The TSF shall enforce the Signature-creation SFP on Sending of DTBS-representation by SCA and Signing of DTBS-representation by Signatory.

FDP_ACF.1 Security attribute based access control

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

Initialisation SFP

FDP_ACF.1.1 /Initialisation SFP	The TSF shall enforce the Initialisation SFP to objects based on the following: General attribute group and Initialisation attribute group

Application note: Type 3 only.

FDP_ACF.1.2 /Initialisation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute “role” set to “Administrator” or set to “Signatory” and with the security attribute “SCD / SVD management” set to “authorized” is allowed to generate SCD/SVD pair,
FDP_ACF.1.3 /Initialisation SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4 /Initialisation SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: The user with the security attribute “role” set to “Administrator” or set to “Signatory” and with the security attribute “SCD / SVD management” set to “not authorized” is not allowed to generate SCD/SVD pair.

SVD Transfer SFP

FDP_ACF.1.1 /SVD_Transfer	The TSF shall enforce the SVD Transfer SFP to objects based on the following: General attribute group.
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled

/SVD_Transfer	subjects and controlled objects is allowed: The user with the security attribute “role” set to “Administrator” or “Signatory” 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

SCD_Import SFP

FDP_ACF.1.1 /SCD_Import	The TSF shall enforce the SCD Import SFP to objects based on the following: General attribute group and Initialisation attribute group.
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: The user with the security attribute “role” set to “Administrator” or to “Signatory” and with the security attribute “SCD / SVD management” set to “authorized” is allowed to import SCD if the security attribute “secure SCD import allowed” is set to “yes”,
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: (a) The user with the security attribute “role” set to “Administrator” or to “Signatory” and with the security attribute “SCD / SVD management” set to “not authorized” is not allowed to import SCD if the security attribute “secure SCD import allowed” is set to “yes”. (b) The user with the security attribute “role” set to “Administrator” or to “Signatory” and with the security attribute “SCD / SVD management” set to “authorized” is not allowed to import SCD if the security attribute “secure SCD import allowed” is set to “no”.

Application note: Type 2 only.

Personalisation SFP

FDP_ACF.1.1 /Personalisation	The TSF shall enforce the Personalisation SFP to objects based on the following: General attribute group
FDP_ACF.1.2 /Personalisation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute “role” set to “Administrator” is allowed to create the RAD.
FDP_ACF.1.3 /Personalisation	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4 /Personalisation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

Signature_Creation SFP

FDP_ACF.1.1 /Signature_Creation	The TSF shall enforce the Signature Creation SFP to objects based on the following: General attribute group and Signature-creation attribute group
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: User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".
FDP_ACF.1.3 /Signature_Creation	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: (a) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS which is not sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes". (b) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no".

FDP_ETC.1 Export of user data without security attributes

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1	The TSF shall enforce the SVD transfer SFP when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.

Application note:

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

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

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow 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: SCD shall be sent by an Authorized SSCD.

Application note:

A SSCD of Type 1 is authorised to send SCD to a SSCD of Type 2, if it is designated to generate the SCD for this SSCD of Type 2 and to export the SCD for import into this SSCD of Type 2. Authorised SSCD of Type 1 are able to establish a trusted channel to the SSCD of Type 2 for SCD transfer as required by FTP_ITC.1.3/SCD export.

Type 2 only.

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

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

FDP_ITC.1.1 /DTBS The TSF shall enforce the Signature_Creation SFP when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3 /DTBS The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: DTBS_representation shall be sent by an Authorized SCA.

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, VAD, RAD.

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

1. SCD
2. RAD
3. 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 Signatory about integrity error.

DTBS-representation

The DTBS representation temporarily stored by TOE has the user data attribute “integrity checked stored data”

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 Signatory about integrity error.

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow 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 be able to receive SCD in a manner protected from unauthorized disclosure.

Application note: Type 2 only.

FDP_UIT.1 Data exchange integrity

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

FDP_UIT.1.1 /SVD Transfer: The TSF shall enforce the SVD Transfer SFP to be able to transmit user data in a manner protected from modification and insertion errors.

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

FDP_UIT.1.1 /TOE DTBS: The TSF shall enforce the Signature creation SFP to be able to receive the DTBS-representation in a manner protected from modification,deletion and insertion errors.

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

6.1.3 Class FIA Identification and Authentication

FIA_AFL.1/PERSO Authentication failure handling

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 10**] unsuccessful authentication attempts occurs related to consecutive failed **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 10: FIA_AFL.1/PERSO refinements

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_ATD.1 User attribute definition

Hierarchical to: No other components
Dependencies: No dependencies

FIA_ATD.1.1 — The TSF shall maintain the following list of security attributes belonging to individual users: RAD.

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. Self test according to FPT_TST.1.
2. Identification of the user by means of TSF required by FIA_UID.1.
3. **No other Signature generation related 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.

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 [Identification of the user by means of TSF required by FIA_UID.1]
2 [Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP_ITC.1/SCD import]
3 [Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE]
4 [Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import]
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.
PIN or BioPIN could be used for user authentication.

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. 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 /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:	No dependencies

FIA_UID.1.1 /SIG	The TSF shall allow 1. Establishing a trusted channel between the TOE and a SSCD ofType 1 by means of TSF required by FTP_ITC.1/SCD import. 2. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE. 3. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import.] 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.

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

6.1.4 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 Signatoryy**.**

FMT_MSA.1/Signatory Management of security attributes

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow 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 Signatory**.**

FMT_MSA.1/AdminKG Management of security attributes

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

FMT_MSA.1.1 /AdminKG The TSF shall enforce the Initialisation SFP to restrict the ability to modify the security attributes SCD / SVD management to Administrator**.**

Application note:

The Initialisation SFP enforcing comes from Type 3

FMT_MSA.1/AdminKI Management of security attributes

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow 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 Administrator**.**

Application note:

The SCD Import SFP enforcing comes from Type 2.

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow 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 Administrator to specify alternative initial values to override the default values when an object or information is created.

Application note: Type 3 only.

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 Administrator to specify alternative initial values to override the default values when an object or information is created.

Application note: Type 2 only.

FMT_MSA.4/Keygen Static attribute value inheritance

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow 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.

FMT_MSA.4/KeyImport Static attribute value inheritance

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow 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 without the S.Sigy being authenticated the same time 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 being authenticated the same time the security attribute "SCD operational" of the SCD shall be set to "yes" after import of the SCD as a single operation.

Application note:
FMT_MSA.4/KeyGen and FMT_MSA.4/KeyImport are not defined in the claimed PP [CWA-14168-2] and [CWA-14168-3]; they have been introduced in [EN-14168-2] and [EN-14168-3]. The ST writer has elected to introduce them in this ST as they provide additional information on security attributes.

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 Administrator.

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 Signatory.

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 Administrator and Signatoryy

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

6.1.5 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 11: 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 11: conditions triggering tests

6.1.6 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 a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 /SCD import: The TSF shall permit the remote 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:
The mentioned "remote trusted IT product" in FTP_ITC.1/SCD import is an SSCD of type 1.

Application note:
The SCD Import must be protected in Integrity. This protection must be ensured by crypto mechanisms in the TOE. No “Trusted Environment” can ensure this integrity.
Type 2 only.

FTP_ITC.1/SVD transfer Inter-TSF trusted Channel

Hierarchical to: No other components
Dependencies: No dependencies

FTP_ITC.1.1 /SVD transfer: The TSF shall provide a communication channel between itself and a remote 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 transfer: The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3 / SVD transfer: The TSF or the CGA shall initiate communication via the trusted channel for SVD transfer.

Application note:
The mentioned "remote trusted IT product" in FTP_ITC.1/SVD transfer is a CGA.

Application note:
The SVD Transfer must be protected in Integrity. This protection can be ensured by crypto mechanisms in the TOE. It can also be ensured by a “Trusted Environment”. At personalization time, the Issuer will be able to assess if the usage environment will be a “Trusted Environment”.

FTP_ITC.1/DTBS import Inter-TSF trusted Channel

Hierarchical to: No other components
Dependencies: No dependencies

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT

/DTBS import	product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 /DTBS import	The TSF shall permit the SCA to initiate communication via the trusted channel.
FTP_ITC.1.3 /DTBS import	The TSF or the SCA shall initiate communication via the trusted channel for signing DTBS-representation.

Application note:
The mentioned "another trusted IT product" in FTP_ITC.1/DTBS import is an SCA.

Application note:
The DTBS Import must be protected in Integrity. This protection can be ensured by crypto mechanisms in the TOE. It can also be ensured by a “Trusted Environment”. At personalization time, the Issuer will be able to assess if the usage environment will be a “Trusted Environment”.

FTP_TRP.1/TOE Trusted Path

Hierarchical to: No other components
Dependencies: No dependencies

FTP_TRP.1.1 /TOE	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure..
FTP_TRP.1.2 / TOE	The TSF shall permit local users to initiate communication via the trusted path.
FTP_TRP.1.3 / TOE	The TSF shall require the use of the trusted path for initial user authentication.

Application note:
The RAD/VAD Import must be protected in Integrity and confidentiality. This protection can be ensured by crypto mechanisms in the TOE. It can also be ensured by a “Trusted Environment”. At personalization time, the Issuer will be able to assess if the usage environment will be a “Trusted Environment”.

6.2 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. TOE SUMMARY SPECIFICATION

7.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the IAS applet and by the chip.
The security functions provided by the platform are described in [ST-PLTF].

7.1.1 SF provided by IAS Applet

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

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 12: *TOE security functions list*

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

- The identification and authentication in personalisation phase as defined in :
  - FIA_AFL.1/PERSO , FIA_UAU.1/PERSO and FIA_UID.1/PERSO
- The identification and authentication in operational phase as defined in :
  - FIA_ATD.1,FIA_AFL.1/SIG , FIA_UAU.1/SIG and FIA_UID.1/SIG

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

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, FCS_COP.1/CORRESP** 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**,

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

- Access management as defined in **FDP_ACC.1** and **FDP_ACF.1** SFR,
- Data input and output as defined in **FDP_ETC.1**, **FDP_ITC.1/SCD**, and **FDP_ITC.1/DTBS**,
- 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**, **FDP_UIT.1/SVD Transfer**, and **FDP_UIT.1/TOE DTBS**,
- Secure channel and secure path as defined in **FTP_ITC.1/SCD Import**, **FTP_ITC.1/SVD Transfer**, **FTP_ITC.1/DTBS Import**, **FTP_TRP.1/TOE**,

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**,
- Secure unavailability of sensitive data as defined in **FDP_RIP**.

7.1.2 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	Protection against snooping
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

Table 13: Security Functions provided by the Multiapp V3 Platform

These SF are described in [ST-PLTF].