MultiApp v2

IAS Classic v3

Common Criteria / ISO 15408
Security Target – Public version
EAL4+

CONTENT

FIGURES

1. ST INTRODUCTION

1.1 ST IDENTIFICATION

Title:	MultiApp v2 - IAS Classic V3 Public Security Target
Version:	v1.1 issued 08 June 2011
ST reference:	ST_D1201112
Origin:	Gemalto
Author:	Antoine DE LAVERNETTE
Product identification:	MultiAppID v2
Security Controllers:	IFX SLE66CLX360PEM m1588 IFX SLE66CLX360PE m1587 IFX SLE66CLX800PEM m1580 IFX SLE66CLX800PE m1581 IFX SLE66CX800PE m1599 IFX SLE66CLX1440PEM m2090 IFX SLE66CLX1440PE m2091 IFX SLE66CX1440PE m2093
TOE identification:	IAS Classic V3 on MultiAppID v2
TOE documentation:	Operational User Guidance [OPE_IAS] Preparative procedures [PRE_IAS]

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.

CPLC field	Length	Value
IC Fabricator	2	IFX
IC Type	2	SLE66CLX360PEM SLE66CLX360PE SLE66CLX800PEM SLE66CLX800PE SLE66CX800PE SLE66CLX1440PEM SLE66CLX1440PE SLE66CX1440PE
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

CPLC field	Length	Value
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.
IC Pre-personalization Eqiopment 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 MultiAppID v2 platform and the electronic signature application IAS Classic.

The platform includes the hardware and the operating system.

The IC is evaluated in conformance with [PP-IC-0002].

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

The IAS Classic application is evaluated in conformance with [PP-SSCD-T2] and [PP-SSCD-T3].

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-2009-07-001, version 3.1 rev 3, July 2009
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2009-07-002, version 3.1 rev 3, July 2009
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2009-07-003, version 3.1 rev 3, July 2009
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology CCMB-2009-07-004, version 3.1 rev 3, July 2009
[CR-IC]	Either [CR-IC-800] or [CR-IC-1440]
[CR-IC-800]	Certification Report, BSI-DSZ-CC-0626-2009 (15-04-2009) SLE66CLX360PEM / m1588 – k11/a15 SLE66CLX800PEM / m1580 - k11/a15
[CR-IC-1440]	Certification Report, BSI-DSZ-CC-0523-2008-MA-01 (09-06-2009) SLE66CLX1440PEM / m2090 - a13
[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_0002]	*Smartcard IC Platform protection Profile* BSI-PP-0002, version 1.0, July 2001

[PP-IC-0035]	*Smartcard IC Platform protection Profile* BSI-PP-0035
[PP-SSCD-T2]	Protection Profile – Secure Signature-Creation Device Type2 BSI-PP-0005, Version 1.04, 25th July 2001
[PP-SSCD-T3]	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-CC-PP-2010-03, Version 2.6, April, 19th 2010
[ST-IC]	*Either* [ST-IC-1440] or [ST-IC-800]
[ST-IC-1440]	*Security Target, IFX SLE66CLX1600PEx and derivates* *Version 1.2 – 2008–09-19*
[ST-IC-800]	*Security Target, IFX SLE66CLX800PEx and derivates* *Version 1.2 – 2008–01-09*
[GP211]	*Global Platform Card Specification v 2.1.1 - March 2003*

Internal References

[IGS]	Installation, Generation and Start Up Procedures
[PRE_IAS]	D1144772 Preparative procedures - IAS Classic v3 on MultiApp v2
[OPE_IAS]	D1144771 Operational User Guidance - IAS Classic v3 on MultiApp v2

1.4 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]).

1.5 TOE OVERVIEW

1.5.1 TOE description

IAS Classic 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.

Three Protection Profiles have been defined. The SSCD PP Type 1, which is a SCD/SVD generation component without signature creation and verification. The SCD generated on a SSCD Type 1 shall be exported to a SSCD Type 2 over a trusted channel [PP/SSCD-TYPE1].

- The SSCD PP for a TOE Type 2, which is a Signature creation and verification component [PP-SSCD-T2]. This device imports the SCD from a SSCD Type 1
- The SSCD PP for a TOE Type 3, which is combination of the TOE Type 1 and Type 2 – i.e Generation and Signature creation/verification component [PP-SSCD-T3].

In this document the terminology of [PP-SSCD-T2] and [PP-SSCD-T3] 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.

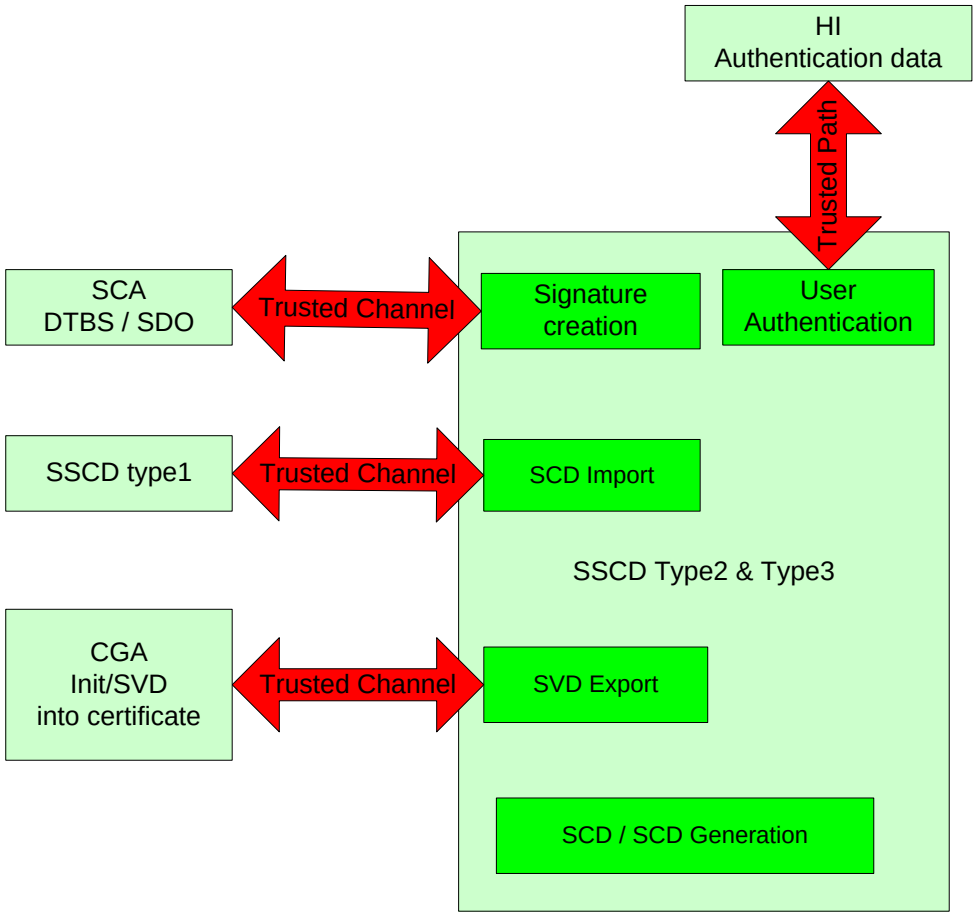


Figure 1: TOE operations

The IAS Classic application is compliant to both the SSCD Type 2 and Type 3 and 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 Classic is aimed to create legal valid signatures and therefore provides mechanisms to ensure the secure signature creation as:

- Authentication of the signatory (by PIN),
- Authentication of the administrator (mutual authentication):
  - Symmetric scheme with TDES or
  - Asymmetric scheme with Diffie-Hellman
- 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.

1.6 TOE BOUNDARIES

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

- The underlying Integrated Circuit
- The MultiAppID v2 platform (JavaCard platform)
- The IAS Application.

Figure 2: TOE Boundaries gives a description of the TOE and its boundaries.

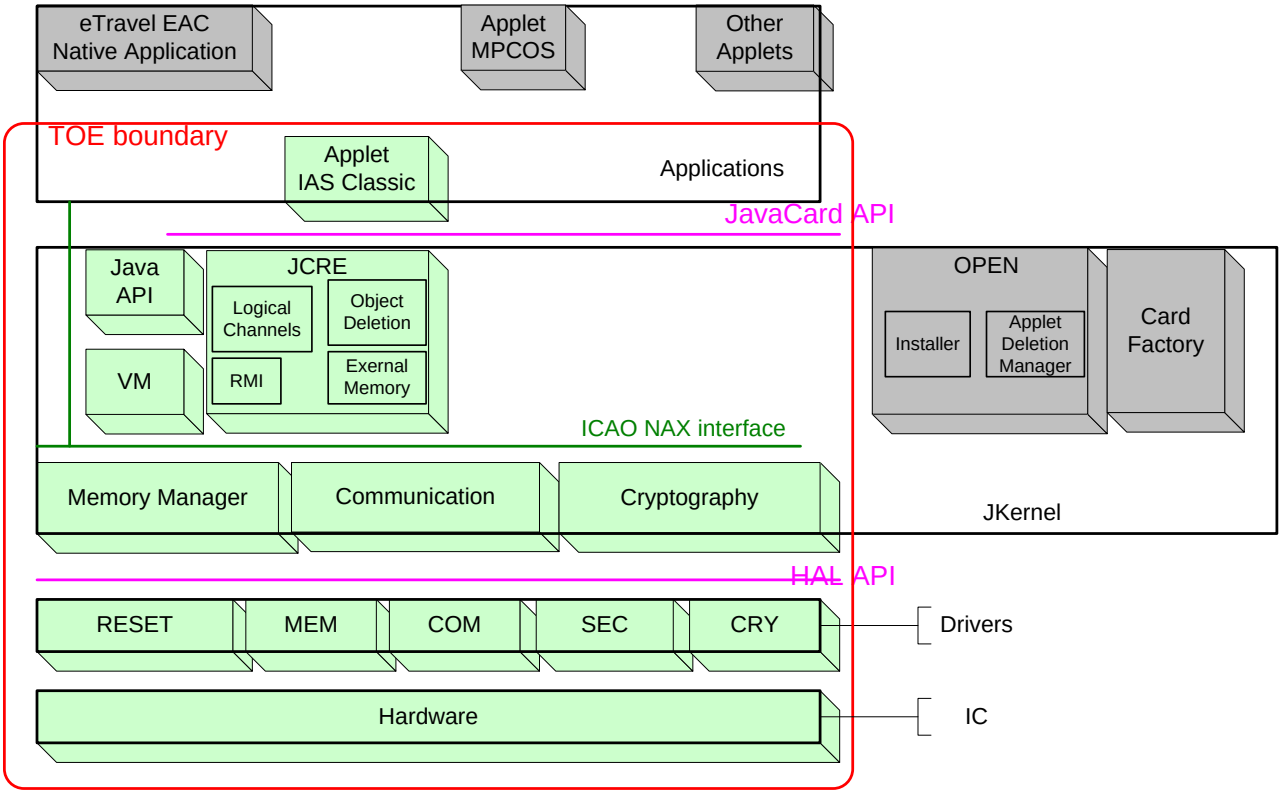


Figure 2: TOE Boundaries

1.7 TOE LIFE-CYCLE

1.7.1 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:

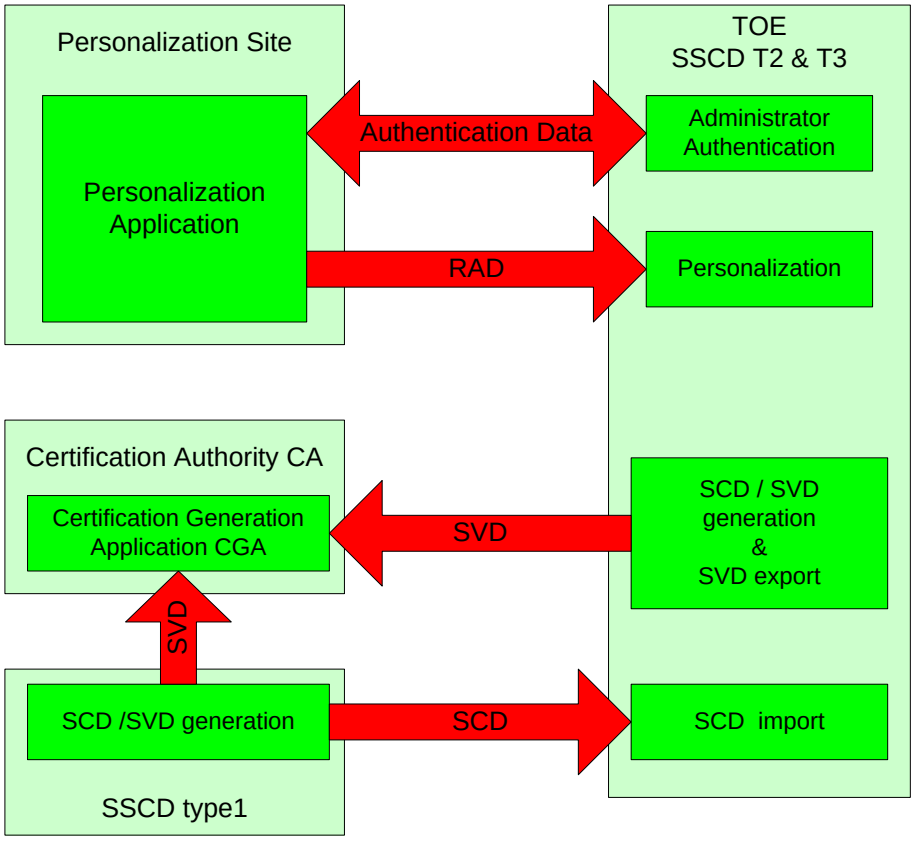


Figure 3: TOE Personalization

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 in the SSCD type1.

The SCD / SVD pair is generated in the SSCD type1.

The SCD is sent to the TOE.

The SVD is sent to the CGA.

The CGA generates the certificate.

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

The SCD / SVD pair is generated in the TOE.

The SVD is sent to the CGA.

The CGA generates the certificate.

Phase 4 “Operational Use”

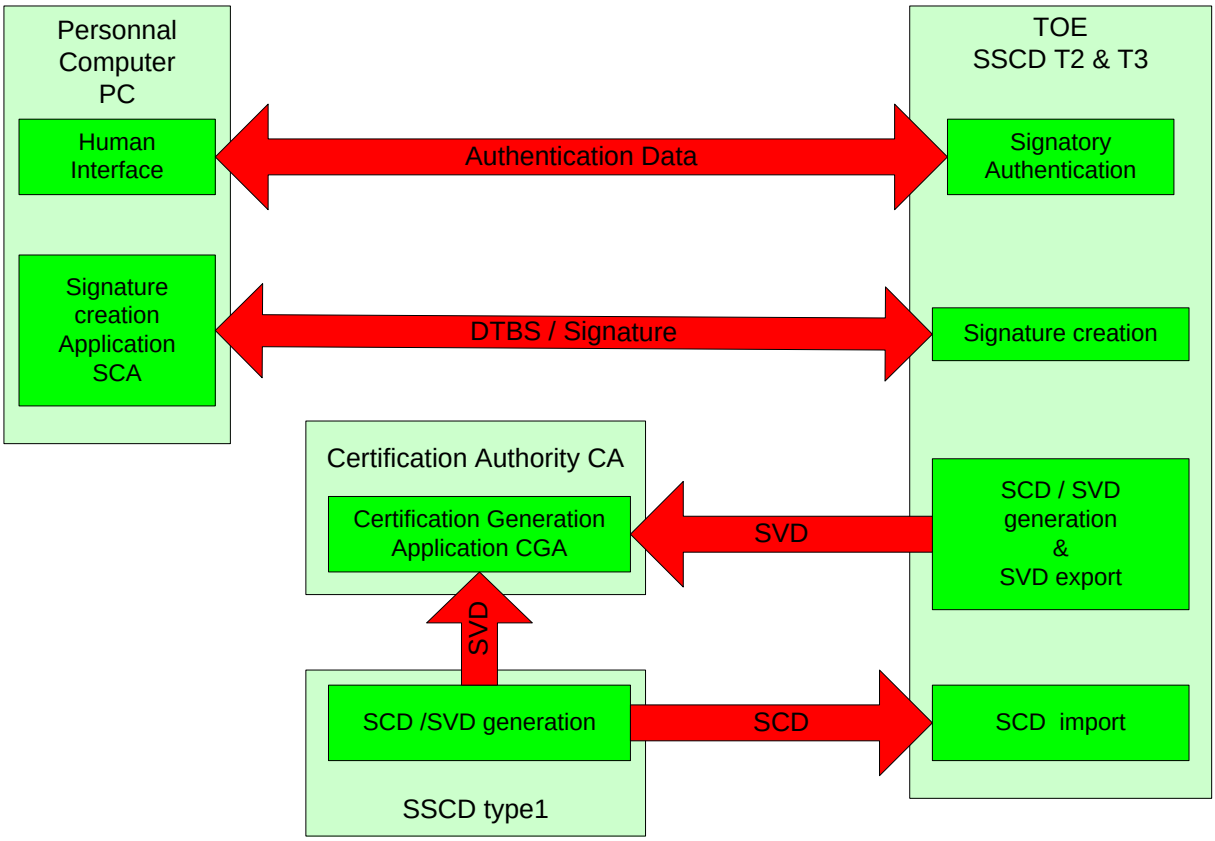


Figure 4: TOE Operational Use

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

The SCD / SVD pair is generated in the TOE.

The SVD is sent to the CGA.

The CGA generates the certificate.

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.

1.7.2 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

1.7.3 Init on module at Gemalto site

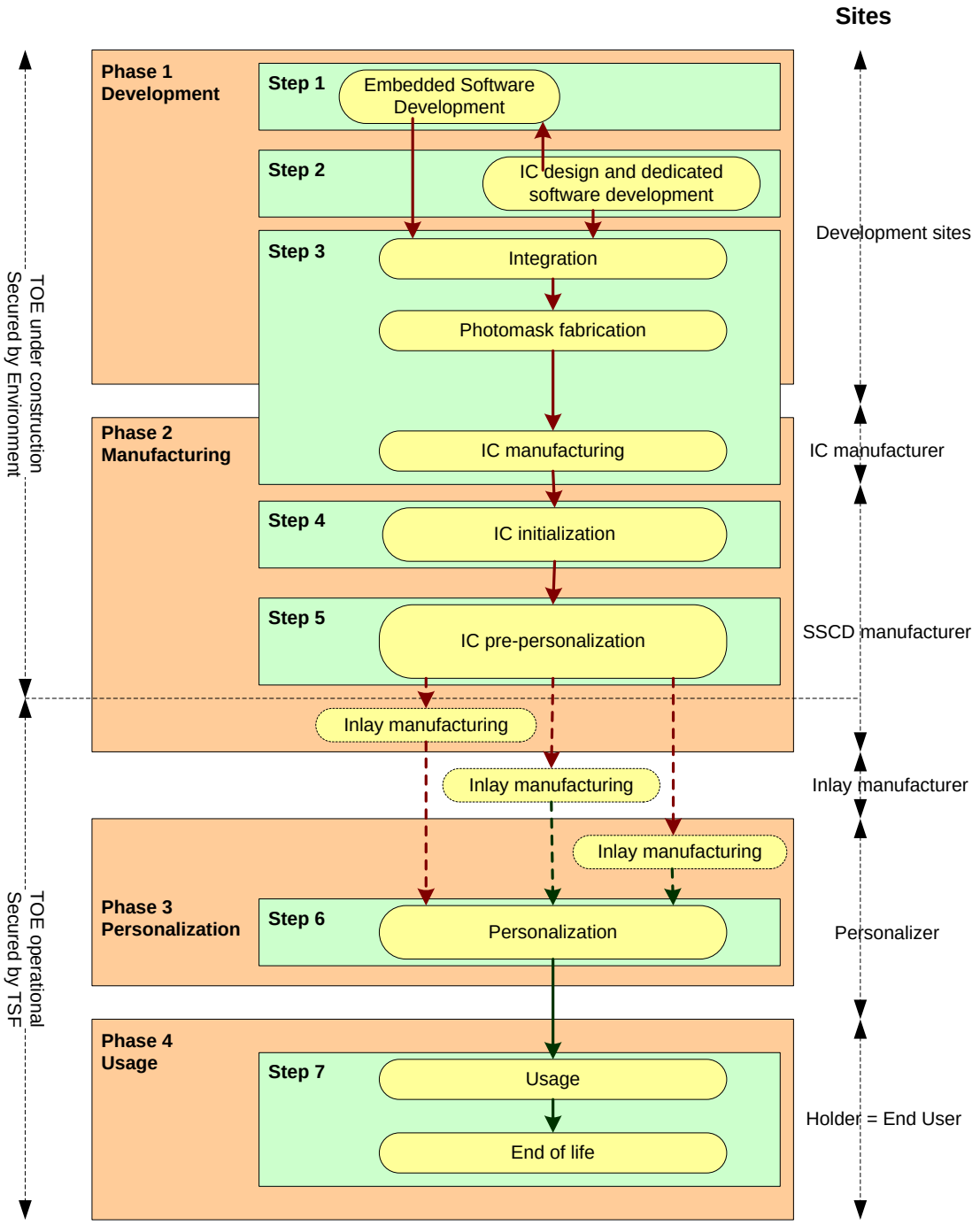


Figure 5: LC1: Init on module at Gemalto site

Figure 5: LC1: Init on module at Gemalto site describes the standard Life Cycle. The module is manufactured at the founder site. It is then shipped to Gemalto site where it is initialized and pre-personalized and then shipped to the Personalizer directly or after through the Inlay manufacturer.

During the shipment from Gemalto to the Personalizer, the module is protected by a diversified key.

1.7.4 Init on module at Founder site

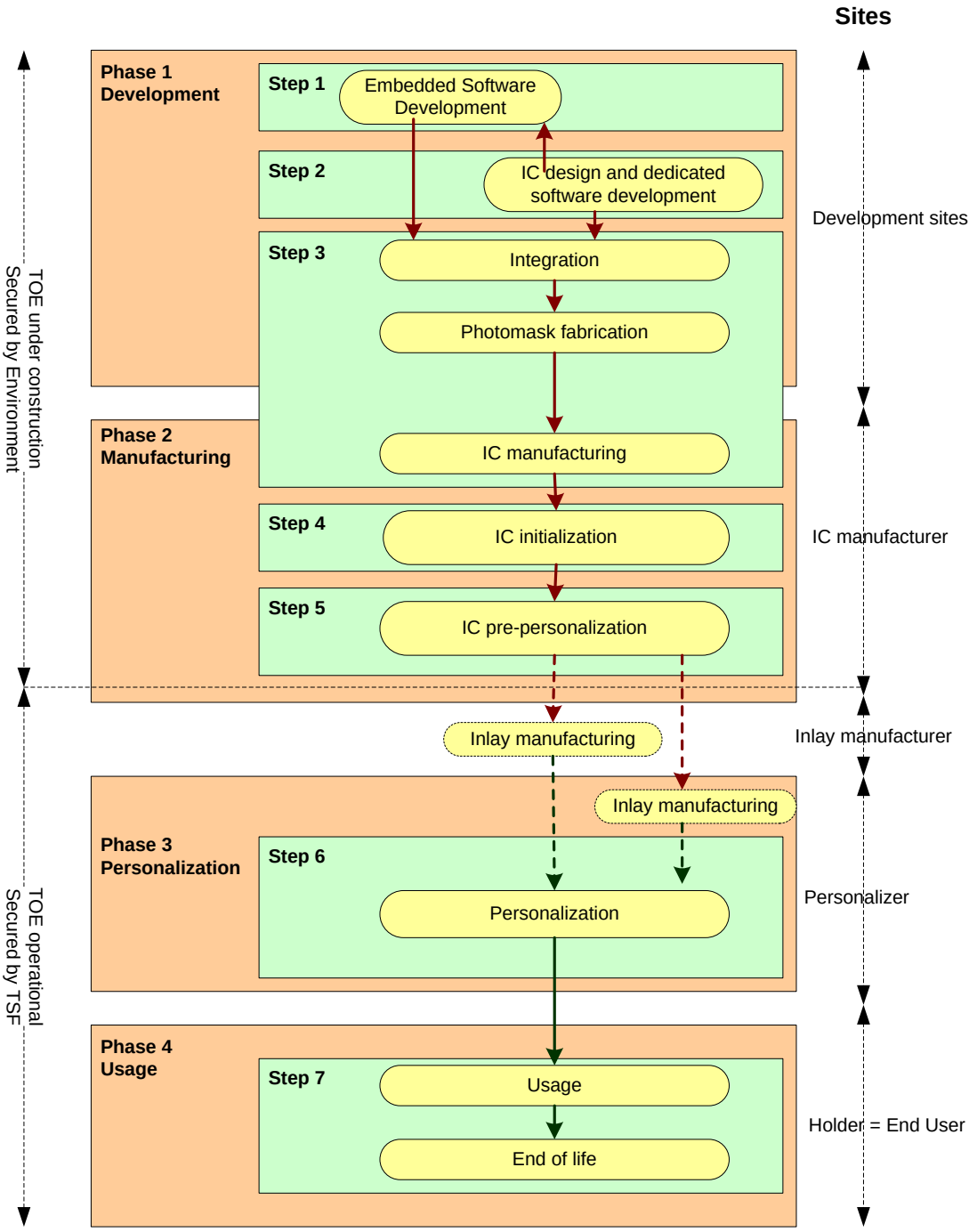


Figure 6: LC2 Init on module at Founder site

LC2 is an alternative to LC1. *Figure 6: LC2 Init on module at Founder site* describes the Life Cycle when the customer whishes to receive wafers directly from the founder. In this case, initialization and pre-personalization, which include sensitive operations such as the loading of patches, take place at the founder site. The creation of files is started by the founder and completed by the personalizer.

During the shipment from the founder to the Personalizer, the module is protected by a diversified key.

1.7.5 Init on inlay at Gemalto site

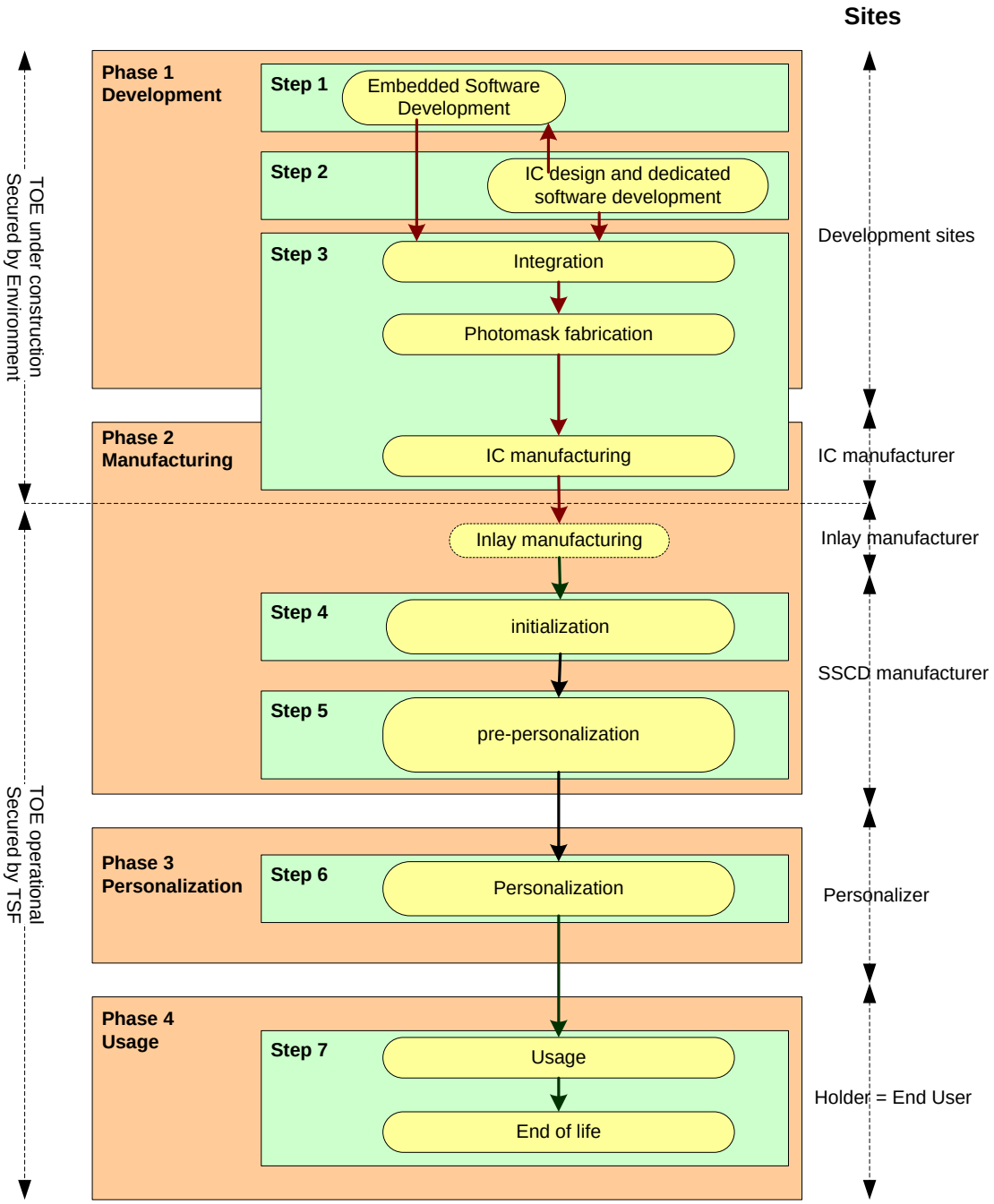


Figure 7: LC3: Init on inlay at Gemalto site

LC3 is another alternative to LC1. *Figure 7: LC3: Init on inlay at Gemalto site* describes the Life Cycle when the Gemalto whishes 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 MultiAppID v2 claiming conformance to [PP-JCS-Open]. The hardware part of the composite evaluation is covered by the certification report [CR-IC].

2.2 PP CLAIM,

This MultiAppID v2 IAS Classic security target claims demonstrable conformance to the Protection Profiles “Secure Signature-creation Device Type 2”, PP-005 version 1.04 ([PP-SSCD-T2]) and “Secure Signature-creation Device Type 3”, PP-006 version 1.05 ([PP-SSCD-T3]).

The evaluation is a composite evaluation and uses the results of the CC evaluation of the MultiAppID v2 platform. The platform embedded software has been evaluated at level EAL 5+. However the security problem definition, the objectives, and the SFR of the platform are not described in this document.

The MultiAppID v2 JCS security target claims strict conformance to the Protection Profile “JavaCard System – Open configuration”, ANSSI-CC-PP-2010-03, Version 2.6 ([PP-JCS-Open]).

2.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL4 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-T2], [PP-SSCD-T3] and [PP-IC-0002].

The present Security Target deals with the assets of [PP-SSCD-T2] and [PP-SSCD-T3]. The assets of [PP-IC-0002] are studied in [ST-IC].

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	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-T2], [PP-SSCD-T3] and [PP-IC-0002].

The present Security Target deals with the threats of [PP-SSCD-T2] and [PP-SSCD-T3]. The threats of [PP-IC-0002] are studied in [ST-IC].

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-T2] and [PP-SSCD-T3].

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.

4. SECURITY OBJECTIVES

The security objectives in this Security Target are those named and described in [PP-SSCD-T2] and [PP-SSCD-T3].

They cover the following aspects:

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

The security objectives stated in [PP-IC_0002] can be found in [ST-IC].

4.1 SECURITY OBJECTIVES FOR THE TOE

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.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.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.

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.SCD_Transfer

Secure transfer of SCD between SSCD

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

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.

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.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.

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).

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 Type1. 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.

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.

5. EXTENDED COMPONENTS DEFINITION

This ST uses one component defined as extensions to CC part 2: FPT_EMSEC.1 which is defined in protection profile [PP-SSCD-T2] and [PP-SSCD-T3].

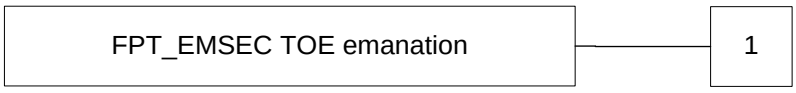
The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena 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_EMSEC)" is specified as follows.

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMSEC.1 TOE emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No other components.

FPT_EMSEC.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_EMSEC.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-T2] and [PP-SSCD-T3].

[ST-IC] deals with the security functional requirements of [PP-IC_0002].

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 Cryptographic key generation

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/RSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA key generation** and specified cryptographic key sizes **1024, 1152, 1280, 1536 and 2048 bits** that meet the following: **No standard**.

FCS_CKM.1.1/TDES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **TDES session key generation** and specified cryptographic key sizes **112 bits** that meet the following: **[ISO7816] Session keys or Diffie-Helman 1024**.

FCS_CKM.4 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**.

FCS_CKM.4.1/TDES	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**.

FCS_COP.1 Cryptographic operation

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 **RSA key computation** and cryptographic key sizes **1024, 1152, 1280, 1536 and 2048 bits** that meet the following: **[No standard]**.

FCS_COP.1.1/SIGNING	The TSF shall perform **electronic signature-generation** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024, 1152, 1280, 1536 and 2048 bits** that meet the following: **PKCS#1**.

FCS_COP.1.1/HASH	The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1, SHA-256** and cryptographic key sizes **none** that meet the following: **FIPS 180-2**.

FCS_COP.1.1/ENC	The TSF shall perform **Encryption and Decryption** in accordance with a specified cryptographic algorithm **TDES** and cryptographic key sizes **112 bits** that meet the following: **GP Secure Messaging**.

FCS_COP.1.1/MAC	The TSF shall perform **Message Authentication Code** in accordance with a specified cryptographic algorithm **TDES** and cryptographic key sizes **112 bits** that meet the following: **GP Secure Messaging**.

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.1.1/ Initialisation SFP	The TSF shall enforce the **Initialisation SFP** on **Generation of SCD/SVD pair by User**.

FDP_ACC.1.1/ SVD transfer SFP	The TSF shall enforce the **SVD transfer SFP** on **export of SVD by User**.

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

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/ Initialization SFP	The TSF shall enforce the **Initialisation** SFP to objects based on **General attribute group** and **Initialisation attribute group**.
FDP_ACF.1.2/ Initialization 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/ Initialization SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**.
FDP_ACF.1.4/ Initialization 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_SFP	The TSF shall enforce the **SVD Transfer_**SFP to objects based on **General attribute group**.
FDP_ACF.1.2/ SVD Transfer_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 "Signatory" is allowed to export SVD.**
FDP_ACF.1.3/ SVD Transfer_SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**.
FDP_ACF.1.4/ SVD Transfer_SFP	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_SFP	The TSF shall enforce the **SCD Import_**SFP to objects based on **General attribute group** and **Initialisation attribute group**.
FDP_ACF.1.2/ SCD Import_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 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_SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**.
FDP_ACF.1.4/ SCD Import_SFP	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".

Personalization SFP

FDP_ACF.1.1/ Personalization SFP	The TSF shall enforce the **Personalization SFP** to objects based on **General attribute group**.
FDP_ACF.1.2/ Personalization SFP	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/ Personalization SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**.
FDP_ACF.1.4/ Personalization SFP	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 SFP	The TSF shall enforce the **Signature-creation SFP** to objects based on **General attribute group** and **Signature-creation attribute group**.
FDP_ACF.1.2/ Signature-creation SFP	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 SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**.
FDP_ACF.1.4/ Signature-creation SFP	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 to outside TSF control

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.

FDP_ITC.1 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 user data when imported from outside the TOE.
FDP_ITC.1.2/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**.

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 user data when imported from outside the TOE.
FDP_ITC.1.2/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, and RAD.**

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1.

Dependencies: No dependency

Persistent data

The following data persistently stored by TOE have the user data attribute “integrity checked persistent stored data”

1. SCD
2. RAD
3. SVD (if persistently stored by TOE)

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.2.1/ 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 data**.
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/ Receiver	The TSF shall enforce the **SCD Import SFP** to **receive** user data in a manner protected from unauthorized disclosure.

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]

SVD transfer

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

FDP_UIT.1.1/ SVD transfer	The TSF shall enforce the **SVD transfer SFP** 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.

Receiver

FDP_UIT.1.1/ TOE DTBS	The TSF shall enforce the **Signature-creation SFP** 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 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

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

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

FIA_ATD.1User 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 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1	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	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application notes:

"Local user" mentioned in component FIA_UAU.1.1 is the user using the trusted path provided between the SGA in the TOE environment and the TOE as indicated by FTP_TRP.1/SCA and FTP_TRP.1/TOE.

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.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1	The TSF shall allow **1 Establishing a trusted channel between the TOE and a SSCD of type 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	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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 **Signatory.**

Attr. owner	Attributes	Allowed values	default value
[User]	Role	Administrator, Signatory, none	None
[User]	SCD/SVD management	Authorized / not Authorized	Not authorized
[SCD]	Secure SCD Import allowed	No/Yes	No
[SCD]	SCD operational	No/Yes	No
[DTBS]	Sent by an authorized SCA	No/Yes	No

Table 3: Attribute's allowed values

Condition	Modification	
	Set attribute	**At value**
Authenticated Administrator	Role [User]	Administrator
Authenticated Signatory AND Operational phase	Role [User]	Signatory

Reset	Role [User]	None
Authenticated Administrator and phase=perso	SCD/SVD management [Signatory]	Authorized
Authenticated Administrator and phase=perso	SCD/SVD management [Administrator]	Not authorized
End perso	Secure SCD Import allowed [SCD]	No
Authenticated SSCD T1 and Authenticated Administrator and phase=perso	Secure SCD Import allowed [SCD]	Yes
Authenticated SSCD T1 and Authenticated Signatory	Secure SCD Import allowed [SCD]	Yes
(SCD Import OR SCD/SVD Generation) and Authenticated Administrator	SCD operational [SCD]	No
(SCD Import OR SCD/SVD Generation) and Authenticated Signatory	SCD operational [SCD]	Yes
NOT (SCD operational [SCD]) and Authenticated Signatory	SCD operational [SCD]	Yes
Authenticated Signatory and Change PIN	SCD operational [SCD]	Yes
Signature creation	Sent by an authorized SCA [DTBS]	No
DTBS import	Sent by an authorized SCA [DTBS]	Yes

Table 4: Attribute's values modifications

Operation	Condition
RAD Creation	Role [User] = Administrator
Signature Creation	(Role [User] = Signatory) AND (Sent by an authorized SCA [DTBS] = Yes)
SCD Import	{(Role [User] = Administrator) OR (Role [User] = Signatory)} AND (SCD/SVD management [User] = Authorized) AND (Secure SCD Import allowed [SCD] = Yes)
SCD/SVD Generation	{(Role [User] = Administrator) OR (Role [User] = Signatory)} AND (SCD/SVD management [User] = Authorized)
SVD Export	(Role [User] = Administrator) OR (Role [User] = Signatory)

Table 5: Operations

FMT_MSA.1 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/ Administrator	The TSF shall enforce the **Initialisation SFP** and **SCD Import SFP** to restrict the ability to **modify** the security attributes **SCD / SVD management and secure SCD import allowed** to **Administrator**.

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.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 security attributes defined in Table 3: Attribute's allowed values.

FMT_MSA.3 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/ Type2	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/ Type2	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:

The security attribute of the SCD "SCD operational" is set to "no" after import of the SCD.

FMT_MSA.3.1/ Type3	The TSF shall enforce the **Initialisation SFP** and **Signature-creation SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/ Type3	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:

The security attribute of the SCD "SCD operational" is set to "no" after generation of the SCD.

FMT_MTD.1 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: **Identification and authentication management, access condition management**.

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 **Signatory**
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_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.1.1	The TOE shall not emit **electromagnetic and current emissions** in excess of **intelligible threshold** enabling access to **RAD and SCD**.
FPT_EMSEC.1.2	The TSF shall ensure any 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: **power shortage, over voltage, over and under clock frequency, integrity problems.**

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 **during initial start-up or when calling a sensitive module** 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

6.1.6 Class FTP Trusted Path / Channel

FTP_ITC.1 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 **SCD import**.

Application note:

The mentioned "another 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.

FTP_ITC.1.1/ SVD transfer	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 transfer	The TSF shall permit **another 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 "another 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.1.1/ DTBS 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/ 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 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1	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	The TSF shall permit **local users** to initiate communication via the trusted path.
FTP_TRP.1.3	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 4 (EAL4) 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 Classic applet, by the MultiAppID v2 platform embedded software, and by the chip.

The security functions provided by the IC are described in [ST-IC]. The security functions provided by the platform are described in [ST-JCS].

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

Identification	Name
SF_SIG_AUTHENTICATION	Authentication management
SF_SIG_CRYPTO	Cryptography management
SF_SIG_INTEGRITY	Integrity monitoring
SF_SIG_MANAGEMENT	Operation management and access control
SF_SIG_SECURE_MESSAGING	Secure messaging management

Table 6: *TOE security functions list*

7.1.1 SF_SIG_AUTHENTICATION: Authentication management

This security function manages the authentication mechanisms such as:

- Authentication operations for role management (i.e. PIN verification)
- Authentication operations for secure channel management (i.e. external authentication with symmetric and asymmetric schemes).

This security function:

- Manages authentication failure: when the **3 (for 5-digit RAD) or 5 (for 6-digit RAD)** unsuccessful authentication attempts has been met or surpassed, the TSF shall block D.RAD.
- Manage the asset D.RAD.
- Handles the authentications (for opening a secure channel) during the personalization and application phases.

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

- Identification of the user
- Establishing a trusted path between local user and the TOE
- Establishing a trusted channel between the SCA and the TOE for D.DTBS import
- Establishing a trusted channel between the TOE and the SSCD Type 1 for D.SCD import

This function is supported by the platform security function SF_CARD_AUTHENTICATION.

7.1.2 SF_SIG_CRYPTO: Cryptography management

This function manages the cryptographic operations of the electronic signature application:

- Key generation and correspondence verification (for RSA keypairs)
- Key destruction
- Perform cryptographic operations

This function is supported by platform security function SF.API that provides cryptographic algorithms SHA, TDES, RSA and RNG and ensures that D.SCD information is made unavailable after use (key destruction).

7.1.3 SF_SIG_INTEGRITY: Integrity monitoring

This SF monitors the integrity of sensitive user data and the integrity of the DTBS. The integrity of persistently stored data such as D.SCD, D.RAD and D.SVD is monitored using the platform security function SF_CARD_INTEGRITY.

In case of integrity error this SF will

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

This SF also monitors the integrity of the access conditions of created data objects.

7.1.4 SF_SIG_MANAGEMENT: operation management and access control

This SF provides application operation management and access control.

Operation management

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

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

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

- Modify **Initialization SFP** and **Signature-creation SFP** attributes
- Specify alternative default values

Access control

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

- Export of D.SVD by S.User
- Import of D.SCD by S.User
- Generation of D.SCD/D.SVD pair by S.User
- Creation of D.RAD by S.Admin
- Signing of D.DTBS-representation by S.Signatory

This SF provides access control to data objects.

This SF enforces the security policy on the import and the export of user data on:

- **SVD Transfer SFP:** D.SVD shall be sent to an authenticated CGA.
- **Signature-creation SFP**: D.DTBS shall be sent by an authenticated SCA.

7.1.5 SF_SIG_SECURE_MESSAGING: secure messaging management

This SF ensures the integrity and the confidentiality of exchanged user data.

This SF ensures that the TSF is able to

- Receive D.SCD with protection from unauthorized disclosure.
- Transmit D.SVD with protection from modification and insertion errors.
- Receive D.DTBS with protection from modification, deletion and insertion errors.
- Determine on received user data whether modification, deletion or insertion has occurred.

This SF manages four modes of secure channel during the personalization phase

- No secure messaging
- Integrity mode
- Confidentiality mode
- Integrity and confidentiality mode

In the application phase, secure channel is opened by a mutual authentication with two modes:

- Integrity mode
- Integrity and confidentiality mode

This function also manages the generation and deletion of session keys:

- Key generation
- Key destruction

This SF is supported by the platform and IC security functions.

7.1.6 TSFs provided by the MultiAppID v2 platform

The evaluation is a composite evaluation and uses the results of the CC evaluation of the MultiAppID v2 platform. The platform embedded software has been evaluated at level EAL 5+.

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.RMI	Remote Method Invocation
SF.ODEL	Object Deletion
SF.CAR	Secure Carrier

Table 7: Security Functions provided by the MultiAppID v2 platform.

7.1.7 TSFs provided by the Infineon chip

The evaluation is a composite evaluation and uses the results of the CC evaluation provided by [CR-IC -800] and [CR-IC-1440]. The IC and its primary embedded software have been evaluated at level EAL 5+.

These SF are the same for the all IC considered in this ST, ie: SLE66CLX360PEM, SLE66CLX360PE, SLE66CLX800PEM, SLE66CLX800PE, SLE66CX800PE, SLE66CLX1440PEM, SLE66CLX1440PE and SLE66CL1440PE.

SF	Description
SEF.1	Operating state checking
SEF.2	Phase management with test mode lock-out
SEF.3	Protection against snooping
SEF.4	Data encryption and data disguising
SEF.5	Random number generation
SEF.6	TSF self test
SEF.7	Notification of physical attack
SEF.8	Memory Management Unit (MMU)
SEF.9	Cryptographic support

Table 8: Security Functions provided by the IFX chip.

These SF are described in [ST-IC-800], and [ST-IC-1440].

7.2 ASSURANCE MEASURES

Assurance Measure	Document title
AM_ASE	MultiAppID v2 IAS Classic Security Target
AM_ADV_Spec	Functional Specifications - MultiAppID v2
AM_ADV_Design	Design – MultiAppID v2
AM_ADV_Int	Internals – MultiAppID v2
AM_ALC	Class ALC – MultiAppID v2
AM_AGD	Guidance – MultiAppID v2
AM_ATE	Class ATE – MultiAppID v2
AM_CODE	Source Code – MultiAppID v2
AM_Samples	Samples – MultiAppID v2

Table 9: Assurance Measures.

The development team uses a configuration management system that supports the generation of the TOE. The configuration management system is well documented and identifies all different configuration items. The configuration management tracks the implementation representation, design documentation, test documentation, guidance documentation. The security of the configuration management is described in detail in a separate document.

The delivery process of the TOE is well defined and follows strict procedures. Several measures prevent the modification of the TOE based on the developer's master copy and the user's version. The Administrator and the User are provided with necessary documentation for initialization and start-up of the TOE.

The implementation is based on an informal design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements.

The correspondence of the Security Functional Requirements (SFR) with less abstract representations will be demonstrated in a separate document. This addresses ADV_ARC, ADV_FSP, ADV_IMP, and ADV_TDS.

The tools used in the development environment are appropriate to protect the confidentiality and integrity of the TOE design and implementation. The development is controlled by a life cycle model of the TOE. The development tools are well defined and documented.

The Gemalto R&E organization is equipped with organizational and personnel means that are necessary to develop the TOE.

As the evaluation is identified as a composite evaluation based on the CC evaluation of the hardware, the assurance measures related to the hardware (IC) will be provided by documents of the IC manufacturer.