Security Target Lite

MultiApp V3.1

IAS Classic V4.2 EN

CONTENT

FIGURES

TABLES

1. ST INTRODUCTION

1.1 ST IDENTIFICATION

Title:	MultiApp V31 IAS EN Security Target
Version:	1.1p
ST reference:	D1296544
Origin:	Gemalto
ITSEF:	SERMA Technologies
Certification Body:	ANSSI
Evaluation scheme	FRENCH
Product identification:	IAS Classic V4.2 on MultiApp V31
Security Controllers:	NXP P60D144P VA
TOE identification:	IAS Classic V4.2 on MultiApp V31
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 MOC Server on MultiApp V3.1
- The MultiApp V3.1 product also includes 2 applications in ROM.

1.2 ST OVERVIEW

The Target of Evaluation (TOE) is composed of the MultiApp V3.1 platform and the electronic signature application IAS with MOC Server.
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 Classic V4.2 application is evaluated in conformance with [PP-SSCD-KG] and [PP-SSCD-KI].

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
[RGS-B1]	Référentiel général de sécurité version 1.0 Annexe B1 Mécanismes cryptographiques…version 1.20 du 26 Janvier 2010
[ST-IC]	[ST-IC-P60D144]
[CR-IC]	[CR-IC-P60D144]
[ST-IC-P60D144]	ST of NXP Secure Smart Card Controller P60D144PVA BSI-DSZ-CC-0845-V2-2013
[CR-IC-P60D144]	Certification Report, BSI-DSZ-CC-0845-V2-2013
[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
[PP-SSCD]	[EN-14169]
[PP-SSCD-KG]	[EN-14169-2]
[PP-SSCD-KI]	[EN-14169-3]
[EN-14169]	Protection profiles for secure signature creation device – EN version
[EN-14169-2]	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-14169-3]	Protection profiles for secure signature creation device – Part3: Device with key import BSI-CC-PP-0075-2012, Version 1.02, July 2012
[EN-14169-4]	Protection profiles for secure signature creation device – Part4: Extension for device with key generation and trusted communication with certificate generation application Not certified yet
[EN-14169-5]	Protection profiles for secure signature creation device – Part5: Extension for device with key generation and trusted communication with signature-creation application Not certified yet
[EN-14169-6]	Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application Not certified yet
[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*

1.3.2 Internal References

[ST-PLTF]	D1278582 JCS Security Target - MultiApp V31 Delphes31
[GUIDE]	IAS V4 user guidance MultiApp V31 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-1].
User data	Data created by and for the user, that does not affect the operation of the TSF [CC-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.

[PP-SSCD] defines protection profiles for SSCD:

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

[PP-SSCD] also defines possible extensions for the above protection profiles:

- [EN-14169-4] defines extensions for [PP-SSCD-KG] with trusted communication between SSCD and CGA.
- [EN-14169-5] defines extensions for PP-SSCD-KG] with trusted communication between SSCD and SCA.
- [EN-14169-6] defines extensions for [PP-SSCD-KI] with trusted communication between SSCD and SCA.

In this document the terminology of [EN-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 V3.1 platform (JavaCard platform)
- The IAS Classic V4.2 application.

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

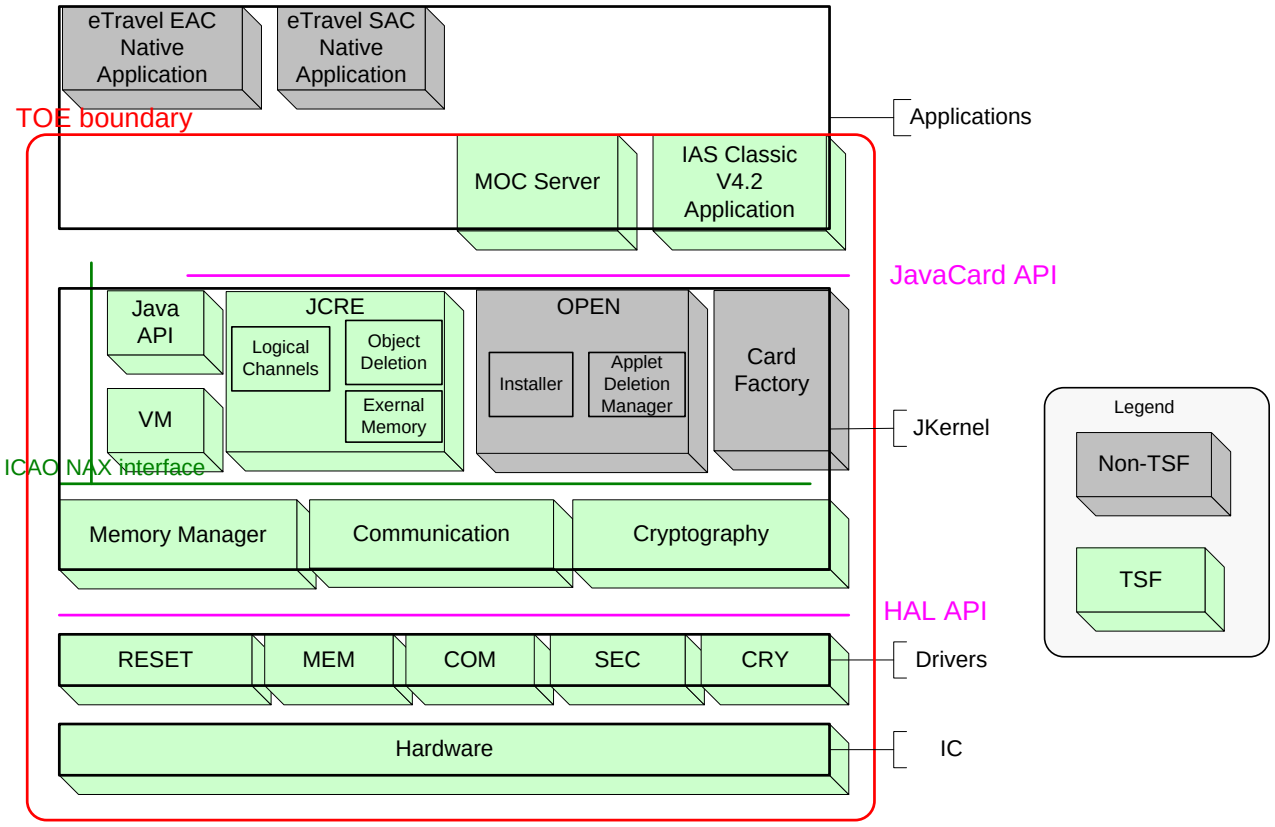


Figure 1: TOE Boundaries

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:

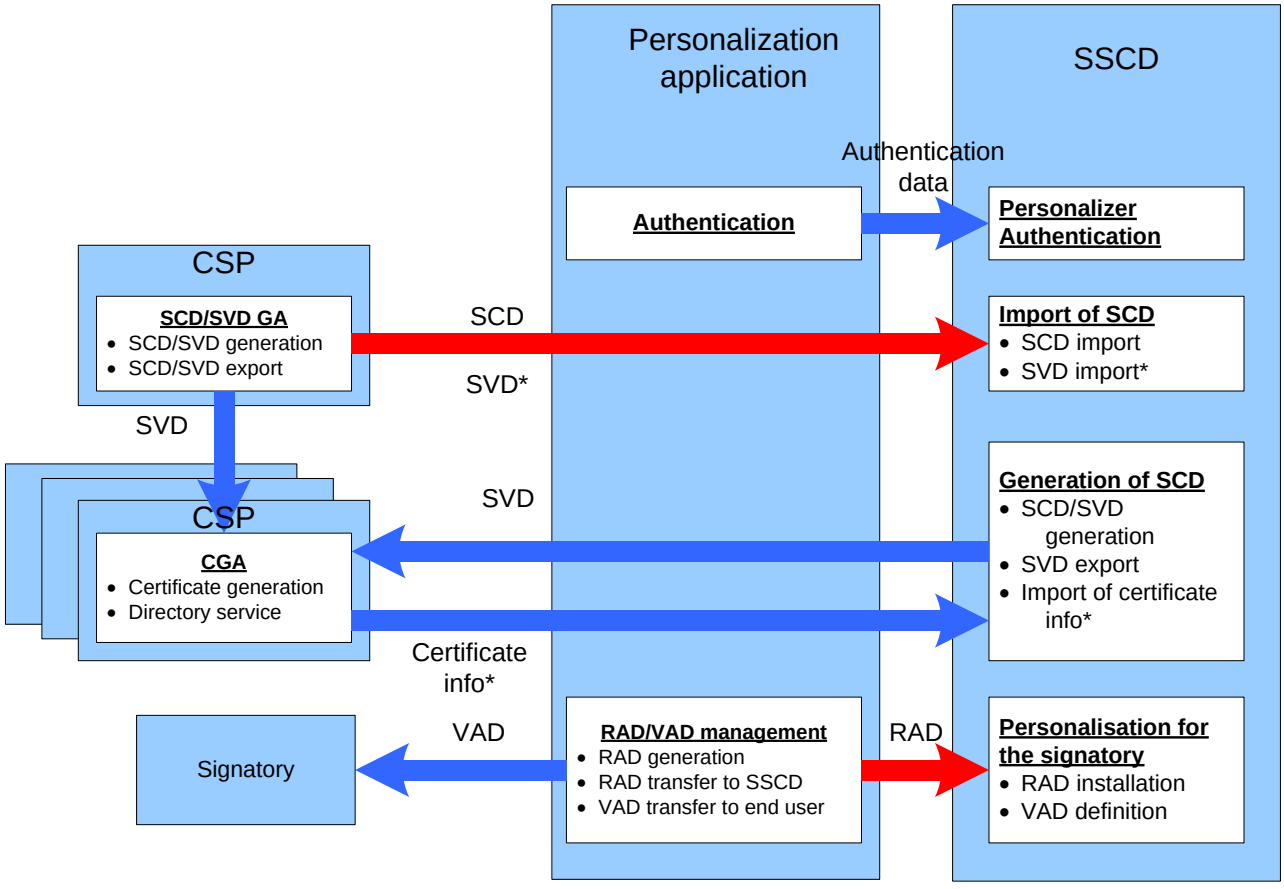


Figure 2: TOE Personalization

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”

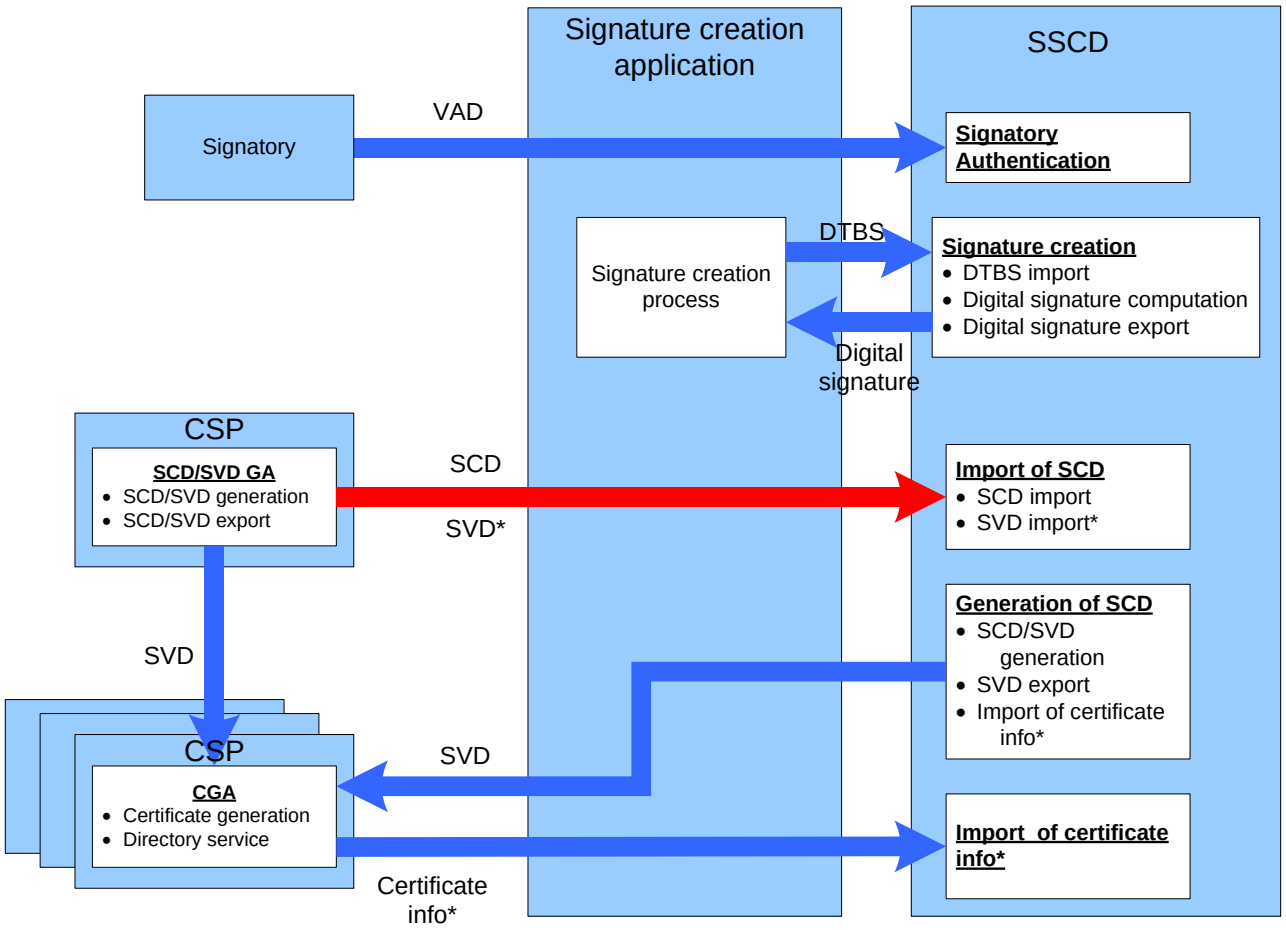


Figure 3: TOE Operational Use

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 SCP.
- 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	NPX
Embedded Software Developer	Gemalto
Integrated Circuit (IC) Manufacturer	NPX
Initializer	Gemalto
Pre-personalizer	Gemalto
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 1: Identification of the actors

1.8.3 Pre-personalization on module at Gemalto site

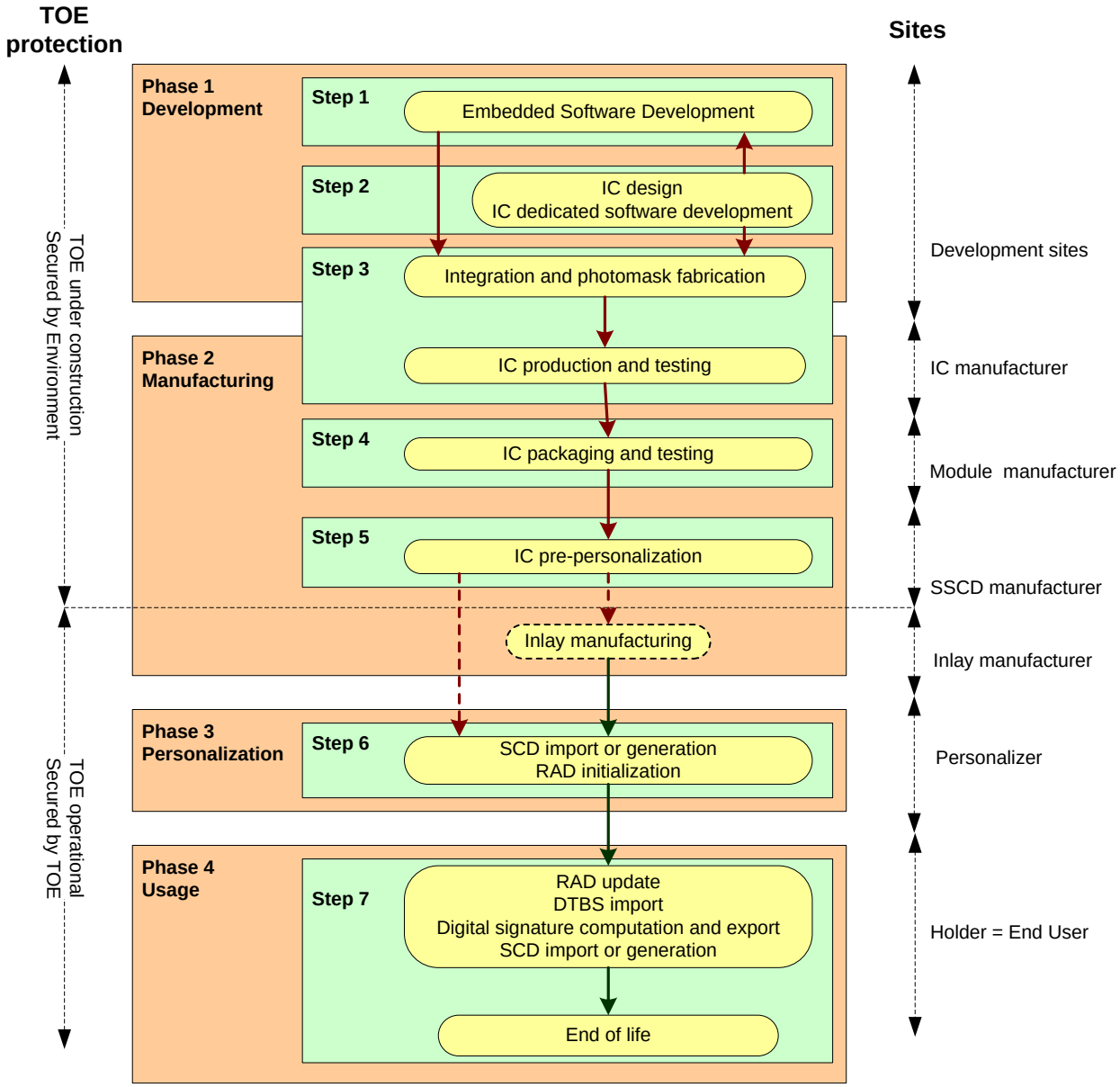


Figure 4: LC1: Pre-personalization on module at Gemalto site

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.

1.8.4 Pre-personalization on inlay at Gemalto site

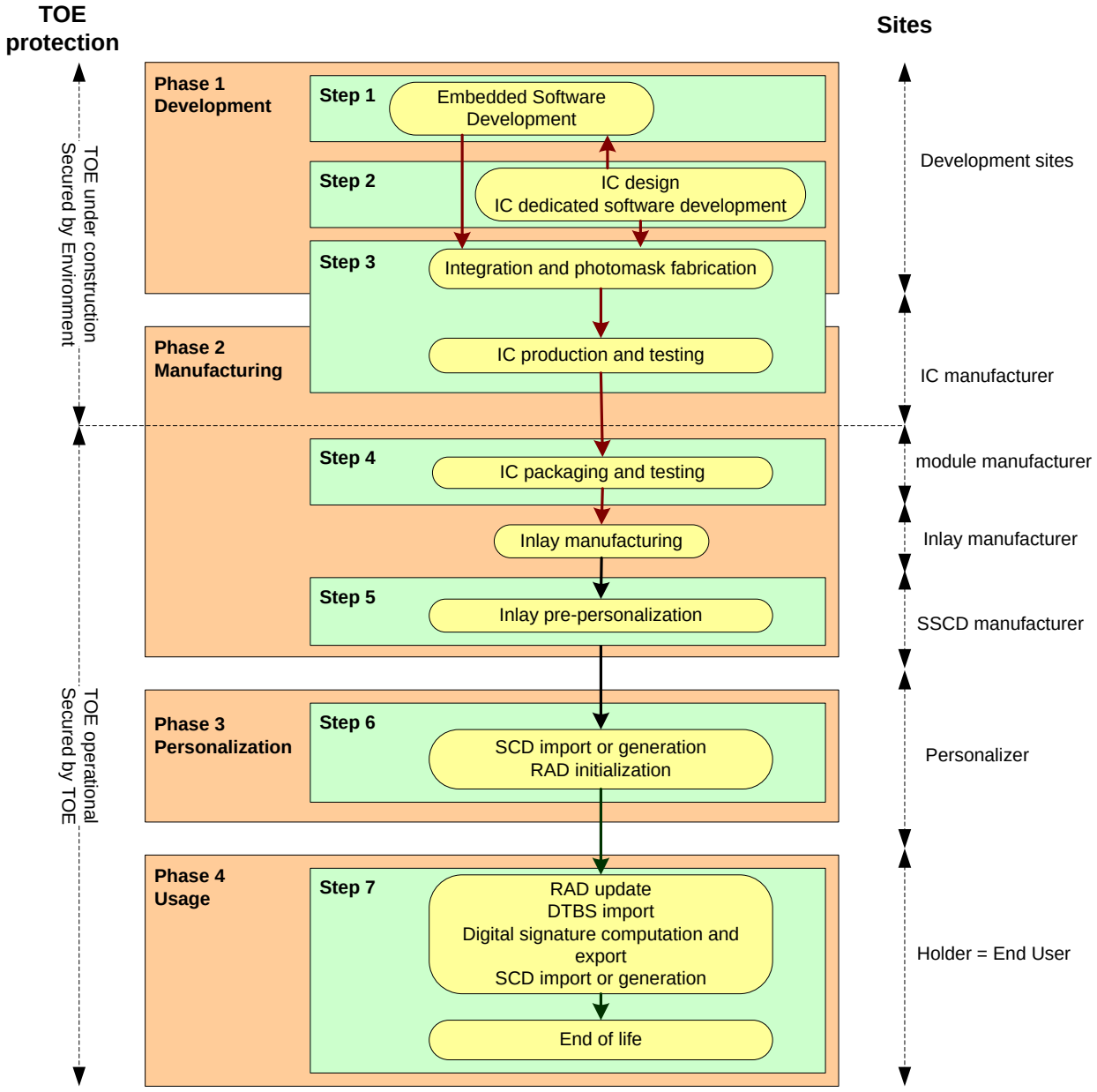


Figure 5: LC3: Pre-personalization on inlay at Gemalto site

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 V3.1 claiming conformance to [PP-JCS-Open].

2.2 PP CLAIM,

This MultiApp v3.1 IAS security target claims strict conformance to the following Protection Profiles:

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

The evaluation is a composite evaluation and uses the results of the CC evaluation of the MultiApp V3.1 platform. The platform embedded software has been evaluated at level EAL 5+.
The security problem definition, the objectives, and the SFR of the platform are not described in this document but in [ST-PLTF].

The MultiApp V3.1 JCS security target [ST-PLTF], claims demonstrable conformance to the Protection Profile “JavaCard System – Open configuration”, ANSSI-PP-2010- 03, Version 2.6 ([PP-JCS-Open]).

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 GENERAL

The assets, threats, OSP, and assumptions of the TOE are those defined in [PP-SSCD-KG], [PP-SSCD-KI]. The present Security Target deals with the assets, threats, OSP, and assumptions of [PP-SSCD-KG] and [PP-SSCD-KI.

The assets of [PP-JCS-Open] are studied in [ST-PLTF].

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

Assets and objects:

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

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

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

User and subjects acting for users:

1. User: End user of the TOE who can be identified as Administrator or Signatory. In the TOE the subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

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

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

Threat agents:

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

3.2 THREATS

T.SCD_Divulg *Storing ,copying, and releasing of the signature-creation data*
An attacker stores or copies the SCD outside the TOE. An attacker can 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 publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

T.Hack_Phys *Physical attacks through the TOE interfaces*
An attacker interacts with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD,SVD and DTBS.

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

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

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

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

3.3 ORGANIZATIONAL SECURITY POLICIES

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

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

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

P.Sigy_SSCD *TOE as secure signature-creation device*
The TOE meets the requirements for an SSCD laid down in Annex III of the Directive [0]. This implies the SCD is used for signature creation under sole control of the signatory and the SCD can practically occur only once.

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

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

3.4 ASSUMPTIONS

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

A.CGA *Trustworthy certification-generation application*
The CGA protects the authenticity of the signatory's name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

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

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

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

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.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,P_Sig_Non-Repud 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.CSP 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.CSP. 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

4.1 GENERALS

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

4.2 SECURITY OBJECTIVES FOR THE TOE

4.2.1 Common Objectives between [PP-SSCD-KG] and [PP-SSCD-KI]

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

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

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

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

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

OT.EMSEC_Design *Provide physical emanations security*
The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

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

OT.Tamper_Resistance *Tamper resistance*
The TOE shall prevent or resist physical tampering with specified system devices and components.

4.2.2 Specific Objectives from [PP-SSCD-KG]

OT.SCD/SVD_Auth_Gen *Authorized SCD/SVD generation*
The TOE shall provide security features to ensure that authorised users only invoke the generation of the SCD and the SVD
OT.SCD_Unique *Uniqueness of the signature-creation data*
The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation can practically occur only once and shall not be reconstructable from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible.

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

4.2.3 Specific Objectives from [PP-SSCD-KI]

OT.SCD_Auth_Imp *Authorised SCD import*
The TOE shall provide security features to ensure that authorised users only invoke the import of the SCD.

4.2.4 Extensions

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

4.3 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).

4.3.1 Common Objectives between [PP-SSCD-KG] and [PP-SSCD-KI]

OE.SVD_AUTH *Authenticity of the SVD*
The operational environment shall ensure the integrity of the SVD send to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

OE.CGA_Qcert *Generation of qualified certificates*
The CGA shall generate a qualified certificate that includes(amongst others)

- (a) the name of the signatory controlling the TOE,
- (b) the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
- (c) the advanced signature of the CSP.

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

OE.SSCD_Prov_Service *Authentic SSCD provided by SSCD Provisioning Service*
The SSCD-provisioning service shall initialise and personalise for the signatory an authentic copy of the TOE and deliver this copy as SSCD to the signatory.

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

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

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

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

4.3.2 Objectives from [PP-SSCD-KI]

OE.SCD/SVD_Auth_Gen *Authorized SCD/SVD generation*
The CSP shall provide security features to ensure that authorised users only invoke the generation of the SCD and the SVD.

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

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

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

4.4 SECURITY OBJECTIVE RATIONALE

	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Auth_Imp	OT_Pre_personalisation	OE.SVD_Auth	OE.CGA_QCert	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE_DTBS_Protect	OE.Signatory	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp
T.SCD_Divulg		X										X									X	X		
T.SCD_Derive			X						X														X	
T.Hack_Phys		X				X	X	X																
T.SVD_Forgery											X			X										X
T.SigF_Misuse	X			X	X												X	X	X	X				
T.DTBS_Forgery					X													X	X					
T.Sig_Forgery			X							X					X								X	
P.CSP_QCert	X										X	X			X						X			X
P.QSign			X	X											X			X						
P.Sigy_SSCD	X	X	X	X	X	X		X	X	X		X				X					X	X	X	
P.Sig_Non-Repud	X	X	X	X	X	X	X	X		X	X			X	X	X		X	X	X		X	X	X
P_Pre-personalisation													X											
A.CGA														X	X									
A.SCA																		X						
A.SCP																					X	X	X	X

Table 2: Threats, Assumptions, Policies vs Security objectives

4.4.1 Threats

T.Hack_Phys (Exploitation of physical vulnerabilities) deals with physical attacks exploiting physical vulnerabilities of the TOE. *OT.SCD_Secrecy* preserves the secrecy of the SCD.

OT.EMSEC_Design counters physical attacks through the TOE interfaces or observation of TOE emanations. *OT.Tamper_ID* and *OT.Tamper_Resistance* counter the threat *T.Hack_Phys* by detecting and by resisting tamper attacks.

T.SCD_Divulg (Storing and copying and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [1], recital (18). This threat is countered by

OE.SCD_Secrecy, which assures the secrecy of the SCD in the CSP environment, and

OT.SCD_secrecy, which assures the secrecy of the SCD during use by the TOE for signature generation.

Furthermore, generation and/or import of SCD known by an attacker is countered by OE.SCD/SVD_Auth_Gen, which ensures that only authorized SCD generation in the environment is possible, and OT.SCD_Auth_Imp, which ensures that only authorised SCD import is possible.

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

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

T.SVD_Forgery (Forgery of the signature verification data) deals with the forgery of the SVD exported by the TOE to the CGA or given to the CGA for certificate generation. T.SVD_Forgery is addressed by OT.SCD_SVD_Corresp or OE.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE or given to the CGA.

T.DTBS_Forgery (Forgery of the DTBS/R) addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of OE.DTBS_Protect, which ensures

that the DTBS/R cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R inside the TOE.

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

4.4.2 Assumptions

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

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

A.CSP (Secure SCD/SVD management by CSP) establishes several security aspects concerning handling of SCD and SVD by the CSP. That the SCD/SVD generation device can only be used by authorized users is addressed by OE.SCD/SVD_Auth_Gen (Authorized SCD/SVD Generation), that the generated SCD is unique and cannot be derived by the SVD is addressed by OE.SCD_Unique (Uniqueness of the signature creation data), that SCD and SVD correspond to each other is addressed by OE.SCD_SVD_Corresp (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are deleted in the environment once exported to the TOE is addressed by OE.SCD_Secrecy (SCD Secrecy).

4.4.3 Organisational security policies

P.CSP_QCert (CSP generates qualified certificates) establishes the CSP generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by OT.Lifecycle_Security, which requires the TOE to detect

flaws during the initialisation,personalisation and operational usage, OE.SCD/SVD_Auth_Gen, which ensures that the SCD/SVD generation can be invoked by authorized users only, OT.SCD_Auth_Imp which ensures that authorised users only may invoke the import of the SCD, OT.SCD_SVD_Corresp , OE.SCD_SVD_Corresp, which require the CSP to ensure the correspondence between the SVD and the SCD during their generation, and OE.CGA_QCert for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

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

P.Sigy_SSCD (TOE as secure signature creation device) requires the TOE to meet the Annex II of **the directive** [1]. This is ensured as follows:

- OT.SCD_Unique and OE.SCD_Unique meet the paragraph 1(a) of **the directive** [1], Annex III, by the requirements that the SCD used for signature creation can practically occur only once.

OE.SCD_Unique, OT.SCD_Secrecy and OE.SCD_Secrecy meet the paragraph 1(a) of **the directive** [1], Annex III, by the requirements to ensure the secrecy of the SCD.OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of SCD against specific attacks.

OT.SCD_Secrecy and OT.Sig_Secure meet the paragraph 1(b) of **the directive** [1], Annex III, by the requirements to ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE.

OT.Sigy_SigF and OE.SCD_Secrecy meet the paragraph 1(c) of **the directive** [1], Annex III, by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others.

OT.DTBS_Integrity_TOE meets the requirements the paragraph 2 of **the directive** [1], Annex III, The TOE must not alter the DTBS/R.

Please take note, the requirements of **the directive** [1], Annex III, 2., that the SSCD does not prevent the data to be signed from being presented to the signatory prior to the signature process is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the signatory and send them to the SSCD for signing. The usage of SCD under sole control of the signatory sole control is ensured by :

- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialisation, personalization and operational usage
- - OE.SCD/SVD_Auth_Gen and OE.SCD/SVD_Auth_Gen, which limit invocation of the generation of the SCD and the SVD to authorised users only,
- OT.SCD_Auth_Imp, which limits SCD import to authorised users only,
- OE.SCD_Secrecy, which ensures the confidentiality of the SCD during generation and export to the TOE, and deletes the SCD after export to the TOE. The CSP does not use the SCD for signature creation
- OT.Sigy_SigF, which requires the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.

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

P.Sig_Non-Repud (Non-repudiation of signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their

certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures created with the TOE.
OE.SSCD_Prov_Service ensures that the signatory uses an authentic copy of the TOE, initialised and personalised for the signatory.
OE.SCD_SVD_Corresp, OE.SCD_Secrecy and OE.SCD_Unique ensure the security of the SCD in the CSP environment. OE.SCD_Secrecy ensures the confidentiality of the SCD during generation, during and after export to the TOE. The CSP does not use the SCD for creation of any signature and deletes the SCD irreversibly after export to the TOE. OE.SCD_Unique provides that the signatory's SCD can practically occur just once. OE.SCD_SVD_Corresp ensures that the SVD in the certificate of the signatory corresponds to the SCD that is implemented in the copy of the TOE of the signatory.
OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD of the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure the authenticity of the SVD as being exported by the TOE under sole control of the signatory. OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD of the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure the authenticity of the SVD as being exported by the TOE under sole control of the signatory.OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. OT.SCD_Unique provides that the signatory's SCD can practically occur just once.
OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD-provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. OE.DTBS_Intend, OE.DTBS_Protect and OT.DTBS_Integrity_TOE ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

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

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

4.4.4.1 Compatibility between objectives for the TOE

OT.Lifecycle_Security, OT.SCD_Secrecy, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID, and OT.Tamper_Resistance deal with physical protection of the TOE. These are supported by O.Phys-Manipulation, O.Phys-Probing, O.Malfunction, O.Leak-Inherent, and O.Leak-Forced.

OT.SCD_SVD_Corresp, OT.SCD/SVD_Auth_Gen,, OT.SCD_Auth_Imp OT.Sig_Secure, OT.Sigy_SigF, OT.SCD_Unique, and OT.Pre-personalisation are objectives specific to [ST-IAS] and they do no conflict with the objectives of [ST-PLTF].

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

4.4.4.2 Compatibility between objectives for the environment

OE.CGA_QCert, OE.SVD_Auth, OE.HID_VAD, OE.SSCD_Prov_Service, OE_DTBS_Intend, OE_DTBS_Protect, OE.SCD_SVD_Corresp, OE.SCD/SVD_Auth_Gen, OE.Signatory, OE.SCD_Secrecy

and OE.SCD_Unique are objectives specific to [ST-IAS] and they do no conflict with the objectives of [ST-PLTF].

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

4.4.5 Justifications for adding objectives on the environment

4.4.5.1 Additions to [PP-SSCD-KG]

The only additional objectives on the environment are: OE.SCD_SVD_Corresp, OE.SCD_Secrecy, OE_SCD_Unique and OE.SCD/SVD_Auth_G. These objectives request the environment to perform several operations when the SCD is generated off-TOE and imported afterwards. These two operations are outside the scope of [PP-SSCD-KG]. Therefore the added objectives on the environment do not weaken the TOE.

5. EXTENDED COMPONENTS DEFINITION

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

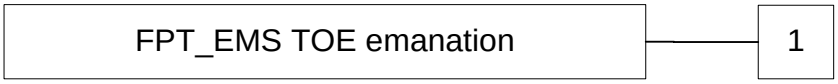
5.1 DEFINITION OF THE FAMILY FPT_EMS

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

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

Family behaviour
This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMS.1 TOE emanation has two constituents:

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

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

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

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

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components
Dependencies: No dependencies.

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

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

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].

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

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

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:
FCS_CKM.1/SCD is named FCS_CKM.1 in [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.**

iteration	algorithm	Key size	standards
/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

FCS_CKM.4/Session Cryptographic key destruction

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **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/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	1024,1536,2048,30	[ISO9796-2]

iteration	operation	algorithm	key size	standards
	verification		72 and 4096	RSA SHA PKCS#1 v1.5 RSA PSS SHA PKCS#1
/DSC-ECC	signature & verification	ECC	224, 256, 384, 512, 521	[TR-03111] ECDSA SHA

Table 7: FCS_COP.1/DSC refinement

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 /Other 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 8: FCS_COP.1/Other refinement

6.1.2 Class FDP User Data Protection

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

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

Table 9: Subjects and security attributes for access control

FDP_ACC.1/Signature_Creation Subset access control

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

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

FDP_ACF.1/Signature_Creation Security attribute based access control

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

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

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

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

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

FDP_ACC.1/SCD/SVD_Generation Subset access control

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

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

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

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

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

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

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

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

FDP_ACC.1/SVD_Transfer Subset access control

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

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

FDP_ACF.1/SVD_Transfer Security attribute based access control

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

FDP_ACF.1.1 /SVD_Transfer: The TSF shall enforce the SVD Transfer SFP to objects based on the following:
1. the S.User is associated with the security attribute Role
2. the SVD .

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled

/SVD_Transfer	subjects and controlled objects is allowed: [**R.Admin or R.Sigy** is allowed to export SVD,
FDP_ACF.1.3 /SVD_Transfer	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4 /SVD_Transfer	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none

FDP_ACC.1/SCD_Import Subset access control

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

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

FDP_ACF.1/SCD_Import Security attribute based access control

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

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

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	The TSF shall ignore any security attributes associated with the SCD when imported from

/SCD outside the TOE.

FDP_ITC.1.3 /SCD The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components
Dependencies: No dependency

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

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

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

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

FDP_SDI.2/Persistent Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring
Dependencies: No dependency

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

FDP_SDI.2.2 /Persistent Upon detection of a data integrity error, the TSF shall :
1. prohibit the use of the altered data
2. inform the S.Sigy about integrity error.

FDP_SDI.2/DTBS Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring
Dependencies: No dependency

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

FDP_SDI.2.2 /DTBS: Upon detection of a data integrity error, the TSF shall :
1. prohibit the use of the altered data
2. inform the S.Sigy about integrity error.

FDP_UCT.1 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 receive SCD in a manner protected from unauthorized disclosure.

6.1.3 Class FIA Identification and Authentication

FIA_AFL.1/SIG Authentication failure handling

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

FIA_AFL.1.1: 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.

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

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

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

FIA_AFL.1.1 /PERSO: The TSF shall detect when [**Number in Table 10**] unsuccessful authentication attempts occurs related to **authentication**.

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_UAU.1/SIG Timing of authentication

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

FIA_UAU.1.1 The TSF shall allow
1. Self test according to FPT_TST.1.
2. Identification of the user by means of TSF required by FIA_UID.1.
3. **No other Signature generation related action**.

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 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.

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
4. Identification of the user by means of TSF required by FIA_UID.1.
5. **No other action**.

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

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

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. Self test according to FPT_TST.1.
2. **No other Signature generation related action**.

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

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

FIA_UID.1/PERSO Timing of identification

Hierarchical to: No other components
Dependencies: No dependencies

FIA_UID.1.1 /PERSO The TSF shall allow
3. **No action**.

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-

/PERSO 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 R.Sigy**.**

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

FMT_MSA.1/AdminKG Management of security attributes

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

FMT_MSA.1 /AdminKG The TSF shall enforce the SCD/SVD Generation SFP to restrict the ability to modify the security attributes SCD / SVD management to R.Admin**.**

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

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

FMT_MSA.3/KeyImport Static attribute initialization

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

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

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

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

FMT_MTD.1/Admin Management of TSF data

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

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

FMT_MTD.1/Signatory Management of TSF data

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

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

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components
Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:
1. Creation and modification of RAD.
2. Enabling the signature-creation function.
3. Modification of the security attribute SCD/SVD management, SCD operational.
4. Change the default value of the security attribute SCD Identifier.
5. **No other security management function**.

FMT_SMR.1 Security roles

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

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

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

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

FTP_ITC.1.2 /SCD import The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3 /SCD import The TSF shall initiate communication via the trusted channel for
1. Data exchange integrity according to FDP_UCT.1/SCD.
2. **[None]**.

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.

6.3 SECURITY REQUIREMENTS RATIONALE

6.3.1 SFR and PP

Requirements	PP-SSCD-KG]	[PP-SSCD-KI]	additions
FCS_CKM.1/SCD	X		
FCS_CKM.1/Session			X
FCS_CKM.4/SCD	X	X	
FCS_CKM.4/Session			X
FCS_COP.1/DSC	X	X	
FCS_COP.1/Session			X
FDP_ACC.1/Signature-creation SFP	X	X	
FDP_ACF.1/Signature-creation SFP	X	X	
FDP_ACC.1/SCD/SVD_Generation SFP	X		
FDP_ACF.1/SCD/SVD_Generation SFP	X		
FDP_ACC.1/SVD transfer SFP	X		
FDP_ACF.1/SVD transfer SFP	X		
FDP_ACC.1/SCD import SFP		X	
FDP_ACF.1/SCD import SFP		X	
FDP_ITC.1/SCD		X	
FDP_RIP.1	X	X	
FDP_SDI.2/Persistent	X	X	
FDP_SDI.2/DTBS	X	X	
FDP_UCT.1/SCD		X	
FIA_AFL.1/PERSO			X
FIA_AFL.1/SIG	X	X	
FIA_UAU.1/PERSO			X
FIA_UAU.1/SIG	X	X	
FIA_UID.1/PERSO			X
FIA_UID.1/SIG	X	X	
FMT_MOF.1	X	X	
FMT_MSA.1/Signatory	X	X	
FMT_MSA.1/AdminKG	X		
FMT_MSA.1/AdminKI		X	
FMT_MSA.2	X	X	
FMT_MSA.3/Keygen	X		
FMT_MSA.3/KeyImport		X	
FMT_MSA.4/Keygen	X		
FMT_MSA.4/KeyImport		X	
FMT_MTD.1/Admin	X	X	
FMT_MTD.1/Signatory	X	X	
FMT_SMF.1	X	X	

Requirements	PP-SSCD-KG]	[PP-SSCD-KI]	additions
FMT_SMR.1	X	X	
FPT_EMS.1	X	X	
FPT_FLS.1	X	X	
FPT_PHP.1	X	X	
FPT_PHP.3	X	X	
FPT_TST.1	X	X	
FTP_ITC.1/SCD Import		X	

Table 12: Objective vs SFR rationale

6.3.2 Security Functional Requirements Rationale

6.3.2.1 Security objectives for the TOE

Requirements	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Auth_Gen (Part 2 only)	OT.SCD_Unique (Part 2 only)	OT.SCD_SVD_Corresp (Part 2 only)	OT.SCD_Auth_Imp (Part 3 only)	OT.Pre-personalisation
FCS_CKM.1/SCD	X	X								X	X		
FCS_CKM.1/Session	X												X
FCS_CKM.4/SCD	X	X											
FCS_CKM.4/Session	X												X
FCS_COP.1/DSC	X		X										
FCS_COP.1/Session	X												X
FDP_ACC.1/Signature-creation SFP	X			X									
FDP_ACF.1/Signature-creation SFP	X			X									
FDP_ACC.1/SCD/SVD_Generation SFP	X								X				
FDP_ACF.1/SCD/SVD_Generation SFP	X								X				
FDP_ACC.1/SVD transfer SFP	X												
FDP_ACF.1/SVD transfer SFP	X												
FDP_ACC.1/SCD import SFP	X											X	
FDP_ACF.1/SCD import SFP	X											X	
FDP_ITC.1/SCD	X												

Requirements	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Auth_Gen (Part 2 only)	OT.SCD_Unique (Part 2 only)	OT.SCD_SVD_Corresp (Part 2 only)	OT.SCD_Auth_Imp (Part 3 only)	OT.Pre-personalisation
FDP_RIP.1		X		X									
FDP_SDI.2/Persistent		X	X								X		
FDP_SDI.2/DTBS				X	X								
FDP_UCT.1/SCD	X	X											
FIA_AFL.1/PERSO													X
FIA_AFL.1/SIG				X									
FIA_UAU.1/PERSO													X
FIA_UAU.1/SIG				X					X			X	
FIA_UID.1/PERSO													X
FIA_UID.1/SIG				X					X			X	
FMT_MOF.1	X			X									
FMT_MSA.1/Signatory	X			X									
FMT_MSA.1/AdminKG	X								X				
FMT_MSA.1/AdminKI	X												
FMT_MSA.2	X			X					X				
FMT_MSA.3/Keygen	X			X					X				
FMT_MSA.3/KeyImport	X			X									
FMT_MSA.4/Keygen	X			X					X		X		
FMT_MSA.4/KeyImport	X			X									
FMT_MTD.1/Admin	X			X									
FMT_MTD.1/Signatory	X			X									
FMT_SMF.1	X			X							X		
FMT_SMR.1	X			X									
FPT_EMS.1		X				X							
FPT_FLS.1		X											
FPT_PHP.1							X						
FPT_PHP.3		X						X					
FPT_TST.1	X	X	X										
FTP_ITC.1/SCD Import	X	X											

Table 13: Objective vs SFR rationale

OT.Lifecycle_Security (*Lifecycle security*) is provided by the SFR for SCD/SVD generation **FCS_CKM.1/SCD**, SCD usage **FCS_COP.1/SCD** and SCD destruction **FCS_CKM.4/SCD** which ensure cryptographically secure lifecycle of the SCD.
The SCD/SVD generation is controlled by TSF according to **FDP_ACC.1/SCD/SVD_Generation** and **FDP_ACF.1/SCD/SVD_Generation**.
The SVD transfer for certificate generation is controlled by TSF according **to FDP_ACC.1/SVD_Transfer** and **FDP_ACF.1/SVD_Transfer**.
The SCD import is controlled by TSF according **to FDP_ACC.1/SCD_Import**, **FDP_ACF.1/SCD_Import** and **FDP_ITC.1/SCD**. The confidentiality of the SCD is protected during import according **to FDP_UCT.1/SCD** in the trusted channel **FTP_ICT.1/SCD Import**.
The SCD usage is ensured by access control **FDP_ACC.1/Signature_Creation , FDP_ACF.1/Signature_Creation** which is based on the security attribute secure TSF management according to **FMT_MOF.1, FMT_MSA.1/AdminKG FMT_MSA.1/AdminKI, FMT_MSA.1/Signatory**, **FMT_MSA.2, FMT_MSA.3/KeyGen, FMT_MSA.3/KeyImport, FMT_MSA.4/Keygen, FMT_MSA.4/KeyImport**, **FMT_MTD.1/Admin**, **FMT_MTD.1/Signatory**, **FMT_SMF.1** and **FMT_SMR.1.** The test functions **FPT_TST.1** provides failure detection throughout the lifecycle.

OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by *FPT_EMS.1*.

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

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

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

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

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

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

OT.Sigy_SigF (*Signature creation function for the legitimate signatory only*) is provided by an SFR for identification authentication and access control.

FIA_UAU.1 and **FIA_UID.1** ensure that no signature generation function can be invoked before the signatory is identified and authenticated. The security functions specified by **FMT_MTD.1/Admin** and **FMT_MTD.1/Signatory** manage the authentication function. SFR **FIA_AFL.1** provides protection against a

number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by **FDP_SDI.2/DTBS** ensures the integrity of stored DTBS and **FDP_RIP.1** prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process).

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

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

SSCD Part 3 only

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

SSCD Part 2 only

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

OT.SCD/SVD_Auth_Gen (*SCD/SVD generation*) addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by **FIA_UID.1** and **FIA_UAU.1** provide user identification and user authentication prior to enabling access to authorized functions. The SFR **FDP_ACC.1/SCD/SVD_Generation_SFP** and **FDP_ACF.1/SCD/SVD_Generation_SFP** provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by **FMT_MSA.1/AdminKG**, **FMT_MSA.2**, and **FMT_MSA.3/Keygen** for static attribute initialization. The SFR **FMT_MSA.4/Keygen** defines rules for inheritance of the security attribute “SCD operational” of the SCD.

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

Extensions

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

6.3.2.2 Dependency Rationale

Requirements	CC Dependencies	Satisfied Dependencies
FCS_CKM.1/SCD	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/DSC, FCS_CKM.4/SDC
FCS_CKM.1/Session	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/Session, FCS_CKM.4/Session
FCS_CKM.4/SCD	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/SDC, FDP_ITC.1/SCD,
FCS_CKM.4/Session	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/Session
FCS_COP.1/DSC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/SCD, FCS_CKM.4/SCD, FDP_ITC.1/DTBS
FCS_COP.1/Session	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/Session, FCS_CKM.4/Session
FDP_ACC.1//SCD/SVD_Generation SFP	(FDP_ACF.1)	FDP_ACF.1//SCD/SVD_Generation SFP
FDP_ACC.1/SVD transfer SFP	(FDP_ACF.1)	FDP_ACF.1/SVD transfer SFP
FDP_ACC.1/SCD import SFP	(FDP_ACF.1)	FDP_ACF.1/SCD import SFP
FDP_ACC.1/Signature-creation SFP	(FDP_ACF.1)	FDP_ACF.1/Signature-creation SFP
FDP_ACF.1/Signature-creation	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/Signature-creation, FMT_MSA.3/KeyGen, FMT_MSA.3/KeyImport
FDP_ACF.1/SCD/SVD_Generation SFP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SCD/SVD_Generation SFP, FMT_MSA.3/Keygen, FMT_MSA.3/KeyImport
FDP_ACF.1/SVD transfer SFP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SVD transfer SFP, FMT_MSA.3/Keygen
FDP_ACF.1/SCD import SFP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SCD import SFP, FMT_MSA.3/KeyImport
FDP_ACF.1/Signature-creation SFP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/Signature-creation SFP, FMT_MSA.3/KeyImport, FMT_MSA.3/Keygen
FDP_ITC.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1/SCD import SFP, FMT_MSA.3/KeyImport
FDP_ITC.1/DTBS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1/Signature-creation SFP, FMT_MSA.3/Type2, FMT_MSA.3/Type3
FDP_RIP.1	No dependencies	
FDP_SDI.2/Persistent	No dependencies	
FDP_SDI.2/DTBS	No dependencies	
FDP_UCT.1/SCD	(FTP_ITC.1 or FTP_TRP.1) (FDP_ACC.1 or FDP_IFC.1)	FTP_ITC.1/SCD, FDP_ACC.1/SCD import SFP,
FIA_AFL.1/PERSO	(FIA_UAU.1)	FIA_UAU.1/PERSO

Requirements	CC Dependencies	Satisfied Dependencies
FIA_AFL.1/SIG	(FIA_UAU.1)	FIA_UAU.1/SIG
FIA_UAU.1/PERSO	(FIA_UID.1)	FIA_UID.1/PERSO
FIA_UAU.1/SIG	(FIA_UID.1)	FIA_UID.1/SIG
FIA_UID.1/PERSO	No dependencies	
FIA_UID.1/SIG	No dependencies	
FMT_MOF.1	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/AdminKG	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/SCD/SVD_Generation SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/AdminKI	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/SCD Import SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/Signature-creation SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.1/SCD/SVD_Generation SFP, FDP_ACC.1/Signature-Creation SFP, FMT_MSA.1/AdminKG FMT_MSA.1/AdminKI FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.3/KeyImport	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/AdminKI, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.3/Keygen	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/AdminKG, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4/ KeyImport	(FDP_ACC.1) or (FDP_IFC.1)	FDP_ACC.1/SCD _Import FDP_ACC.1/Signature_Creation
FMT_MSA.4/Keygen	(FDP_ACC.1) or (FDP_IFC.1)	FDP_ACC.1/SCD/SVD_Generation FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FPT_EMS.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_PHP.1	No dependencies	
FPT_PHP.3	No dependencies	
FPT_TST.1	No dependencies	
FTP_ITC.1/SCD Import	No dependencies	

Table 14: Dependency rationale

6.3.3 Security Assurance Requirements Rationale

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

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

FCS_CKM.1 and FCS_COP.1 of [ST-IAS] are supported by FCS_CKM.1and FCS_COP.1 of [ST-PLTF].
FDP_SDI.2 of [ST-IAS] is supported by FDP_SDI.2 of [ST-PLTF].
FPT_EMS.1, FPT_FLS.1, FPT_PHP.1 and FPT_PHP.3 of [ST-IAS] are supported by FPT_EMS.1, FPT_FLS.1, FPT_PHP.1 and FPT_PHP.3 of [ST-PLTF].

FCS_CKM.4, FDP_ACC.1, FDP_ACF.1, , FDP_ITC.1, FDP_RIP.1, FDP_UCT.1, FDP_UIT.1, FIA_AFL.1, , FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4 FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FTP_ITC.1, and are SFR specific to the IAS application and they do no conflict with the SFR of [ST-PLTF].

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

7. TOE SUMMARY SPECIFICATION

7.1 TOE SECURITY FUNCTIONS

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

7.1.1 SF provided by IAS Application

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 15: *TOE security functions list*

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

- Signatory authentication failure as defined in **FIA_AFL.1/SIG**,
- Timing of signatory identification and authentication as defined in **FIA_UID.1/SIG** and **FIA_UAU.1/SIG**,
- Pre-personaliser authentication failure as defined in **FIA_AFL.1/PERSO**,
- Timing of pre-personaliser identification and authentication as defined in **FIA_UID.1/PERSO** and **FIA_UAU.1/PERSO**.

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

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

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

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

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_ITC.1/SCD**,
- Management of functions as defined in **FMT_MOF.1** and **FMT_SMF.1**,
- Management of security attributes **FMT_MSA.1/AdminKG**, **FMT_MSA.1/AdminKI**, **FMT_MSA.1/Signatory**, **FMT_MSA.2**, **FMT_MSA.3/KeyImport**, **FMT_MSA.3/KeyGen**, **FMT_MSA.4/KeyImport**, **FMT_MSA.4/KeyGen**,
- Management of TSF data as defined in **FMT_MTD.1/Admin** and **FMT_MTD.1/Signatory**,
- Management of roles as defined in **FMT_SMR.1**,

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

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

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 16: Security Functions provided by the MultiApp V31 Platform

These SF are described in [ST-PLTF].

7.2 TOE SUMMARY SPECIFICATION RATIONALE

7.2.1 TOE security functions rationale

Requirements	SF.Authentication	SF.Crypto	SF.Integrity	SF.Management	SF.Secure_Messaging	SF.CSM
FCS_CKM.1/SCD		X				
FCS_CKM.1/Session		X				
FCS_CKM.4/SCD		X				
FCS_CKM.4/Session		X				
FCS_COP.1/DSC		X				
FCS_COP.1/Session		X				
FDP_ACC.1/Signature-creation				X		
FDP_ACF.1/Signature-creation				X		
FDP_ACC.1/SCD/SVD_Generation				X		
FDP_ACF.1/SCD/SVD_Generation				X		
FDP_ACC.1/SVD transfer				X		
FDP_ACF.1/SVD transfer				X		
FDP_ACC.1/SCD import				X		
FDP_ACF.1/SCD import				X		
FDP_ITC.1/SCD				X		
FDP_RIP.1						X
FDP_SDI.2/Persistent			X			
FDP_SDI.2/DTBS			X			
FDP_UCT.1/SCD					X	
FIA_AFL.1/SIG	X					
FIA_UAU.1/SIG	X					
FIA_UID.1/SIG	X					
FMT_MOF.1				X		
FMT_MSA.1/AdminKG				X		
FMT_MSA.1/AdminKI				X		
FMT_MSA.1/Signatory				X		
FMT_MSA.2				X		
FMT_MSA.3/KeyImport				X		
FMT_MSA.3/KeyGen				X		
FMT_MSA.4/KeyImport				X		

Requirements	SF.Authentication	SF.Crypto	SF.Integrity	SF.Management	SF.Secure_Messaging	SF.CSM
FMT_MSA.4/KeyGen				X		
FMT_MTD.1/Admin				X		
FMT_MTD.1/Signatory				X		
FMT_SMF.1				X		
FMT_SMR.1				X		
FPT_EMS.1						X
FPT_FLS.1						X
FPT_PHP.1						X
FPT_PHP.3						X
FPT_TST.1						X
FTP_ITC.1/SCD Import					X	

Table 17: Rationale table of functional requirements and security functions