

IAS on M7793 Security Target Lite

UPDATES

Date	Author	Modification
January 15 th 2016	Gemalto	Creating from evaluated ST (V1.2)

CONTENT

1. SECURITY TARGET INTRODUCTION	4
1.1 SECURITY TARGET REFERENCE	4
1.2 TOE REFERENCE	4
1.3 SECURITY TARGET OVERVIEW	4
1.4 REFERENCES	6
1.4.1 External References	6
1.4.2 Internal References	8
1.5 ACRONYMS AND GLOSSARY	8
2. TOE OVERVIEW	10
2.1 TOE DESCRIPTION	10
2.2 TOE BOUNDARIES	10
2.3 TOE LIFE-CYCLE	11
2.3.1 Four phases	11
2.3.2 Actors	14
2.3.3 Involved sites	14
2.3.4 Pre-personalization at Gemalto site	15
2.3.5 Pre-personalization on inlay at Gemalto site	16
3. CONFORMANCE CLAIMS	16
3.1 CC CONFORMANCE CLAIM	16
3.2 PP CLAIM	17
3.3 PACKAGE CLAIM	17
4. SECURITY PROBLEM DEFINITION	18
4.1 GENERAL	18
4.2 THREATS	18
4.3 ORGANIZATIONAL SECURITY POLICIES	19
4.4 ASSUMPTIONS	20
4.5 COMPATIBILITY BETWEEN SECURITY ENVIRONMENTS OF [ST-IAS] AND [ST-PLTF]	20
4.5.1 Compatibility between threats of [ST-IAS] and [ST-PLTF]	20
4.5.2 Compatibility between OSP of [ST-IAS] and [ST-PLTF]	20
4.5.3 Compatibility between assumptions of [ST-IAS] and [ST-PLTF]	21
4.6 JUSTIFICATIONS FOR ADDING ASSUMPTIONS ON THE ENVIRONMENT	21
4.6.1.1 Additions to [PP-SSCD-KG]	21
5. SECURITY OBJECTIVES	22
5.1 GENERALS	22
5.2 SECURITY OBJECTIVES FOR THE TOE	22
5.2.1 Common to Part 2 and Part 3	22
5.2.2 Part 2 specific	23
5.2.3 Part 3 specific	23
5.2.4 Part 4 specific (additional security objectives related to part 2)	23
5.2.5 Part 5 and part 6 extension (additional security objectives related to part 2 & part 3)	23
5.2.6 Extensions	24
5.3 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	24
5.3.1 Common to Part 2 and Part 3	24
5.3.2 Part 3 specific	24
5.3.3 Part 4 specific (additional security objectives related to part 2)	25
5.3.4 Part 5 and part 6 extension (additional security objectives related to part 2 & part 3)	26
5.4 SECURITY OBJECTIVE RATIONALE	27
5.4.1 Threats	27
5.4.2 Organisational security policies	29
5.4.3 Assumptions	31
5.4.4 Compatibility between objectives of [ST-IAS] and [ST-PLTF]	32
5.4.4.1 Compatibility between objectives for the TOE	32
5.4.4.2 Compatibility between objectives for the environment	32
5.4.5 Justifications for adding & substitution objectives on the environment	32

5.4.5.1	Additions to [PP-SSCD-KG]	32
5.4.5.2	Additions to [PP-SSCD-KI].....	33
5.4.5.3	Substitution.....	33
6.	EXTENDED COMPONENTS DEFINITION.....	34
6.1	DEFINITION OF THE FAMILY FPT_EMS.....	34
6.2	DEFINITION OF THE FAMILY FIA_API.....	35
7.	SECURITY REQUIREMENTS	35
7.1	SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE	35
7.1.1	<i>Class Cryptographic Support (FCS)</i>	36
7.1.2	<i>Class FDP User Data Protection</i>	38
7.1.3	<i>Class FIA Identification and Authentication</i>	42
7.1.4	<i>Class FMT Security Management</i>	44
7.1.5	<i>Class FPT Protection of the Security Functions</i>	47
7.1.6	<i>Class FTP Trusted Path/Channel</i>	49
7.2	SECURITY ASSURANCE REQUIREMENTS FOR THE TOE.....	50
8.	TOE SUMMARY SPECIFICATION	51
8.1	TOE SECURITY FUNCTIONS.....	51
8.1.1	<i>SF provided by IAS Application</i>	51
8.1.2	<i>TSFs provided by the platform</i>	52

FIGURES

Figure 1:	TOE Boundaries.....	11
Figure 2:	TOE Personalization	12
Figure 3:	TOE Operational Use.....	13
Figure 4:	LC1: Pre-personalization on module at Gemalto site	15
Figure 5:	LC2: Pre-personalization on inlay at Gemalto site.....	16

TABLES

Table 1:	Identification of the actors	14
Table 3:	Threats, Assumptions, and Policies vs. Security objectives	27
Table 4:	FCS_CKM.1/SCD refinement	36
Table 5:	FCS_CKM.1/Session refinement	36
Table 6:	FCS_CKM.4 refinement.....	37
Table 7:	FCS_CKM.4 refinement.....	37
Table 8:	FCS_COP.1/DSC refinement	37
Table 9:	FCS_COP.1/Other refinement	38
Table 10:	Subjects and security attributes for access control.....	38
Table 11:	FIA_AFL.1/PERSO refinements	43
Table 12:	conditions triggering tests.....	48
Table 16:	TOE security functions list	51
Table 17:	Security Functions provided by the Multiapp V3 Platform	52

1. SECURITY TARGET INTRODUCTION

1.1 SECURITY TARGET REFERENCE

Title :	MultiApp Essential IAS V1 Security Target Lite on M7793
Version :	1.2p
ST Reference :	D1341165_93
Origin :	Gemalto
IT Security Evaluation scheme :	Serma Technologies
IT Security Certification scheme :	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

1.2 TOE REFERENCE

Product Name :	MultiApp Essential v1.0
TOE Name :	IAS Classic v3 over MultiApp Essential v1.0 on M7793
TOE Version :	3.4.e
Security Controllers :	M7793
TOE documentation :	Guidance [AGD]

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

The TOE and the product differ, as further explained in §2.2 TOE boundaries:

- The TOE is the IAS application.
- Additionally, other applets – not determined at the moment of the present evaluation – may be loaded on the smartcard before or after issuance.

1.3 SECURITY TARGET OVERVIEW

The Target of Evaluation (TOE) is composed of the MultiApp Essential V1.0 platform and the electronic signature application IAS.

The platform includes the hardware and the operating system.

The IC is evaluated in conformance with [PP-IC-0035].

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

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

The main objectives of this Security Target 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.

1.4 REFERENCES

1.4.1 External References

[CC]	Common Criteria 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-2009-07-004, version 3.1 rev 4, September 2012
[PP-IC-0035]	<i>Smartcard IC Platform protection Profile</i> 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
[PP-SSCD-KG TCCGA TCSCA]	[EN-14169-2] & [EN-14169-4] & [EN-14169-5]
[PP-SSCD-KI TCSCA]	[EN-14169-3] & [EN-14169-6]
[EN-14169-2]	Protection profiles for secure signature creation device – Part2 : Device with key generation BSI-CC-PP-0059-2009-MA-01, Version 2.0;1, February 2012
[EN-14169-3]	Protection profiles for secure signature creation device – Part3: Device with key import BSI-CC-PP-0075-2012, Version 1.0.2, September 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 BSI-CC-PP-0071-2012, Version 1.0.1, December 2012
[EN-14169-5]	Protection profiles for secure signature creation device – Part5: Extension for device with key generation and trusted communication with signature-creation application BSI-CC-PP-0072-2012, Version 1.0.1, December 2012
[EN-14169-6]	Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application BSI-CC-PP-0076-2013, Version 1.0.4, April 2013
[IFX]	Infineon References
[ST-IC]	[ST-IC-M7793] & [ST-IC-M7794]
[ST-IC-M7793]	ST of M7793 A12 and G12 – version 1.4 2013-11-14
[ST-IC-M7794]	ST of M7794 A12 and G12 – version 2.3 2011-11-27
[CR-IC]	[CR-IC-M7793] & [CR-IC-M7794]
[CR-IC-M7793]	<i>Certification Report, SLE77CFX2400P / M7793 A12 and G12 BSI-DSZ-CC-0926-2014</i>

MultiApp Essential: IAS Security Target Lite on M7793

[CR-IC-M7794]	<i>Certification Report, SLE77CLFX2400PH / M7794 A12 and G12 BSI-DSZ-CC-0917-2014</i>
[NIST]	NIST references
[FIPS180-2]	<i>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</i>
[FIPS46-3]	<i>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</i>
[ISO]	ISO references
[ISO15946-1]	<i>ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002</i>
[ISO15946-2]	<i>ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures, 2002</i>
[ISO15946-3]	<i>ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment, 2002</i>
[ISO7816]	<i>ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS2004</i>
[ISO9796-2]	<i>ISO/IEC 9797: Information technology – Security techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002</i>
[ISO9797-1]	<i>ISO/IEC 9797: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, 1999</i>
[RSA]	RSA Data Security Inc. references
[PKCS#3]	<i>PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993</i>
[JCS]	Javacard references
[PP-JCS-Open]	<i>Java Card System Protection Profile – Open Configuration ANSSI-PP-2010-03M01, Version 3.0, May 2012</i>
[GP]	Global Platform references
[GP221]	<i>GlobalPlatform Card Technology Secure Channel Protocol 03 Card Specification v 2.2 – Amendment D Version 1.0 Public Release April 2009</i>
[GP221Amend D]	<i>Global Platform Specification 2.2 Amendment D – SCP03 v1.1.1</i>
[GP221Amend E]	<i>Global Platform Specification 2.2 Amendment E – Security Upgrade v1.0.1</i>
[GP221 MpGd]	<i>Global Platform Mapping guidelines v1.0.1</i>
[GP221 Id Config]	<i>Global Platform – ID Configuration v1.0.</i>
[Euro]	European Union
[DirectiveEC]	<i>DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures</i>

1.4.2 Internal References

[ST-PLTF]	D1341162_93 MultiApp Essential: JCS Security Target on M7793
[GUIDE]	IAS v3 user guidance Multiapp V3 platform User Guidance
[PRE_IAS]	Preparative procedures
[OPE_IAS]	Operational User Guidance

1.5 ACRONYMS AND GLOSSARY

Acr.	Term	Definition
SCD	Signature-creation data	private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature.
SVD	Signature-verification data	public cryptographic key that can be used to verify an electronic signature.
SCA	Signature-creation application	application complementing an SSCD with a user interface with the purpose to create an electronic signature.
CGA	Certificate-generation application	collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate.
	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 I (IC identification data).
IC	Integrated circuit	Electronic component(s) designed to perform processing and/or memory functions. The MultiApp's chip is a integrated circuit.
	Personalization	The process by which the portrait, signature and biographical data are applied to the document. [SS]
	Personalization Agent	The agent acting on the behalf of the issuing State or organization to personalize the TOE for the holder.
	Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
	Pre- personalization Data	Any data that is injected into the non-volatile memory of the TOE by the TOE Manufacturer (Phase 2) for traceability of non-personalized TOE's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair.
	Pre –personalized TOE's chip	TOE's chip equipped with pre-personalization data.

	TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [1]).
	User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [1]).

2. TOE OVERVIEW

2.1 TOE DESCRIPTION

IAS is a Java Card application that provides a Secure Signature Creation Device [SSCD] as defined in the 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 (included in this TOE):

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

The IAS application can be used in contact 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
- Authentication of the administrator (mutual authentication):
 - Symmetric scheme with TDES or AES
 - Asymmetric scheme with Diffie-Hellman based on RSA
- 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

2.2 TOE BOUNDARIES

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

- The underlying Integrated Circuit
- The MultiApp Essential V1.0 platform (Java Card platform)
- The IAS Application

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

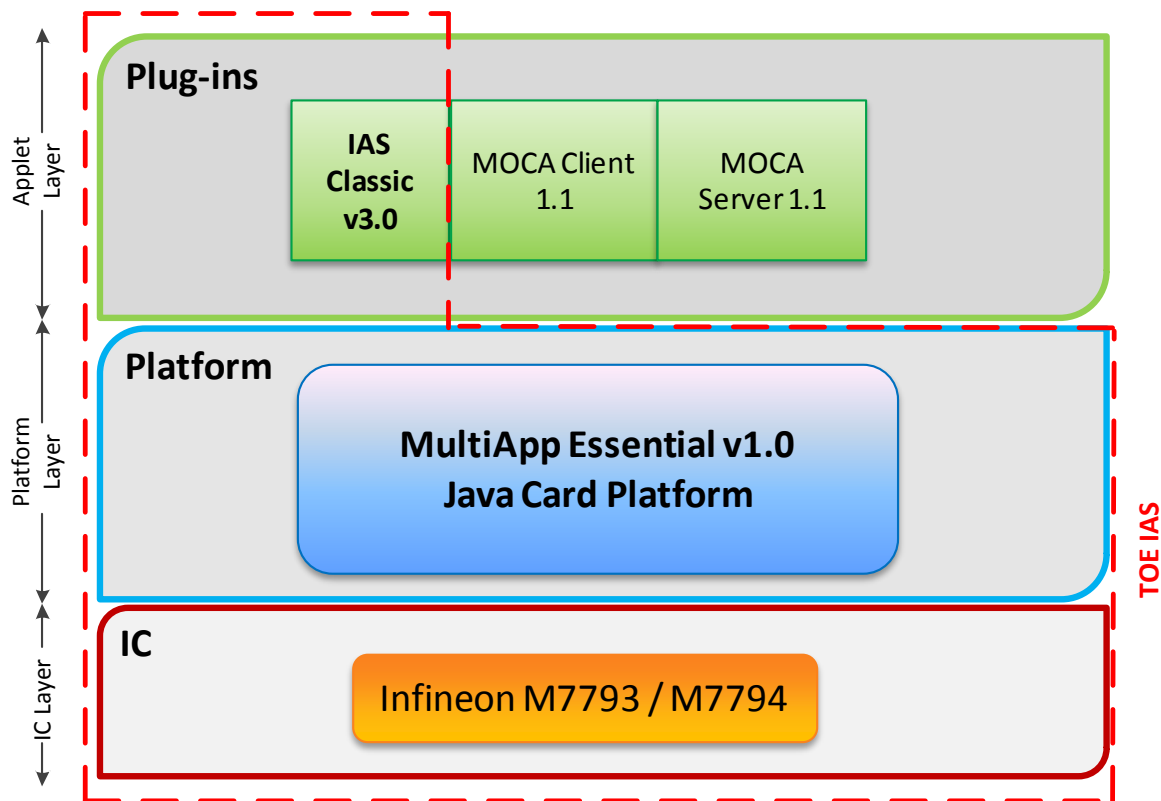


Figure 1: TOE Boundaries

2.3 TOE LIFE-CYCLE

2.3.1 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 including flash loader and dedicated transport key. The IC is securely delivered from the IC manufacturer to the SSCD manufacturer.

The SSCD manufacturer has the following tasks:

- **Initialization:** Load software in the flash memory,
- **Pre-personalization:** initialization of the SSCD application,

Phase 3 Personalization of the TOE:

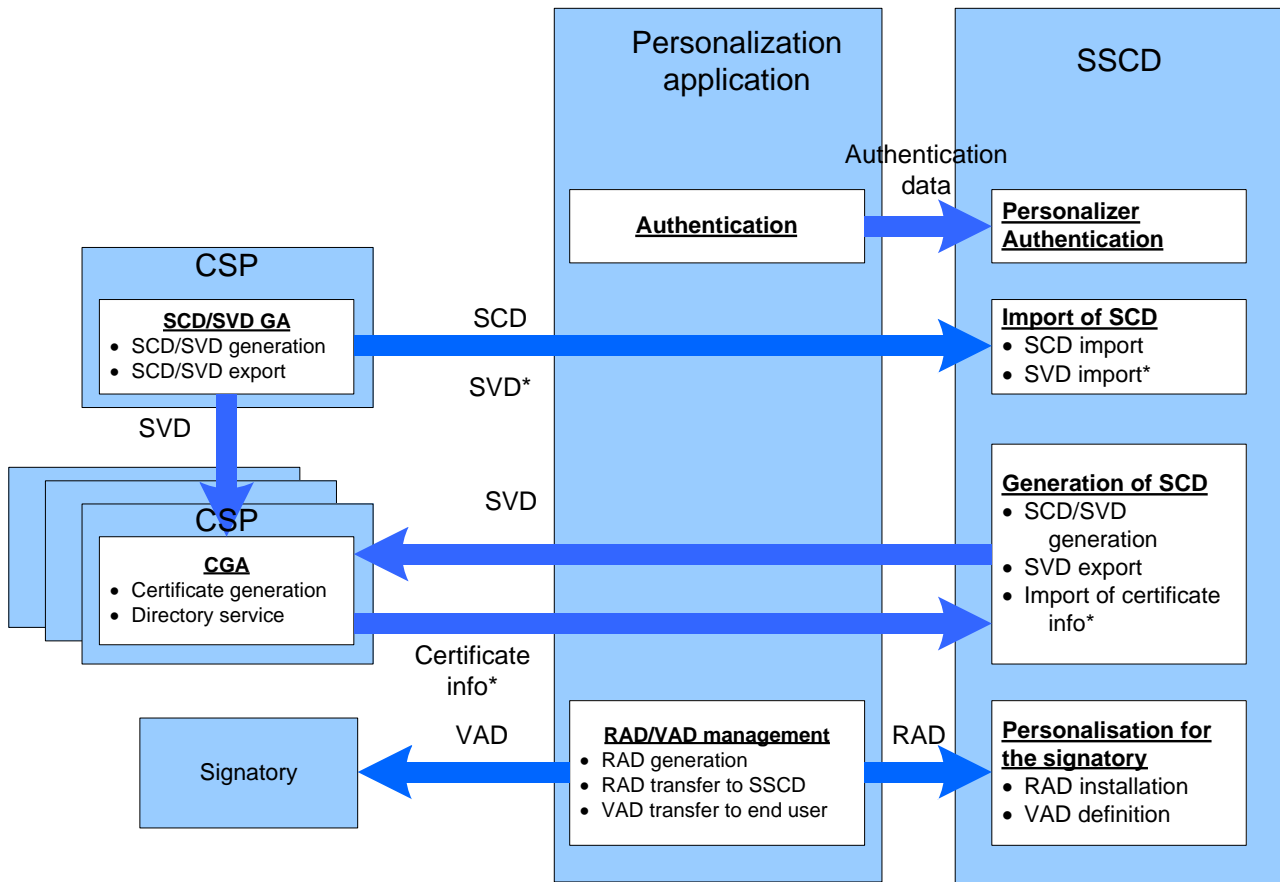


Figure 2: TOE Personalization

RAD Import in the Personalization phase,

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

SCD Import in the Personalization phase,

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

Phase 4 "Operational Use"

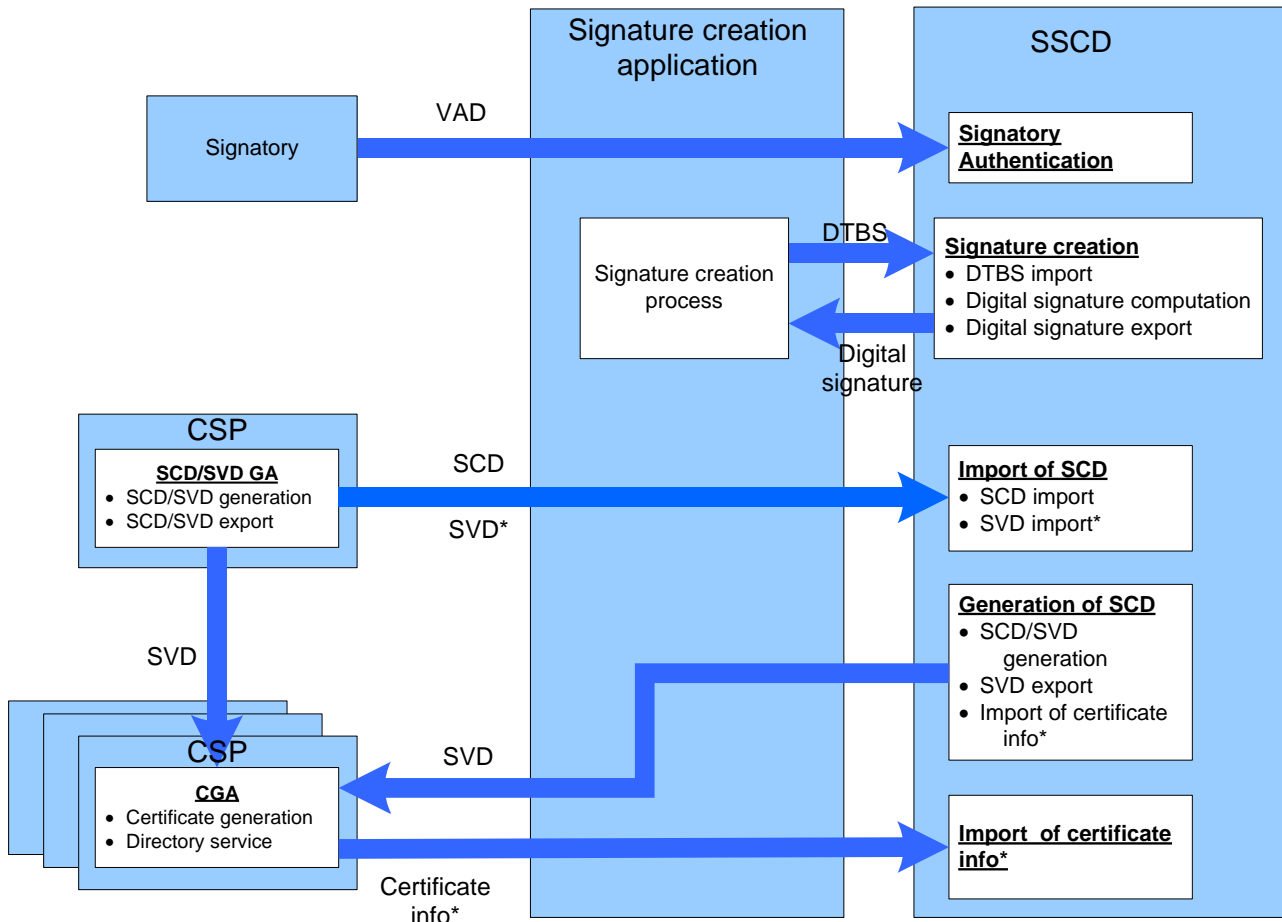


Figure 3: TOE Operational Use

SCD/SVD generation in the usage phase,

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

SCD Import in the usage phase,

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

Signature Creation in the usage phase,

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

- The TOE computes the Signature.
- The TOE sends the Signature to the SCA.

2.3.2 Actors

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

Table 1: Identification of the actors

2.3.3 Involved sites

Life cycle phase	Involved sites
Embedded software development (Phase 1)	Gemalto Meudon Gemalto Singapore
IC development (Phase 2)	Infineon development site(s) mentioned in [CR-IC-M7793] and [CR-IC-M7794]
IC Manufacturing & Testing (Phase 3)	Infineon production site(s) mentioned in [CR-IC-M7793] and [CR-IC-M7794]
IC initialization, packaging & testing (Phase 4)	Scenario LC1: Gemalto Gémenos site Gemalto Singapore site
Prepersonalization & testing (Phase 5)	Scenario LC1: Gemalto Gémenos site Gemalto Singapore site Gemalto Tczew site Gemalto Vantaa site

2.3.4 Pre-personalization at Gemalto site

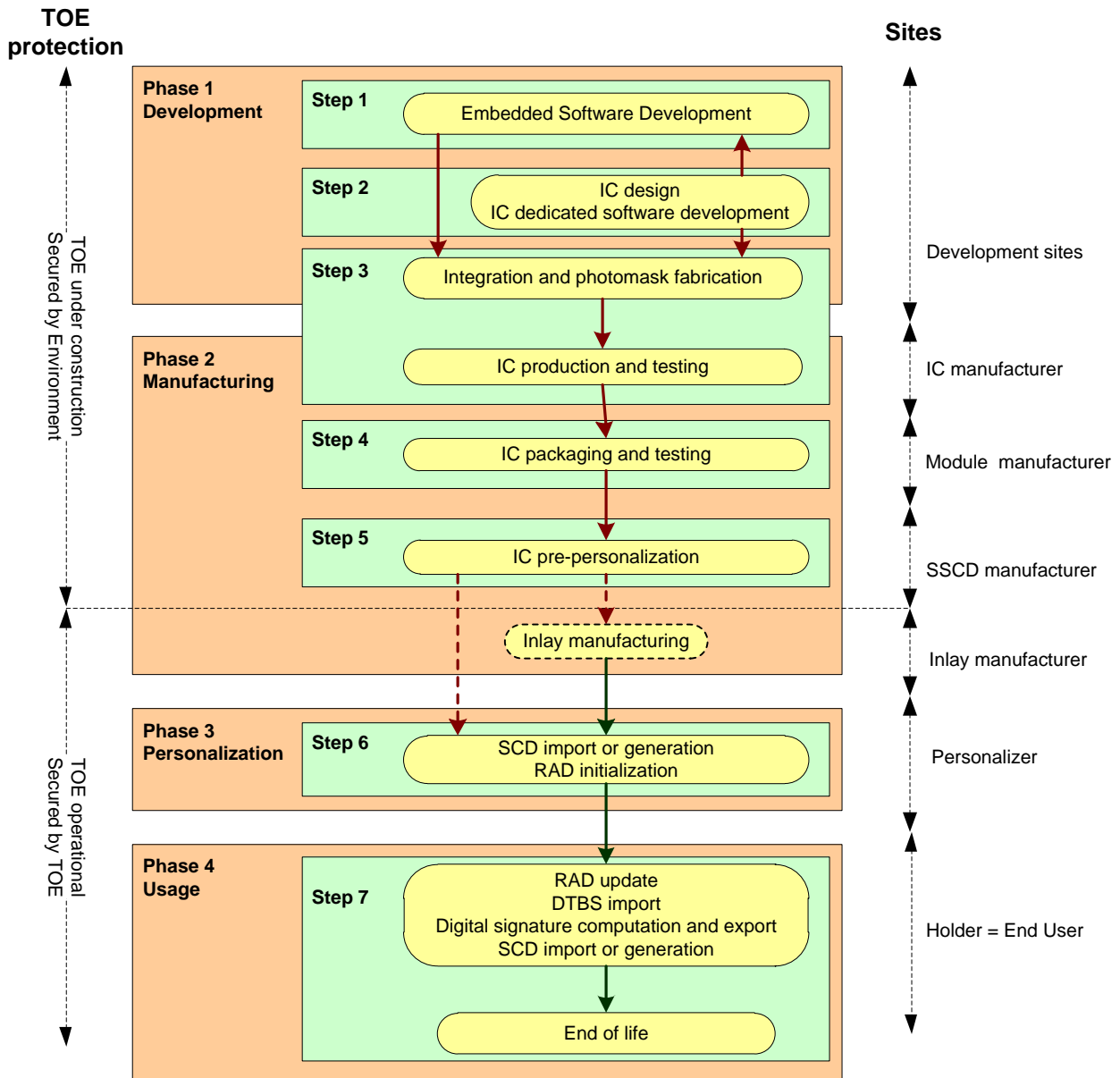


Figure 4: LC1: Pre-personalization on module at Gemalto site

Figure 4: LC1: Pre-personalization on module at Gemalto site describes the standard Life Cycle. The IC 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.

2.3.5 Pre-personalization on inlay at Gemalto site

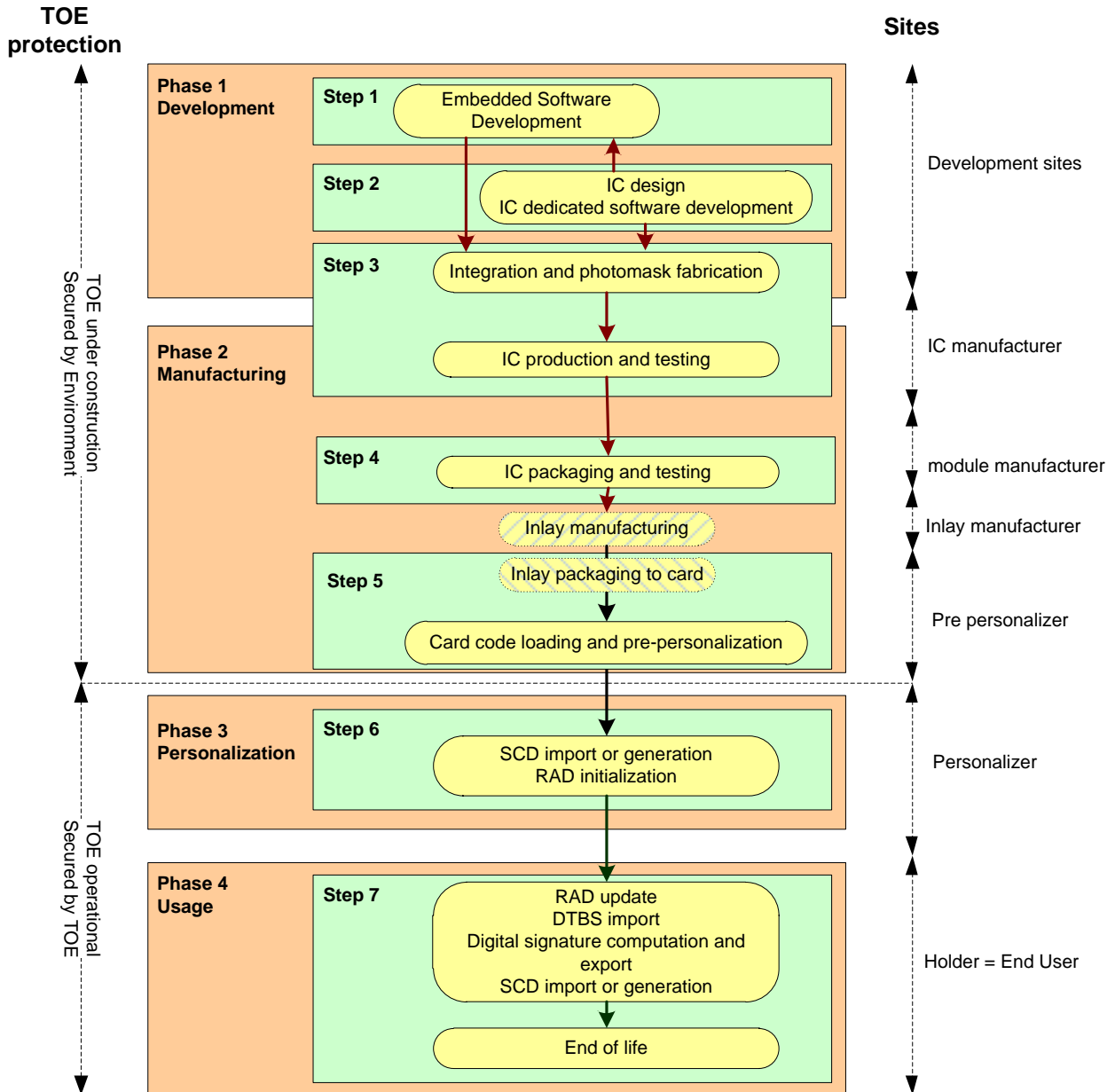


Figure 5: LC2: Pre-personalization on inlay at Gemalto site

LC2 is another alternative to LC1. *Figure 5: LC2: 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.

3. CONFORMANCE CLAIMS

3.1 CC CONFORMANCE CLAIM

This security target claims conformance to

- [CC-1]

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

as follows

- Part 2 extended,
- Part 3 conformant.

The

- [CEM] has to be taken into account.

The evaluation of the TOE uses the result of the CC evaluation of the platform MultiApp V3 claiming conformance to [PP-JCS-Open].

3.2 PP CLAIM

This MultiApp Essential IAS V1.0 security target claims strict conformance to the following Protection Profiles:

- [PP-SSCD-KG TCCGA TCSCA] including [PP-SSCD-KG], which defines security requirements for an SSCD with SCD/SVD key generation and signature creation, with extension [EN14169-4] related to trusted communication between SSCD and CGA and extension [EN-14169-5] related to trusted communication between SSCD and SCA.
- [PP-SSCD-KI TCSCA] including [PP-SSCD-KI], which defines security requirements for an SSCD with SCD key import and signature creation with extension [EN-14169-6] related to trusted communication between SSCD and SCA.

The evaluation is a composite evaluation and uses the results of the CC evaluation of the MultiApp Essential V1 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-JCS].

The MultiApp Essential V1 JCS security target [ST-JCS], claims demonstrable conformance to the Protection Profile “JavaCard System – Open configuration”, ANSSI-PP-2010- 03, Version 2.6 ([PP-JCS-Open]).

3.3 PACKAGE CLAIM

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

4. SECURITY PROBLEM DEFINITION

4.1 GENERAL

The assets, threats, OSP, and assumptions of the TOE are those defined in [PP-SSCD-KG], [PP-SSCD-KI] (no additional assets, threats, OSP, and assumptions in extension [EN 14169-4], [EN 14169-5], [EN 14169-6]) The present Security Target deals with the assets, threats, OSP, and assumptions of [PP-SSCD-KG] and [PP-SSCD-KI].

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

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

Assets and objects:

1. SCD: private key used to perform an electronic signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.
2. SVD: public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported must be maintained.
3. DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.

User and subjects acting for users:

1. User: End user of the TOE who can be identified as Administrator or Signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.
2. Administrator: User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as Administrator.
3. Signatory: User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.

Threat agents:

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

4.2 THREATS

T.SCD_Divulg *Storing , copying, and releasing of the signature-creation data*

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

T.SCD_Derive *Derive the signature-creation data*

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

T.Hack_Phys *Physical attacks through the TOE interfaces*

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

T.SVD_Forgery *Forgery of signature-verification data*

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

T.SigF_Misuse *Misuse of the signature creation function of the TOE*

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

T.DTBS_Forgery *Forgery of the DTBS-representation*

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

T.Sig_Forgery *Forgery of the electronic signature*

An attacker forges a signed data object, maybe using an electronic signature which has been created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

4.3 ORGANIZATIONAL SECURITY POLICIES

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

P.CSP_QCert *Qualified certificate*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (see [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 by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under his sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

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

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

The TOE meets the requirements for an SSCD laid down in Annex III of the Directive [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 life cycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

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

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

4.4 ASSUMPTIONS

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

A.CGA *Trustworthy certification-generation application*

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

A.SCA *Trustworthy signature-creation application*

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

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

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

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

4.5.1 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.SVD_Forgery, T.DTBS_Forgery, T.Sig_Repud, 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.

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

P.CSP_QCert, P.Qsign, P.Sigy_SSCD, P.Sig_Non_Repud 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.

4.5.3 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 not conflict with the assumptions of [ST-PLTF].

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

4.6 JUSTIFICATIONS FOR ADDING ASSUMPTIONS ON THE ENVIRONMENT

4.6.1.1 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.

5. SECURITY OBJECTIVES

5.1 GENERALS

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

The security objectives of the TOE are those defined in [PP-SSCD-KG], [PP-SSCD-KI] and updated regarding related extension [EN-14169-4], [EN 14 169-5], [EN 14169-6]

The present Security Target deals with security objectives of [PP-SSCD-KG] and [PP-SSCD-KI] and updated regarding related extension [EN-14169-4], [EN 14 169-5], [EN 14169-6]

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

5.2 SECURITY OBJECTIVES FOR THE TOE

5.2.1 Common to Part 2 and Part 3

OT.Lifecycle_Security *Lifecycle security*

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

OT.SCD_Secrecy *Secrecy of signature-creation data*

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

OT.Sig_Secure *Cryptographic security of the electronic signature*

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

OT.Sigy_SigF *Signature generation function for the legitimate signatory only*

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

OT.DTBS_Integrity_TOE *DTBS/R integrity inside the TOE*

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

OT.EMSEC_Design *Provide physical emanations security*

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

OT.Tamper_ID *Tamper detection*

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

OT.Tamper_Resistance *Tamper resistance*

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

5.2.2 Part 2 specific

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

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

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

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

OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*

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

5.2.3 Part 3 specific

OT.SCD_Auth_Imp *Authorised SCD import*

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

5.2.4 Part 4 specific (additional security objectives related to part 2)

OT.TOE_SSCD_Auth *Authentication proof as SSCD*

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

OT.TOE_TC_SVD_Exp *TOE trusted channel for SVD export*

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

5.2.5 Part 5 and part 6 extension (additional security objectives related to part 2 & part 3)

OT.TOE_TC_VAD_Imp *Trusted channel of TOE for VAD import*

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

OT.TOE_TC_DTBS_Imp *Trusted channel of TOE for DTBS import*

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

5.2.6 Extensions

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

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

5.3 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

5.3.1 Common to Part 2 and Part 3

OE.SVD_Auth *Authenticity of the SVD*

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

OE.CGA_Qcert *Generation of qualified certificates*

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

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

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

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

The signatory shall use a trustworthy SCA that

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

OE.Signatory *Security obligation of the Signatory*

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

5.3.2 Part 3 specific

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

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

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

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

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

OE.SCD_Secrecy *SCD Secrecy*

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

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

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

OE.SCD_SVD_Corresp *Correspondence between SVD and SCD*

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

5.3.3 Part 4 specific (additional security objectives related to part 2)

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

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

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

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

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

OE.CGA_TC_SVD_Imp *CGA trusted channel for SVD import*

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

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

weaken the security objectives of and requirements to the TOE but enforce more security functionality of the TOE for additional method of use. Therefore it does not conflict with the CC conformance claim to the core [PP_SSCD_KG]

5.3.4 Part 5 and part 6 extension (additional security objectives related to part 2 & part 3)

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

OE.HID_TC_VAD_Exp *Trusted channel of HID for VAD export*

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

OE.SCA_TC_DTBS_Exp *Trusted channel of SCA for DTBS export*

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

5.4 SECURITY OBJECTIVE RATIONALE

Threats - Assumptions / Policies / Security objectives	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	OT.TOE_SSCD_Auth (part 4)	OT.TOE_TC_SVD_Exp (part 4)	OT.TOE_TC_VAD_Imp (part 5 & 6)	OT.TOE_TC_DTBS_Imp (part 5 & 6)	OE.SVD_Auth	OE.CGA_QCert	OE.SSCD_Prov_Service (part 3)	OE.DTBS_Intend	OE.Signatory	OE.SCD/SVD_Auth_Gen	OE_SCD_Secrecy	OE_SCD_Unique	OE.SCD_SVD_Corresp	OE.Dev_Prov_Service (part 4) replace OE.SSCD_Prov_Service (in part 2)	OE.CGA_SSCD_Auth (part 4)	OE.CGA_TC_SVD_Imp (part 4)	OE.HID_TC_VAD_Exp (part 5 & 6) replace OE.HID_VAD	OE.SCA_TC_DTBS_Exp (part 5 & 6) replace OE.DTBS_Protect		
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									X	X		
T.DTBS_Forgery					X												X				X											X	
T.Sig_Forgery			X						X									X						X									
P.CSP_Qcert	X									X	X			X				X					X		X		X						
P.QSign			X	X														X		X													
P.Sigy_SSCD	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
P.Sig_Non-Repud	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
P.Pre-personalisation													X																				
A.SCA																				X													
A.CGA																		X	X														
A.CSP																								X	X	X	X						

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

5.4.1 Threats

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

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

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

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

T.SCD_Derive (*Derive the signature creation data*) deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD.

OT.SCD/SVD_Auth_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD pair (when SCD is generated on-TOE).

OE.SCD_Unique counters this threat by implementing cryptographically secure generation of the SCD/SVD pair (when SCD is generated off-TOE).

OT.Sig_Secure ensures cryptographically secure electronic signatures.

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

T.SVD_Forgery (*Forgery of the signature verification data*) deals with the forgery of the SVD exported by the TOE to the CGA for certificate generation. T.SVD_Forgery is addressed by:

- OT.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD (when SCD is generated on-TOE),
 - OE.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD (when SCD is generated off-TOE), and
 - OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA and verification of the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.
- (This is specific to [PP SSCD KG] extended with part 4.) Additionally T.SVD_Forgery is addressed by OT.TOE_TC_SVD_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA_TC_SVD_Imp, which provides verification of SVD authenticity by the CGA.

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

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

T.Sig_Forgery (*Forgery of the electronic signature*) deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique and OE.CGA_QCert address this threat in general. OT.Sig_Secure (*Cryptographic security of the electronic signature*) ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together.

OT.SCD_Unique (when SCD is generated on-TOE) or OE.SCD_Unique (when SCD is generated off-TOE) ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

5.4.2 Organisational security policies

P.CSP_QCert (*CSP generates qualified certificates*)

Dedicated to [PP SSSD KI]

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

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

Dedicated to [PP SSSD KG] extended with part 4

provides that the TOE and the SCA may be employed to sign data with (qualified) electronic signatures, as defined by **the directive** (article 5, paragraph 1) refers to SSSDs to ensure the functionality of advanced signatures. The OE.CGA_QCert addresses the requirement of qualified (or advanced) electronic signatures as being based on qualified (or non-qualified) certificates. According to OT.TOE_SSSD_Auth the copies of the TOE will hold unique identity and authentication data as SSSD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSSD to prove this identity as SSSD to the CGA. The OE.CGA_SSSD_Auth ensures that the SP checks the proof of the device presented of the applicant that it is a SSSD. The OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE to the CGA corresponds to the SCD stored in the TOE and used by the signatory. The OT.Lifecycle_Security ensures that the TOE detects flaws during the initialisation, personalisation and operational usage.

P.QSign (*Qualified electronic signatures*) provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE creates electronic signatures, which cannot be forged without 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_SSSD (*TOE as secure signature creation device*) requires the TOE to meet Annex III of **the directive**.

Dedicated to [PP SSSD KI]

This is ensured as follows

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

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

Dedicated to [PP SSCD KG] extended with part 4

The paragraph 1(a) of Annex III is ensured by OT.SCD_Unique requiring that the SCD used for signature creation can practically occurs only once. The OT.SCD_Secrecy OT.Sig_Secure and OT.EMSEC_Design and OT.Tamper_Resistance address the secrecy of the SCD (cf. paragraph 1(a) of Annex III).

OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE. OT.Sigy_SigF meets the requirement in paragraph 1(c) of Annex III by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others. OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of Annex III as the TOE must not alter the DTBS/R. The usage of SCD under sole control of the signatory is ensured by OT.Lifecycle_Security, OT.SCD/SVD_Gen and OT.Sigy_SigF.

OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised TOE from an SSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD In the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA_SSCD_Auth and the received SVD is sent by this SSCD as required by OE.CGA_TC_SVD_Imp. Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

P.Sig_Non-Repud (Non-repudiation of signatures)

[PP SSCD KI] & [PP SSCD KG] extended with part 5 and part 6

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

TOE and used under sole control of the signatory. OT.SCD_SVD_Corresp (when SCD is generated on-TOE) or OE.SCD_SVD_Corresp (when SCD is generated off-TOE) ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. OT.SCD_Unique (when SCD is generated on-TOE) or OE.SCD_Unique (when SCD is generated off-TOE) provides that the signatory's SCD can practically occur just once.

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

Dedicated to [PP SSCD KG] extended with part 4

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

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

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

5.4.3 Assumptions

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

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

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

This assumption is only applicable when SCD is generated off-card.

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

5.4.4.1 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.Sig_Secure, OT.Sig_SigF, OT.SCD/SVD_Auth_Gen, OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.SCD_Auth_Imp, OT.TOE_SSCD_Auth, OT.TOE_TC_SVD_Exp, OT.TOE_TC_VAD_Imp, OT.TOE_TC_DTBS_Imp, 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.

5.4.4.2 Compatibility between objectives for the environment

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

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

5.4.5 Justifications for adding & substitution objectives on the environment

5.4.5.1 Additions to [PP-SSCD-KG]

The only additional objectives on the environment are: OE.SCD/SCD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OE.SCD_SVD_Corresp. 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.

5.4.5.2 Additions to [PP-SSCD-KI]

Additional objectives on the environment are: OE.Dev_Prov_Service, (who replace OE.SSCD_Prov_Service) , OE.CGA_SSCD_Auth, OE.CGA_TC_SVD_Imp, and link to trusted communication with certificate generation application.

This is outside the scope of [PP-SSCD-KI]. Therefore the added objectives on the environment do not weaken the TOE

5.4.5.3 Substitution

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

6. EXTENDED COMPONENTS DEFINITION

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

- FPT_EMS.1 which is defined in [PP-SSCD-KG] and [PP-SSCD-KI].
- FIA_API.1 which is defined in [EN-14169-4].
-

6.1 DEFINITION OF THE FAMILY FPT_EMS

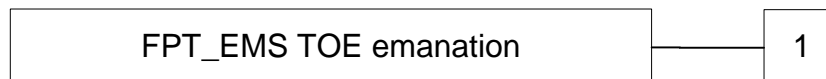
The sensitive family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena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

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

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMS.1 TOE emanation has two constituents:

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

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

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

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

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components

Dependencies: No dependencies.

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

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

6.2 DEFINITION OF THE FAMILY FIA_API

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

FIA_API Authentication Proof of Identity

Family behaviour

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

Component levelling:



FIA_API.1 Authentication Proof of Identity:

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

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components
Dependencies: No dependencies.

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

7. SECURITY REQUIREMENTS

7.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

This chapter defines the security functional requirements for the TOE using functional requirements components as specified in [PP-SSCD-KI], [PP-SSCD-KG] and [EN-14169-4] adding an operation of FIA_UAU.1 and adding SFRs: FIA_API.1, FDP_DAU.2/SVD, FTP_ITC.1/SVD. and [EN-14169-5] & [EN-14169-6] adding an operation of FIA_UAU.1 and adding SFRs: FDP_UIT.1/DTBS, FTP_ITC.1/VAD and FTP_ITC.1/DTBS

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

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

7.1.1 Class Cryptographic Support (FCS)

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

Hierarchical to: No other components
 Dependencies: [FCS_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)

Table 3: FCS_CKM.1/SCD refinement

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

Application note:

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

FCS_CKM.1/Session Cryptographic key generation for session keys

Hierarchical to: No other components
 Dependencies: [FCS_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.

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

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

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,	[ISO9796-2] RSA SHA PKCS#1 v1.5 RSA PSS SHA PKCS#1

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]
/MAC-TDES	MAC computation & Verification	TDES	112	[SP800-67] [ISO9797-1] DES MAC ISO9797-1 M2

Table 8: FCS_COP.1/Other refinement

7.1.2 Class FDP User Data Protection

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

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

Table 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 to objects based on the following:

1. Subjects: S.User,
2. Objects: DTBS/R, SCD
3. Operations: signature creation.

FDP_ACF.1/Signature_Creation Security attribute based access control

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

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

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

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

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

FDP_ACF.1.4 /Signature_Creation The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no".

FDP_ACC.1/SCD/SVD_Generation Subset access control

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

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

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

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

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

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

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

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

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

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

FDP_ACC.1/SVD_Transfer Subset access control

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

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

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

FDP_ACF.1/SVD_Transfer Security attribute based access control

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

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

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

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

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

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

FDP_ACC.1/SCD_Import Subset access control

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

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

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

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

FDP_ACF.1/SCD_Import Security attribute based access control

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

FDP_ACF.1.1 /SCD_Import The TSF shall enforce the SCD Import SFP to objects based on the following:
the S.User is associated with the security attribute “SCD/SVD Management”.

FDP_ACF.1.2 /SCD_Import The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
S.User with the security attribute “SCD/SVD Management” set to “authorised” is allowed to import SCD.

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

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

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

FDP_DAU.2/SVD_ Data Authentication with Identity of Guarantor

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

FDP_DAU.2.1 /SVD The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of SVD.

FDP_DAU.2.2 /SVD The TSF shall provide CGA with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

Application note: Part 4 extension [EN-14169-4] related to core PP key generation [PP-SSCD-KG]..

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

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

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

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

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

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

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components
Dependencies: No dependency

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

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

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

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

FDP_SDI.2/Persistent Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1
Dependencies: No dependency

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for integrity error

/Persistent on all objects, based on the following attributes: integrity checked persistent stored data.

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

FDP_SDI.2/DTBS Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1
Dependencies: No dependency

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

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall :
/DTBS 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 The TSF shall enforce the SCD Import SFP to receive SCD in a manner protected from
/SCD unauthorized disclosure.

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

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

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

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

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

Application note: Part 5 extension [EN-14169-5] related to core PP key generation [PP-SSCD-KG] and Part 6 extension [EN-14169-6] related to core PP key importation [PP-SSCD-KI].

7.1.3 Class FIA Identification and Authentication

FIA_AFL.1/SIG Authentication failure handling

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

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

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

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 attempts using ISK key**.

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.
ISK key	3	Block ISK Key.

Table 10: FIA_AFL.1/PERSO refinements

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components
Dependencies: No dependencies.

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

Application note: Part 4 extension [EN-14169-4] related to core PP key generation [PP-SSCD-KG]..

FIA_UAU.1/PERSO Timing of authentication

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

FIA_UAU.1.1 /PERSO The TSF shall allow
 1. Identification of the user by means of TSF required by FIA_UID.1.
 2. **No other action.**
 on behalf of the user to be performed before the user is authenticated.

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

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

FIA_UAU.1/SIG Timing of authentication

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

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

Application note:

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

Application note: Part 4 extension [EN-14169-4], Part 5 extension [EN-14169-5] and Part 6 extension [EN-14169-6] add operations on FIA-UAU.1/SIG.

FIA_UID.1/PERSO Timing of identification

Hierarchical to: No other components
Dependencies: No dependencies

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

FIA_UID.1/SIG Timing of identification

Hierarchical to: No other components
Dependencies: 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.

7.1.4 Class FMT Security Management

FMT_MOF.1 Management of security functions behaviour

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

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

FMT_MSA.1/Signatory Management of security attributes

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

FMT_MSA.1.1 The TSF shall enforce the Signature-creation SFP to restrict the ability to modify the /Signatory 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.1.1 The TSF shall enforce the SCD/SVD Generation SFP to restrict the ability to modify the /AdminKG security attributes SCD / SVD management to R.Admin.

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

FMT_MSA.1/AdminKI Management of security attributes

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

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

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

FMT_MSA.2 Secure security attributes

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

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

FMT_MSA.3/KeyImport Static attribute initialization

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

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

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

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

FMT_MSA.4/Keygen Static attribute value inheritance

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

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

FMT_MSA.4/KeyImport Static attribute value inheritance

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, 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 while S.Sigy is not currently authenticated, the security attribute “SCD operational” of the SCD shall be set to “no” after import of the SCD as a single operation.
2. If S.Admin imports SCD while the S.Sigy is currently authenticated, the security attribute “SCD operational” of the SCD shall be set to “yes” after import of the SCD as a single operation.

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

FMT_MTD.1/Admin Management of TSF data

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

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

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components
Dependencies: No dependencies

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

1. Creation and modification of RAD.
2. Enabling the signature-creation function.
3. Modification of the security attribute SCD/SVD management, SCD operational.
4. Change the default value of the security attribute SCD Identifier.
5. **No other security management function.**

FMT_SMR.1 Security roles

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

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

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

7.1.5 Class FPT Protection of the Security Functions

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components
Dependencies: No dependencies

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

FPT_EMS.1.2 The TSF shall ensure **[unauthorized users]** are unable to use the following interface:

smart card circuit contacts to gain access to RAD and SCD.

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components
Dependencies: No dependencies

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

FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components
Dependencies: No dependencies

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

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

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components
Dependencies: No dependencies

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

FPT_TST.1 TSF testing

Hierarchical to: No other components
Dependencies: No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests **[see Table 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

7.1.6 Class FTP Trusted Path/Channel

FTP_ITC.1/SCD import Inter-TSF trusted Channel

Hierarchical to: No other components
Dependencies: No dependencies

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

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

FTP_ITC.1.3 /SCD import The TSF shall initiate communication via the trusted channel for

1. Data exchange integrity according to FDP_UCT.1/SCD.
2. **[None].**

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

FTP_ITC.1/SVD Inter-TSF trusted Channel

Hierarchical to: No other components
Dependencies: No dependencies

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

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

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

1. Data authentication with Identity of Guarantor according to FIA_API.1 and FDP_DAU.2/SVD,
2. [None].

Application note: Part 4 extension [EN-14169-4] related to core PP key generation [PP-SSCD-KG]..

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

Hierarchical to: No other components
Dependencies: No dependencies

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

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

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

1. User authentication according to FIA_UAU.1/SIG.,

2. **[None]**.

Application note: Part 5 extension [EN-14169-5] related to core PP key generation [PP-SSCD-KG] and Part 6 extension [EN-14169-6] related to core PP key importation [PP-SSCD-KI].

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

Hierarchical to: No other components
Dependencies: No dependencies

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

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

FTP_ITC.1.3 / DTBS The TSF **or the SCA** shall initiate communication via the trusted channel for
1. signature creation...
2. **[None]**.

Application note: Part 5 extension [EN-14169-5] related to core PP key generation [PP-SSCD-KG] and Part 6 extension [EN-14169-6] related to core PP key importation [PP-SSCD-KI].

7.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

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

8. TOE SUMMARY SPECIFICATION

8.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the IAS application with its OS, and by the chip.

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

8.1.1 SF provided by IAS Application

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

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

Table 12: TOE security functions list

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

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

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

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

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

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

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

- Access management as defined in **FDP_ACC.1** 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**, in **FTP_ITC.1/SVD**, in **FTP_ITC.1/VAD**, in **FTP_ITC.1/DTBS**,

SF.CSM provides cards security protection. It encompasses:

- Protection against physical attacks as defined in **FPT_EMS.1**, **FPT_FLS.1**, **FPT_PHP.1**, and **FPT_PHP.3**,
- Testing of the card as defined in **FPT_TST**,
- Secure unavailability of sensitive data as defined in **FDP_RIP**.

8.1.2 TSFs provided by the platform

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

SF	Description
SF_FW	Firewall
SF_API	Protection against snooping
SF.CSM	Card Security Management
SF.AID	AID Management
SF.INST	Installer
SF.ADEL	Applet Deletion
SF.ODEL	Object Deletion
SF.CAR	Secure Carrier
SF.SCP	Smart Card Platform
SF.CMG	Card Manager
SF.APIS	Specific API
SF.RND	RNG

Table 13: Security Functions provided by the Multiapp V3 Platform

These SF are described in [ST-PLTF].

END OF DOCUMENT