MultiApp ID IAS ECC
Wafer process
Security Target

UPDATES

Date	Author	Modifications
July 21, 2010	Christine Crippa-Martinez	Creating from evaluated ST (V1.1)

CONTENT

1 ST INTRODUCTION 5

1.1 ST REFERENCE 5
1.2 TOE REFERENCE 5
1.3 TOE OVERVIEW 6
1.3.1 TOE type 7
1.3.2 TOE boundaries and out of TOE 7
1.4 TOE DESCRIPTION 8
1.4.1 Platform description 8
1.4.2 IAS ECC Applet description 9
1.4.3 TOE life-cycle 11
1.4.3.1 TOE Phases 13
1.4.4 TOE Environment 13
1.4.4.1 Development phase 14
1.4.4.2 Production environment 15
1.4.4.3 Personalization environment 15
1.4.4.4 User environment 15
1.4.5 The actors and roles 16
1.4.6 TOE intended usage 17
1.5 REFERENCES, GLOSSARY AND ABBREVIATIONS 19
1.5.1 External references 19
1.5.2 Glossary 20
1.5.3 Abbreviations 21

2 CONFORMANCE CLAIMS 23

2.1 CC CONFORMANCE CLAIM 23
2.2 PP CLAIM, PACKAGE CLAIM 23
2.3 CONFORMANCE RATIONALE 23
2.4 PP REFINEMENTS 23
2.5 PP ADDITIONS 27
2.6 ASSURANCE REQUIREMENTS ADDITIONAL TO THE PP 27
2.7 PP CLAIMS RATIONALE 27

3 SECURITY PROBLEM DEFINITION 28

3.1 DIGITAL SIGNATURE ASSETS 28
3.2 DIGITAL SIGNATURE SUBJECTS 28
3.3 DIGITAL SIGNATURE THREATS 29
3.4 DIGITAL SIGNATURE ASSUMPTIONS 29
3.5 ORGANIZATIONAL SECURITY POLICIES 30

4 SECURITY OBJECTIVES 30

4.1 SECURITY OBJECTIVES FOR THE TOE 31
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 32
4.3 SECURITY OBJECTIVES RATIONALE 33
4.3.1 Threats 33
4.3.2 Assumptions 35
4.3.2.1 Additional 35
4.3.3 Organisational security policies 35

5 EXTENDED COMPONENTS DEFINITION 36

6 SECURITY REQUIREMENTS 37

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 37
6.1.1 Security functional requirements list 37

6.1.2 FCS – Cryptographic support 38
6.1.2.1 FCS_CKM cryptographic key management 38
6.1.2.2 FCS_COP Cryptographic operation 39
6.1.3 FDP: User data protection 40
6.1.3.1 FDP_ACC Access Control policy 40
6.1.3.2 FDP_ACF access control function 41
6.1.3.3 FDP_ETC :Export to outside TSF control 43
6.1.3.4 FDP_ITC Import From outside TSF control 43
6.1.3.5 FDP_RIP Residual information protection 44
6.1.3.6 FDP_SDI Stored data integrity 44
6.1.3.7 FDP_UCT Inter-TSF user data confidentiality transfer protection 45
6.1.3.8 FDP_UIT Inter-TSF user data integrity transfer protection 45
6.1.4 FIA: Identification and authentication 46
6.1.4.1 FIA_AFL Authentication failure 46
6.1.4.2 FIA_ATD User attribute definition 46
6.1.4.3 FIA_UAU User authentication 46
6.1.4.4 FIA_UID User Identification 47
6.1.5 FMT: Security management 47
6.1.5.1 FMT_MOF Management of functions in TSF 47
6.1.5.2 FMT_MSA Management of security attributes 47
6.1.5.3 FMT_MTD Management of TSF data 48
6.1.5.4 FMT_SMF Specification of Management Functions 48
6.1.5.5 FMT_SMR Security management roles 48
6.1.6 FPT: Protection of the TSF 49
6.1.6.1 FPT_EMSEC TOE Emanation 49
6.1.6.2 FPT_FLS Failure secure 49
6.1.6.3 FPT_PHP TSF physical Protection 49
6.1.6.4 FPT_TST TSF self test 50
6.1.7 FTP: Trusted Path / Channel 50
6.1.7.1 FTP_ITC Inter-TSF trusted channel 50
6.1.7.2 FTP_TRP Trusted path 51
6.2 SECURITY ASSURANCE REQUIREMENTS 53
6.2.1 TOE security assurance requirements list 53

7 TOE SUMMARY SPECIFICATION 56

7.1 TOE SECURITY FUNCTIONALITIES PROVIDED BY PLATFORM 56
7.1.1 TSF_CARD_EMANATION: Emanation protection 56
7.1.2 TSF_CARD_PROTECT: Card operation protection 56
7.2 TOE SECURITY FUNCTIONALITIES PROVIDED BY IAS ECC APPLET 56
7.2.1 TSF_ AUTHENTICATION: Authentication management 56
7.2.2 TSF_CRYPTO: Cryptography management 57
7.2.3 TSF_INTEGRITY: Integrity monitoring 57
7.2.4 TSF_MANAGEMENT: operation management and access control 58
7.2.5 TSF_SECURE_MESSAGING: secure messaging management 58

FIGURES

Figure 1 - Multiapp ID IAS ECC Card 8
Figure 2 - MultiApp platform architecture 9
Figure 3 - Type 2 and Type 3 SSCD operations 11
Figure 4 - Product Life Cycle “Wafer delivery” 12
Figure 5 - TOE Usage 18

TABLES

Table 1. TOE component 5
Table 2. Multiapp ID IAS ECC Card components 6
Table 3. Smart Card Product Life Cycle 13
Table 4. PP functional requirements that have been refined 24
Table 5. IAS Classic security functional requirements list 38
Table 6. SAR CC V2.3 versus CC V3.1 54
Table 7. TOE security assurance requirements list 55

1 ST INTRODUCTION

1.1 ST REFERENCE

ST Title:	IAS-ECC wafer process - Security Target
ST Reference:	D1152705-Pub
Origin:	GEMALTO
ITSEF	Serma
Certification scheme:	French (ANSSI)

This ST has been built with:

Common Criteria for Information Technology Security Evaluation Version 3.1 which comprises [CCPART1], [CCPART2], and [CCPART3]

Table 1 gives an overview of the components of the TOE.

Component	Version number	Supplier
Hardmask in ROM	1.0	Gemalto
Softmask	1.2	Gemalto
Applet IAS ECC	4.2.7.A	Gemalto
Micro-controller P5CD144	V0B	NXP

Table 1. *TOE component*

Remark: Product identification is in the card identity data, (Gemalto flow version refer this product).

1.2 TOE REFERENCE

TOE Title:	IAS ECC wafer process
Product name:	Multiapp ID IAS ECC wafer process
Commercial name:	MultiApp ID IAS ECC wafer process
Product reference:	T1015174

1.3 TOE OVERVIEW

The Target of Evaluation (TOE) is composed of the **Multiapp** platform and the electronic signature application **IAS ECC**. The platform includes the hardware and the operating system.

The product is a Smart Card Integrated Circuit (IC) with the **Multiapp** platform, the **IAS ECC** applet and the (out-of-TOE) applications defined in Table 2. All ROMed applets are deactivated; **IAS ECC** application is installed in EEPROM.

TOE Components	**Version**	**Constructor**
Micro Controller (P5CD144)	V0B	NXP
Embedded software (platform)	Multiapp version 1.0	GEMALTO
Digital signature application (Applet) in (E2PROM)	IAS ECC	GEMALTO
Other non TOE Components	**Version**	**Constructor**
Instantiable ROMed applet	N/A	
Not instantiable ROMed applets (entry point deactivated)	CryptoManager IAS Premium Gemsafev2 OATH	Precise Biometrics GEMALTO GEMALTO GEMALTO

Table 2. Multiapp ID IAS ECC Card components

The TOE defined in this Security Target is the Secure Signature Creation Device (SSCD) functionalities provided by the IAS ECC application, and supported by the Multiapp Java Card platform.

The other applications are locked and cannot be instantiated or personalized. They are not in the TOE scope and therefore not part of the evaluation.

The TOE will be designed and produced in a secure environment and used by each citizen in a hostile environment.

The product provides an electronic signature services:

- Signature creation
- Signature verification
- Key importation
- Key generation (on board)

The Gemalto **IAS ECC** application is compliant with E-sign specifications (PK and SK authentication).

It covers the identity, digital signature and data storage services. The Digital signature key size is 1024, 1536 or 2048 bits.

The other applications are not in the TOE Scope of Control and therefore not part of the evaluation.

The TOE is a Secure Signature Creation Device (SSCD) that provides both SCD/SVD generation and Signature creation as described in the Protection Profile [PP SSCD2] and Protection Profile [PP SSCD3].

The electronic signature security functions take advantage of the platform security functions:

- Hardware Tamper Resistance is managed by the chip security layer that meets PP SSVG [PP/BSI-0002].

- Secure operation of the Multiapp platform managed inside platform component.

1.3.1 TOE type

The product is a smartcard including a plastic card and a module performing the interface between reader and the embedded chip. Other smart card product elements (such as holograms, security printing…) are outside the scope of this Security Target. The Target of Evaluation (TOE) is the Smart Card Integrated Circuit with Embedded Software in operation and in accordance to its functional specifications.

1.3.2 TOE boundaries and out of TOE

The TOE is composed of the IC, the software platform and a digital signature application:

- **P5CD144** IC which has been certified separately according to [IC-ST] claiming [PP/BSI-0002]
- **Multiapp** platform
- **IAS ECC** application

The **TSFs** are composed of:

1. The digital-signature related functions of the **IAS ECC** application: Signatory Authentication, Signature Creation, SCD/SVD Generation, SCD Import & storage, SVD Export, RAD Import & storage. (Other functions are out of the TOE)
2. Part of Multiapp platform that installs and supports the **IAS ECC** application. (Other multiapp platform function are out of the TOE)
3. **The P5CD144 IC** to supports the Multiapp platform.

Beside the TOE, the product also contains other Java Card applications (out of scope of the TOE)

Figure 1 represents the product. The TOE is bordered with bold and un-continuous line. The architecture of Multiapp inside the TOE is presented in platform description chapter below.

Remark: ROMed applications are deactivated (entry point deactivated).

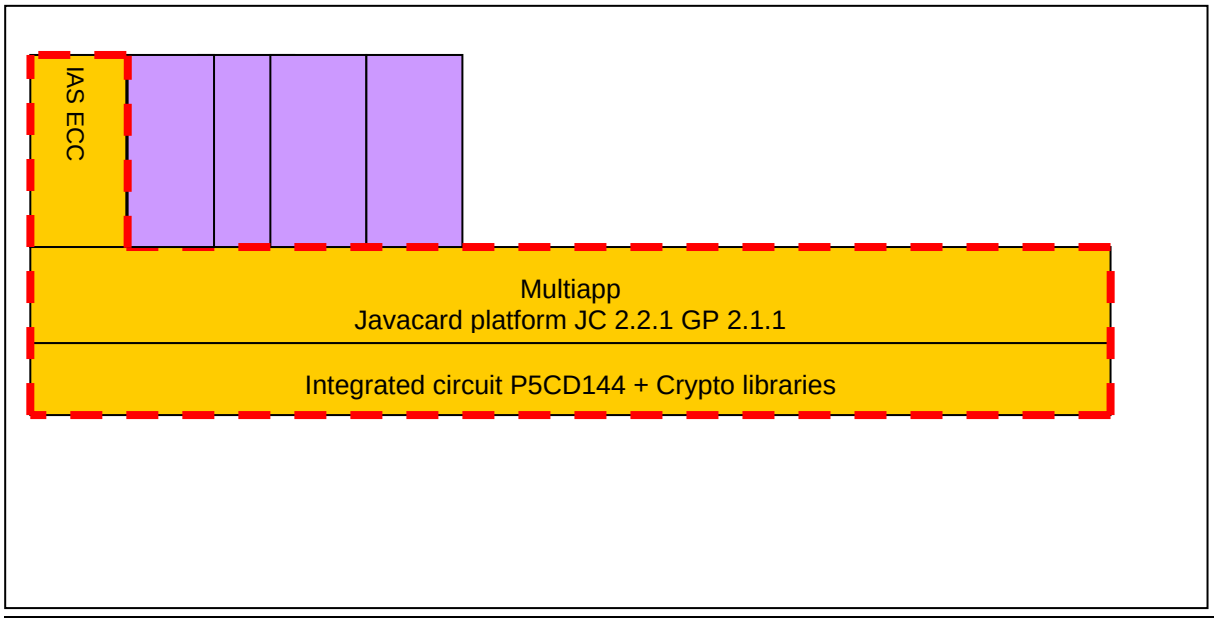


Figure 1 - Multiapp ID IAS ECC Card

1.4 TOE DESCRIPTION

1.4.1 Platform description

MultiApp is a Java Open Platform that complies with two major industry standards:

1. Sun's Java Card 2.2.1, which consists of the Java Card 2.2.1 Virtual Machine, Java Card 2.2.1 Runtime Environment and the Java Card 2.2.1 Application Programming Interface.
2. The GlobalPlatform Card Specification version 2.1.1

MultiApp contains the following components (see Figure 2):

- **The *Native Layer*** that provides the basic card functionalities (memory management, I/O management and cryptographic libraries) with native interface with the dedicated IC. The cryptographic library includes TDES, RSA CRT (1024, 1536, 2048), hashing (SHA-1, SHA-256), OBKG (RSA), and RNG.
- **The *Java Card Runtime Environment***, which provides a secure framework for the execution of Java Card programs and data access management (firewall).
- **The *Java Card Virtual Machine***, which provides the secure interpretation of bytecodes.
- The ***API*** including the standard Java Card API, the JCF API (Biometry) and Gemalto proprietary API (SecureAPI, GemUtil, Mifare, CryptoTest).
- **The *Open Platform Card Manager***, which provides card, key and application management functions (contents and life-cycle) and security control.

The MultiApp platform provides the following services:

Remark: Points 2, 3 and 4 are services available in development environment phase and no available in operational environment (not part of the evaluation scope).

1. Initialization of the Card Manager and management of the card life cycle,
2. Secure installation of the application under Card Manager control,
3. Extradition services to allow several applications to share a dedicated security domain,
4. Deletion of applications under Card Manager control,
5. Secure operation of the applications through the API,
6. Card basic security services as follows:
   - Checking environmental operating conditions using information provided by the IC,
   - Checking life cycle consistency,
   - Ensuring the security of the PIN objects,
   - Generating random number,
   - Handling secure data object and backup mechanisms,
   - Managing memory content,

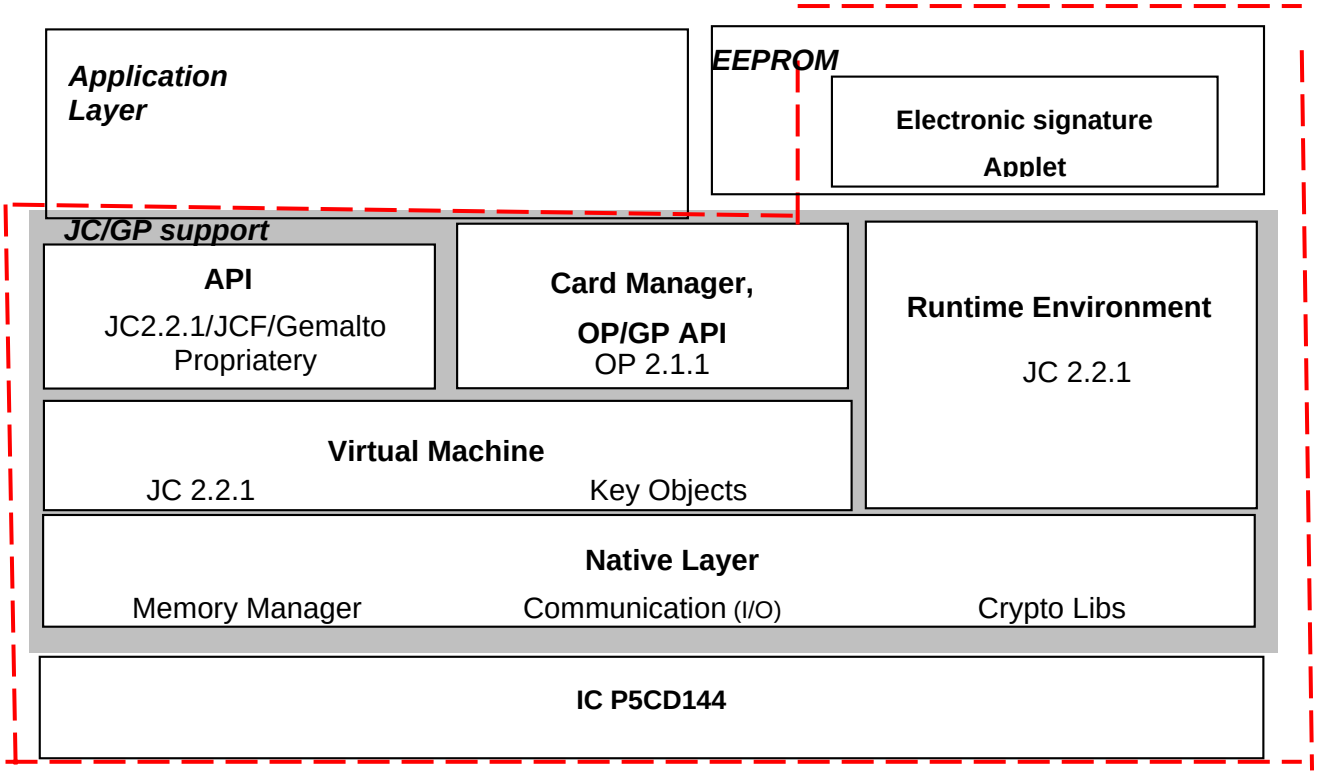


Figure 2 - *MultiApp platform architecture*

1.4.2 IAS ECC Applet description

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

Three Protection Profiles have been defined:

- The SSCD PP Type 1, which is a SCD/SVD generation component without signature creation and verification. The SCD generated on a SSCD Type 1 shall be exported to a SSCD Type 2 over a trusted channel [PP SSCD1].
- The SSCD PP for a TOE Type 2, which is a Signature creation and verification component [PP SSCD2]. This device imports the SCD from a SSCD Type 1
- The SSCD PP for a TOE Type 3, which is combination of the TOE Type 1 and Type 2 – i.e. Generation and Signature creation/verification component [PP SSCD3].

Terminology

In this document the terminology of [PP SSCD2] and [PP SSCD3] is used.

The SSCD Application uses public key encryption. The Signature Creation Data (SCD) is the private key and the Signature Verification Data (SVD) is the public key.

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.

SSCD Application provides the following functions necessary for devices involved in digital electronic signatures:

1. Generate the (SCD) and the correspondent (SVD), or Load the SCD,
2. Create qualified electronic signatures:

   (a) After allowing for the Data To Be Signed (DTBS) to be displayed correctly by an appropriate environment,

   (b) Using appropriate hash functions agreed according to [CWA-ALGO] suitable for qualified electronic signatures,

   (c) After appropriate authentication of the signatory by the TOE itself,

   (d) Using appropriate cryptographic signature function that employs appropriate cryptographic parameters agreed according to [CWA-ALGO].

The TOE implements all IT security functionalities, which are necessary to ensure the secrecy of the SCD. To prevent the unauthorized usage of the SSCD the TOE provides user authentication and access control. The TOE implements IT measures to support a trusted path to a trusted human interface device. Therefore, the TOE holds Signatory's Reference Authentication Data (RAD) that is used to verify the verification data provided by the user as Signatory's Verification Authentication Data (VAD).

The TOE is initialized by importing an SCD or by generating a pair of SCD and SVD. The SCD is protected so as to be solely used in the signature-creation process by the legitimate signatory during the validity of this SCD/SVD pair.

The TOE stores the SCD and may export the SVD. The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP).

When in usage phase, the TOE allows the creation of a new SCD/SVD pair. The previous SCD shall be destroyed before the creation of the new SCD/SVD pair.

The signatory uses a signature-creation system to create electronic signatures. The signature-creation device consists of the TOE.

The SCA presents the DTBS to the signatory and prepares the DTBS-representation that the signatory wishes to sign for performing the cryptographic function of the signature.

The TOE returns the digital electronic signature.

The TOE implements the SSCD of type 2 and type 3, and all functions concerning the SSCD to create electronic signatures in a secure way.

The Figure below shows the type 3 and type 2 TOE operations as defined in [PP SSCD2] & [PP SSCD3].

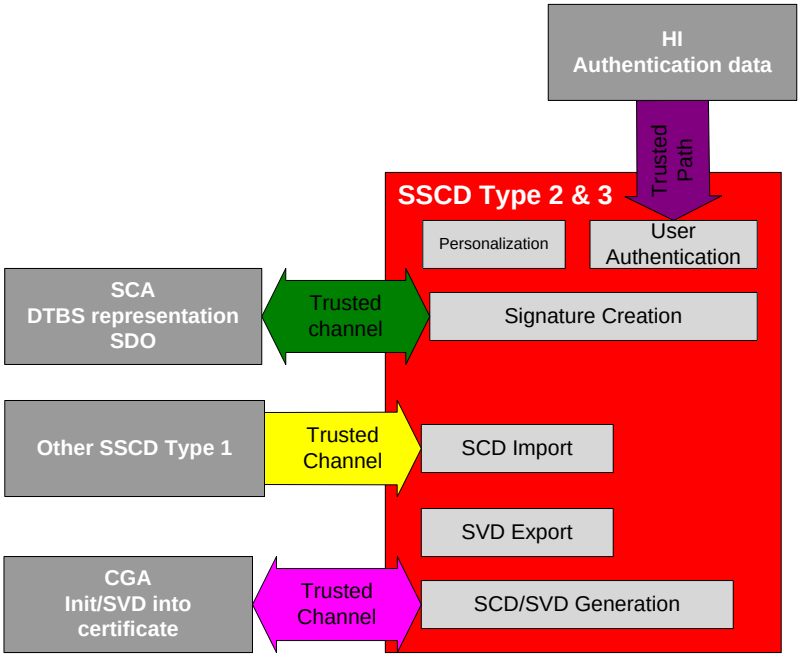


Figure 3 - Type 2 and Type 3 SSCD operations

1.4.3 TOE life-cycle

The product life cycle is described in Figure 4 - Product Life Cycle. Some remarks are added to explain this figure regarding Table 3. Smart Card Product Life Cycle.

This Product life cycle is called “wafer delivery”.

- The TOE is the product at the end of the phase 3 “IC manufacturing”.
- **Platform design**, **application design** and **EEPROM image design** correspond to the phase 1 “Smart card software development”.
- **Hardware design** corresponds to the phase 2 “IC development”.
- **Hardware fabrication** corresponds to the phase 3” IC manufacturing “,
- **IC packaging and testing c**orresponds to the phase 4.
- **Loading of application data**, **SCD/SVD import (type 2), and SVD export (for certificate)** are done in the phase 6 “Smart card personalization”.
- **SCD/SVD generation (type 3) and signature creation** correspond to the phase 7“Smart card end-usage”.
- **SSCD destruction** corresponds to the end of the phase 7.

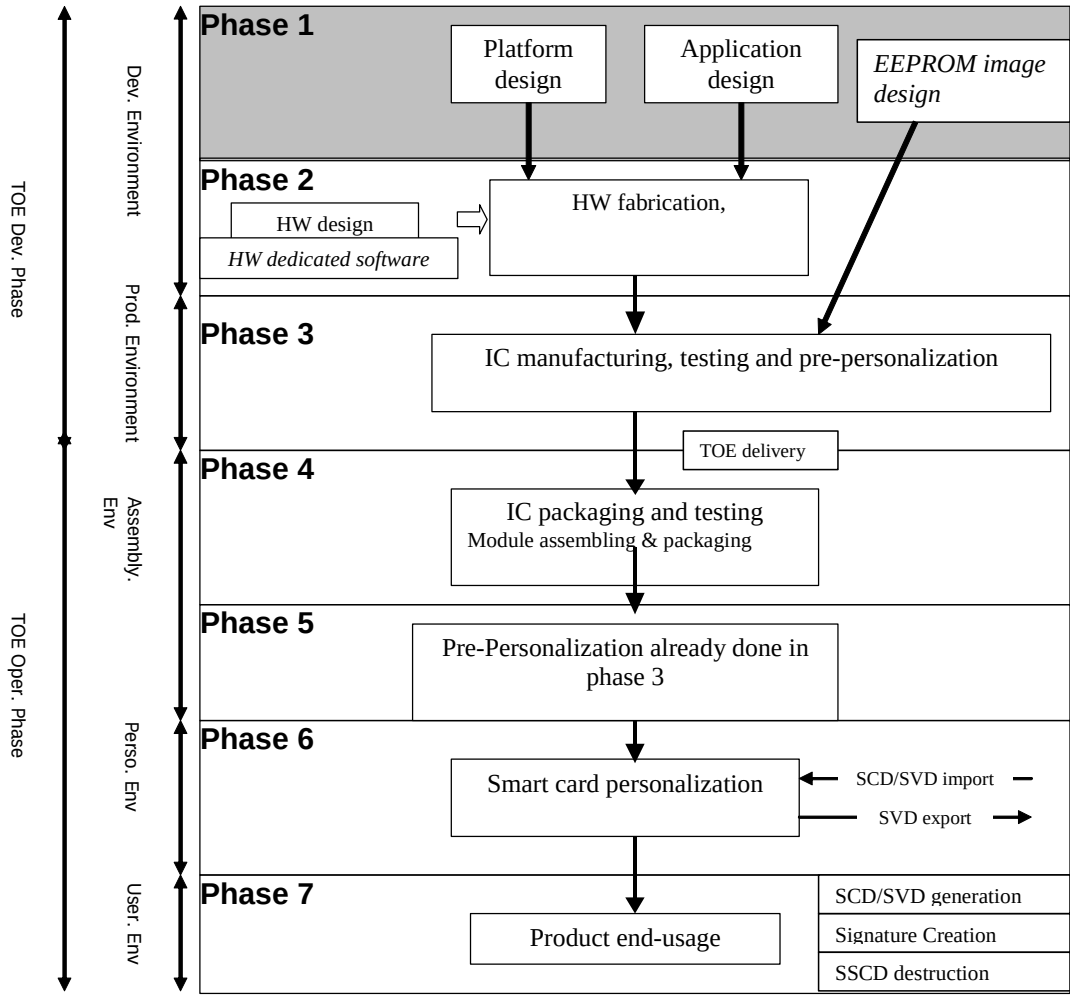


Figure 4 - Product Life Cycle "Wafer delivery"

The global security requirements of the TOE mandate to consider, during the development phase, the threats to security occurring in the other phases.

Therefore, this ST addresses the functions used in the phases 6 and 7 but developed during the phases 1 to 3. The limits of the evaluation process correspond to phases 1 to 3 including the TOE under development delivery from the party responsible of each phase to the parties responsible of the following phases. (Phase 4 will be done by a manufacturer selected by the customer. This phase is not in the development phase).

These different phases may be performed at different sites. This implies that procedures on the delivery process of the TOE must exist and be applied for every delivery within a phase or between phases. This includes any kind of delivery performed from phase 1 to 3 to subsequent phases, including:

- Intermediate delivery of the TOE or the TOE under construction within a phase,
- Delivery of the TOE or the TOE under construction from one phase to the next.

These procedures must be compliant with the security assurance requirements developed in TOE "Security Assurance Requirements".

1.4.3.1 TOE Phases

1.4.3.1.1 TOE Actors & roles

For the digital signature application, two roles have been identified, the Administrator and the Signatory.

1. The Administrator acts during the personalization phase (phase 6). He creates the Signatory's PIN and optionally imports the first SCD into the TOE.
2. The Signatory that owns the TOE is the End-User in the usage phase (phase 7). He can sign, destroy the SCD and generate a new SCD/SVD pair.

At the first usage of the TOE, the Signatory must change his PIN code before he is allowed to sign. A new PIN is also required each time a new SCD/SVD pair is generated.

1.4.3.1.2 Smart Card product life cycle

The Smart card product life cycle, as defined in [PP/BSI-0002], is split up into 7 phases where the following authorities are involved:

Phase 1	Smart card software development	**The smart card embedded software developer** is in charge of the smart card embedded software development and the specification of IC pre-personalization requirements.	
Phase 2	IC Development	**The IC designer** designs the integrated circuit, develops IC firmware if applicable, provides information, software or tools to the smart card software developer, and receives the software from the developer, through **trusted delivery and verification procedures**. From the IC design, IC firmware and smart card embedded software, he constructs the smart card IC database, necessary for the IC photo mask fabrication.	
Phase 3	IC manufacturing and testing	**The IC manufacturer** is responsible for producing the IC through three main steps: IC manufacturing, testing, and IC pre-personalization	
Phase 4	IC packaging and testing	**The IC packaging manufacturer** is responsible for the IC packaging and testing.	
Phase 5	Smart card product finishing process	**Nothing done in this specific "wafer delivery" life cycle process**	
Phase 6	Smart card personalization	**The Personalizer** is responsible for the smart card personalization and final tests.	**Administrator**
Phase 7	Smart card end-usage	**The smart card issuer** is responsible for the smart card product delivery to **the smart card end-user**, and for the end of life process.	**Signatory** **Administrator**

Table 3. Smart Card Product Life Cycle

1.4.4 TOE Environment

The TOE environment is defined as follow:

- For TOE development phase:
  - **Development environment** corresponding to the software developer environment (phase1), and the hardware fabrication environment (phase 2);
  - **Production environment** corresponding to the generation of the masked Integrated Circuit, the initialization of the JavaCard, the installation of the applet and the diversification of data required.

- For TOE operational phase
  - **Assembly environment** corresponding to module assembling and packaging (phase 4)
  - **Personalization environment** corresponding to personalization and testing the loading of TOE application data and the import of the SCD (phase 6), during which the card generates the signatures on behalf of the end user.
  - **User environment** corresponding to card usage (phase 7). End of life environment, during which the TOE is made inapt for the signature creation (end of the phase 7).

Phase 1	Software development (Multiapp, IAS ECC, softmask) Pre-personalization design	Gemalto Meudon
Phase 2	IC design Hardware fabrication	NXP
Phase 3	IC manufacturing & testing	NXP
Phase 4	IC packaging & testing Module assembling Module packaging	Manufacturer selected by Gemato customer
Phase 5	Pre-personalization	NXP during phase 3

1.4.4.1 Development phase

1.4.4.1.1 Software development ((Phase 1)

This environment is limited to GEMALTO Meudon site.

In order to ensure security, the environment in which the development takes place must be made secure with access control tracing entries. Furthermore, it is important that all authorized personnel feels involved and fully understands the importance and the rigid implementation of the defined security procedures.

The development begins with the TOE specification. All parties in contact with sensitive information are required to abide by Non-disclosure Agreement.

Design and development of the ES then follows. The engineers use a secure computer system (preventing unauthorized access) to make the conception, design, implementation and test performances.

To ensure security, access to development tools and products elements (PC, emulator, card reader, documentation, source code, etc…) is protected. The protection is based on measures for prevention and detection of unauthorized access. Two levels of protection are applied:

- Access control to GEMALTO Meudon office and sensitive areas.
- Access to development data through the use of a secure computer system to design, implement and test software.

Storage of sensitive documents, databases on tapes, diskettes, and printed circuit layout information are in appropriately locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

Testing, programming and deliveries of the TOE then take place. When these are done offsite, they must be transported and worked on in a secure environment with accountability and traceability of all (good and bad) products.

During the electronic transfer of sensitive data, procedures must be established to ensure that the data arrive, only at the destination and is not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies). It must also be ensured that transfer is done without modification or alteration.

1.4.4.1.2 Hardware fabrication (Phase 2)

This environment is limited to NXP sites.

The IC development environment is described in [IC-ST]. A transport key protects the IC delivery from Gemalto to NXP. We are only interested below in the software aspect of the TOE.

1.4.4.2 Production environment

1.4.4.2.1 IC manufacturing (Phase 3)

This environment is limited to NXP sites.

The IC manufacturing environment is described in [IC-ST].

1.4.4.2.2 IC Packaging (phase 4)

This environment can be GEMALTO site.

Regarding this specific product life cycle called “wafer delivery”, this phase is out of the TOE construction. And module assembling could be done by manufacturer selected by Gemalto customer.

Recommendation is that, access to fabrication site is physically protected. The protection is based on measures for prevention and detection of unauthorized access.

1.4.4.2.3 Pre-personalization: Card Initialization and applet installation (phase 5)

Regarding this specific product life cycle called “wafer delivery”, Phase 5 content will be included in phase 3 and done by IC NXP.

1.4.4.3 Personalization environment

This environment can be GEMALTO site.

Recommendation is that, access to personalization site is physically protected. The protection is based on measures for prevention and detection of unauthorized access.

Additional data may be loaded and the SCD may be imported. Then the TOE is issued to the Card Holder (Signatory).

1.4.4.4 User environment

At the end of phase 6, the Card Issuer delivers the Smart Card to the Card Holder.

Once delivered to the Card Holder (phase 7), the TOE can generate the SCD/SVD key pair. The TOE then exports the public part of the key to the Certification Authority for certification.

The TOE is owned by the Card Holder who cannot impose strict security rules. It is the responsibility of the TOE and of the signature protocols to ensure that the signature security requirements are met.

The signatory will generate the SCD/SVD keys pair.

The signatory will export the public key (SVD)

The signatory will have to present his PIN (VAD) before being allowed to create signature.

The end of life environment is corresponding to the physical destruction of the card.

1.4.5 The actors and roles

The actors can be divided in:

Developers

The IC designer and Dedicated Software (DS) developer designs the chip and its DS. For this TOE, it is NXP.

The Embedded Software developer designs the OS according to IC/DS specifications, the IAS ECC application and the softmask. For this TOE, it is GEMALTO.

Manufacturers

The IC manufacturer -or founder- designs the photomask, manufactures the IC with its DS and hardmask from the Product Developer. For this TOE, the founder is NXP.

The IC die bonding manufacturer is responsible for the die bonding the ICs provided by the founder. For this TOE, the IC die bonding manufacturer is GEMALTO is the manufacturer selected by GEMALTO customer.

Personalizer

The Smart Card Personalizer personalizes the card by loading the cardholder data as well as cryptographic keys and PINs. For this TOE, the personalizer is the Card Issuer.

At the end of this phase, no more applets may be loaded on the card (post-issuance is not allowed). The card is issued in OP_SECURED state.

Card Issuer, Administrator

The Card Issuer -short named “issuer”- is a National Administration. It issues cards to the citizens who are the “Card holders”. The Card Issuer has also the role of Administrator. Therefore, the Card Issuer is responsible for selecting and managing the personalization, for managing applets, for creating the Signatory’s PIN, for optionally importing the first SCD into the TOE, as well as for distribution and invalidation of the card.

End-user, Signatory

The Signatory is the End-user in the usage phase (phase 7) and owns the TOE. The card is personalized with his or her identification and secrets. The Signatory can sign, destroy the SCD and generate a new SCD/SVD pair.

The roles (administration and usage) are defined in the following tables.

Phase	Administrator	Environment
6 and 7	Card Issuer	Personalization and Usage Environment

Phase	User	Environment
7	Signatory	Usage Environment

During the delivery between phases the responsibility is transferred from the current phase administrator to the next phase administrator.

1.4.6 TOE intended usage

SCD import:

1. The SCA authenticates itself to the TOE.
2. The signatory authenticates to the TOE (see above).
3. The signatory requests the import of SCD from a SSCD Type 1 device.
4. The SCD is imported to the TOE.
5. The CGA generates the certificate for the corresponding SVD and sends it ot the TOE.

SCD/SVD Key generation in the final usage phase,

1. The SCA authenticates itself to the TOE.
2. The signatory enters his PIN code.
3. The signatory requests the generation of a SCD / SVD key pair
4. The SCD / SVD are generated in the TOE.
5. The SVD is sent to the CGA.
6. The CGA generates the certificate and sends it to the TOE.

Signature Creation in the final usage phase,

1. The SCA authenticates itself to the TOE.
2. The signatory enters his PIN code.
3. The signatory sends the DTBS to the TOE.
4. The TOE computes the Signature.
5. The TOE sends the Signature to the SCA.

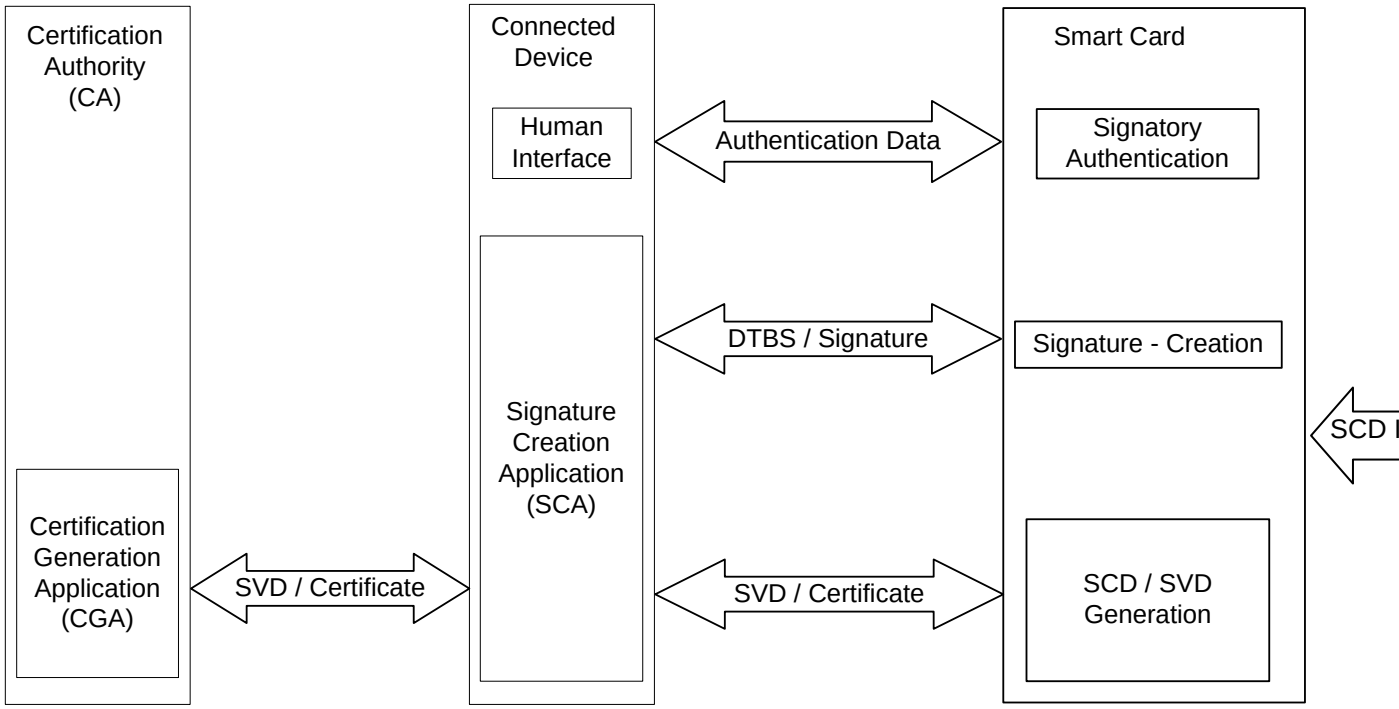


Figure 5 - TOE Usage

1.5 REFERENCES, GLOSSARY AND ABBREVIATIONS

1.5.1 External references

Reference	Title - Reference
[CCPART1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2006-09-001, version 3.1, September 2006 (conform to ISO 15408).
[CCPART2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional components CCMB-2007-09-002, version 3.1, September 2007 (conform to ISO 15408).
[CCPART3]	Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCMB-2007-09-003, version 3.1, September 2007 (conform to ISO 5408).
[CEM]	Common Methodology for Information Technology Security Evaluation CCMB-2007-09-004, version 3.1, September 2007.
[PP SSCD1]	Protection Profile Creation Device Type 1 Version 1.05 BSI-PP-0004-2002T- 03-04-2002
[PP SSCD2]	Protection Profile Creation Device Type 2 Version 1.04 BSI-PP-0005-2002T-03-04-2002
[PP SSCD3]	Protection Profile Creation Device Type 3 Version 1.05 BSI-PP-0006-2002T-03-04-2002
[PP/BSI-0002]	Smartcard IC Platform Protection Profile - BSI-PP-0002-2001; Version 1.0, July 2001
[DIRECTIVE]	DIRECTIVE 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures" DIRECTIVE 1999/93/EC
[E-Sign 1]	Application Interface for Smart Cards used as Secure Signature Creation Device CEN/ISSS WS/E-Sign Draft CWA Group K part 1 – Basic requirements. Version 1 Release 9 (17th September 2003)
[E-Sign 2]	Application Interface for Smart Cards used as Secure Signature Creation Device CEN/ISSS WS/E-Sign Draft CWA Group K part 2 – Additional services. Version 0 Release:19 (12th December 2003)
[IC-ST]	Security Target of P5CD144 (NXP) Microcontroller for Smart Cards. Version Rev. 1.3 —4 February 2008
[CC-COMP]	Composite product evaluation for Smart Card and similar devices – ISCI-WG1
[JC2.2.1]	Java Card 2.2.1 Virtual Machine - 2.2.1 - Oct 2003
[JCRE221]	Java CardTM Runtime Environment Specification version 2.2.1, Sun Microsystems, Inc, 2003.
[JCAPI221]	Java CardTM APIs specification version 2.2.1, Sun Microsystems, Inc, June 23, 2003.
[GP2.1.1]	Global Platform - Card specification v2.1.1 - 2.1.1 - March 2003

1.5.2 Glossary

CEN workshop agreement (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN). This Protection Profile (PP) represents Annex A to the CWA that has been developed by the European Electronic Signature Standardization Initiative (EESSI) CEN/ISSS electronic signature (E-SIGN) workshop, Area F on secure signature-creation devices (SSCD).
Certificate means an electronic attestation which links the SVD to a person and confirms the identity of that person. (defined in the Directive [1], article 2.9)
Certification generation application (CGA) means a collection of application elements which requests the SVD from the SSCD for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair by the SSCD, if the requested SVD has not been generated by the SSCD yet. The CGA verifies the authenticity of the SVD by means of (a) the SSCD proof of correspondence between SCD and SVD and (b) checking the sender and integrity of the received SVD.
Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. (defined in the Directive [1], article 2.11)
Data to be signed (DTBS) means the complete electronic data to be signed (including both user message and signature attributes).
Data to be signed representation (DTBS-representation) means the data sent by the SCA to the TOE for signing and is a hash-value of the DTBS or an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or the DTBS. The SCA indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.
Qualified certificate means a certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1]. (defined in the Directive [1], article 2.10)
Qualified electronic signature means an advanced signature which is based on a qualified certificate and which is created by a SSCD according to the Directive [1], article 5, and paragraph 1.
Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorized user.
Secure signature-creation device (SSCD) means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive [1]. (SSCD is defined in the Directive [1], article 2.5 and 2.6).
Signatory means a person who holds a SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. (defined in the Directive [1], article 2.3)
Signature attributes means additional information that is signed together with the user message.

Signature-creation application (SCA) means the application used to create an electronic signature, excluding the SSCD. I.e., the SCA is a collection of application elements 1. to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision, 2. to send a DTBS-representation to the TOE, if the signatory indicates by specific non-misinterpretable input or action the intend to sign, 3. to attach the qualified electronic signature generated by the TOE to the data or provides the qualified electronic signature as separate data.
Signature-creation data (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. (defined in the Directive [1], article 2.4)
Signature-creation system (SCS) means the overall system that creates an electronic signature. The signature-creation system consists of the SCA and the SSCD.
Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (defined in the Directive [1], article 2.7)
Signed data object (SDO) means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.
Sub-Referential. Consistent set of software components (Example: test scripts, specification documents,). A Sub-referential belongs to a Referential.
SSCD provision service means a service that prepares and provides a SSCD to subscribers.
Tip Revision. The latest revision of a line of development (the trunk or a branch)
User means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics.

1.5.3 Abbreviations

Abreviations	
AVA	Vulnerability Assessment
CC	Common Criteria
CSP	certificate-service-provider
DTBS	Data To Be Signed
IC	Integrated Circuit
OS	Operating System
RAD	Reference Authentication Data
SAR	Security Assurance Requirements
SCD	Signature Creation Data
SF	Security Function
SFR	Security functional requirements
SSCD	Secure Signature Creation Device
ST	Security Target

SVD	Signature Verification Data
TOE	Target Of Evaluation
TSF	TOE Security Functionality
VAD	Verification Authentication Data

2 CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIM

This Security Target is built with CC V.3.1

This ST is [CCPART2] extended.

This ST is [CCPART3] conformant.

The TOE includes Integrated Circuit certified with CC V2.3 EAL5+ ALC_DVS.2, AVA_MSU.3; AVA_VLA.4.This IC has its own ST [IC-ST]. The assets, threats, objectives, SFR and security functions specific to the IC are described in [IC-ST] and are not repeated in the current ST.

2.2 PP CLAIM, PACKAGE CLAIM

This ST claims a strict compliance with [PP SSCD2] and [PP SSCD3].

[IC-ST] refines the assets, threats, objectives and SFR of [PP/BSI-0002].

This TOE claims conformance to EAL4 augmented (+) with:

- ALC_DVS.2: Sufficiency of security measures.
- AVA_VAN.5: Advanced methodical vulnerability analysis

Equivalence between CC v2.3 EAL4 augmented (+) and CC v3.1 EAL4 augmented (+)

- ADV_IMP.2 (Development – Implementation of the FSP) in CC v2.3 is equivalent to ADV_IMP.1 in CC v3.1 managed by EAL4 (augmentation not required)
- ALC_DVS.2 (Sufficiency of security measures) augmentation is maintained in CC v3.1 EAL4 augmented
- AVA_MSU.3 (Analysis and testing for insecure states) this CC V3.1 assurance family moved in AGD families in CC3.1 managed by EAL4
- AVA_VLA.4 (Highly resistant) en CC v2.3 is equivalent to AVA_VAN.5 in CC v3.1, augmentation maintain in CC v3.1 EAL4 augmented

The strength level for the TOE security functional requirements is “SOF high” (Strength Of Functions high).

2.3 CONFORMANCE RATIONALE

This Security Target is built with CC V3.1 as referenced in External references.

This ST is conformant with [CCPART2] extended due to additional components as stated in Protection Profile [PP SSCD2], [PP SSCD3] and [PP/BSI-0002].

This ST is conformant with [CCPART3] augmented due to augmentation given in [PP SSCD2], [PP SSCD3] and [PP/BSI-0002].

[IC-ST] refines the assets, threats, objectives and SFR of [PP/BSI-0002] see BSI certificate and certification report.

The current ST refines the assets, threats, objectives and SFR of [PP SSCD2], [PP SSCD3] and [BSI PP].

2.4 PP REFINEMENTS

Refinements of [PP/BSI-0002] are described in [IC-ST] and are not repeated here.

The table below shows the functional requirements refined in PP and in ST.

Functional requirement	Refined in [PP SSCD2]	Refined in [PP SSCD3]	Refined in ST
FCS_CKM.1		_	X
FCS_CKM.4	_	_	X
FCS_COP.1	X	X	X
FDP_ACC.1	X	X	(X)
FDP_ACF.1	X	X	X
FDP_ETC.1	X	X	(X)
FDP_ITC.1	X	X	(X)
FDP_RIP.1	X	X	(X)
FDP_SDI.2	X	X	(X)
FDP_UCT.1	X		(X)
FDP_UIT.1	X	X	(X)
FIA_AFL.1	X	X	X
FIA_ATD.1	X	X	(X)
FIA_UAU.1	X	X	X
FIA_UID.1	X	X	X
FMT_MOF.1	X	X	(X)
FMT_MSA.1	X	X	(X)
FMT_MSA.2	NA	NA	NA
FMT_MSA.3	X	X	(X)
FMT_MTD.1	X	X	(X)
FMT_SMF.1			X
FMT_SMR.1	X	X	(X)
FPT_AMT.1[1]	_	_	
FPT_EMSEC.1	_	_	X
FPT_FLS.1	_	_	X
FPT_PHP.1	NA	NA	NA
FPT_PHP.3	_	_	X
FPT_TST.1	_	_	X
FTP_ITC.1	X	X	(X)
FTP_TRP.1	X	X	X

Table 4. PP functional requirements that have been refined

[1] This CC2.3 SFR is removed from CC3.1 SFR (no dependencies with FPT_TST in CC 3.1).

The functional requirements are both refined in the claimed PP and in this ST. This section demonstrates the compatibility of the refinements done in both documents.

-: No refinement

(X): no additional refinement has been made in the ST.

X: Refinement

NA: the functional requirement requires no refinement.

FCS_CKM.1: Cryptographic key generation

This functional requirement has been refined from [PP SSCD3] with a specific list of approved algorithms that gives the cryptographic key generation algorithms and key sizes used by the TOE.

FCS_CKM.4: Cryptographic key destruction

This functional requirement is refined from [PP SSCD2] and [PP SSCD3] with a description of the key destruction method used that follows [no specific standard].

FCS_COP.1: Cryptographic operation

This functional requirement partially refined in [PP SSCD2] and [PP SSCD3] has been completed in the ST with a specific list of cryptographic algorithms and key sizes that are used by the TOE. Furthermore, two iterations have been added, one for Hashing and one for the MAC computation.

FDP_ACC.1: Subset access control

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FDP_ACF.1: Security based access control functions

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3]. Additional refinement is done in the ST.

FDP_ETC.1: Export of user data without security attributes

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FDP_ITC.1: Import of user data without security attributes

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FDP_RIP.1: Subset residual information protection

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FDP_SDI.2: Stored data integrity monitoring and action

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FDP_UCT.1 Basic data exchange confidentiality

This functional requirement is already refined in [PP SSCD2] and no other refinement has been added in the ST.

FDP_UIT.1: Data exchange integrity

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FIA_AFL.1: Basic authentication failure handling

This functional requirement is partially refined in [PP SSCD2] and [PP SSCD3]. In the ST the number of authentication failures has been refined.

FIA_ATD.1: User attribute definition

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FIA_UAU.1: Timing of authentication

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3]. Additional refinement is done in the ST.

FIA_UID.1: Timing of identification

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3]. Additional refinement is done in the ST.

FMT_MOF.1: Management of security functions behavior

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FMT_MSA.1: Management of security attributes

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FMT_MSA.2: Secure security attributes

There is no refinement required for this security requirement.

FMT_MSA.3: Static attributes initialization

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FMT_MTD.1: Management of TSF data

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FMT_SMF.1: Specification of Management

This functional requirement is added to [PP SSCD2] and [PP SSCD3] in order to fulfill dependencies of CC.

FMT_SMR.1: Security roles

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FPT_EMSEC.1: TOE emanation

This functional requirement, extended from CC is not refined in [PP SSCD2] and [PP SSCD3]. It is entirely refined in the ST.

FPT_FLS.1: Failure with preservation of secure state

This functional requirement is not refined in [PP SSCD2] and [PP SSCD3] and is entirely refined in the ST.

FPT_PHP.1: Passive detection of physical attacks

There is no refinement required for this security requirement.

FPT_PHP.3: Resistance to physical attack

This functional requirement is not refined in [PP SSCD2] and [PP SSCD3] and is entirely refined in the ST.

FPT_TST.1: Testing

This functional requirement is not refined in [PP SSCD2] and [PP SSCD3] and is entirely refined in the ST.

FTP_ITC.1: Inter-TSF trusted channel

This functional requirement is already refined in [PP SSCD2] and [PP SSCD3] and no other refinement has been added in the ST.

FTP_TRP.1: Trusted path

This functional requirement is partly refined in [PP SSCD2] and [PP SSCD3]. Additional refinement is done in the ST.

2.5 PP ADDITIONS

The table below shows the functional requirements refined in PP and in ST.

	Addition in ST
Assets	-
Threats	-
Assumptions	-
Organizational Security Policies	-
Security objectives for the TOE	-
Security objectives for the operational environment	-
Security functional requirements	X
security assurance requirements	-
Security Requirements for the IT Environment	-

2.6 ASSURANCE REQUIREMENTS ADDITIONAL TO THE PP

There is no assurance requirement, which is not in [PP SSCD2], [PP SSCD3] or [PP/BSI-0002].

2.7 PP CLAIMS RATIONALE

This security target presents all PP SSCD Type 2 and Type 3 threats, assumptions, objectives, functional requirements and assurance measures.

The additional SFR **FMT_SMF.1.1** (for CCv3.1) does not introduce contradiction.

There are no additional assurance measures to PP SSCD Type 2 and Type 3. The strength of function claimed is high, and the claimed level is EAL4+ as required by the claimed PP. The IC security functions used by the platform also claim high level and the used IC is compliant to level EAL4+. Therefore, no inconsistency is introduced and the PP SSCD Type 2 & 3 claim is fulfilled.

3 SECURITY PROBLEM DEFINITION

This section describes the security aspects of the TOE environment and addresses the description of the assets to be protected, the threats, the organizational security policies and the assumptions.

Remark: This chapter “Security problem definition” in CC V3.1 is equivalent to “TOE security environment” in CC V2.3 and in PP SSCD [PP SSCD2], [PP SSCD3].

3.1 DIGITAL SIGNATURE ASSETS

The assets of the TOE are those defined in [PP SSCD2], [PP SSCD3] and [PP/BSI-0002].

This Security Target deals with the assets of [PP SSCD2] and [PP SSCD3]. The assets of [PP/BSI-0002] are studied in [IC-ST].

D.SCD	SCD: private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).
D.SVD	SVD: public key linked to the SCD and used to perform electronic signature verification (integrity of the SVD when it is exported must be maintained).
D.DTBS	DTBS and DTBS-representation: set of data or its representation which is intended to be signed (their integrity must be maintained)
D.VAD	VAD: PIN code data entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)
D.RAD	RAD: Reference PIN code authentication reference used to identify and authenticate the End User (Integrity and confidentiality of RAD must be maintained)
D.SSCD	Signature-creation function of the SSCD using the SCD: (The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures)
D.SIG	Electronic signature: (enforceability of electronic signatures must be assured).

3.2 DIGITAL SIGNATURE SUBJECTS

S.User	End user of the TOE which can be identified as S.Admin or S.Signatory.
S.Admin	User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions.
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.
S.OFFCARD	**Attacker**. A human or process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker is to access Application sensitive information. The attacker has a **high level potential attack** and **knows no secret.**

3.3 DIGITAL SIGNATURE THREATS

T.Hack_Phys	*Physical attacks through the TOE interfaces.* An attacker **S.OFFCARD** interacts with the TOE interfaces to exploit vulnerabilities to gain fraudulent access to the **Assets**.
T.SCD_Divulg	*Storing, copying, and releasing of signature-creation **D.SCD.*** An attacker **S.OFFCARD** can store, copy the SCD**D.SCD** outside the TOE. An attacker **S.OFFCARD** can release the SCD **D.SCD** during generation, storage and use for signature-creation in the TOE.
T.SCD_Derive	*Derive the signature-creation data **D.SCD.*** An attacker **S.OFFCARD** derives the SCD **D.SCD** from public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.
T.Sig_Forgery	*Forgery of electronic signature D.SIG.* An attacker **S.OFFCARD** forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.
T.Sig_Repud	*Repudiation of signatures **D.SIG.*** If an attacker **S.OFFCARD** can successfully threaten any of the assets, then the non repudiation of the electronic signature is compromised. The signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.
T.SVD_Forgery	*Forgery of the signature- verification data **D.SVD.*** An attacker **S.OFFCARD** forges the SVD **D.SVD** presented by the TOE. This result in loss of SVD integrity in the certificate of the signatory.
T.DTBS_Forgery	*Forgery of the DTBS-representation **D.DTBS.*** An attacker **S.OFFCARD** modifies the DTBS-representation **D.DTBS.** sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intends to sign.
T.SigF_Misuse	*Misuse of the Signature-Creation function of the TOE* An attacker **S.OFFCARD** misuses the signature-creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

3.4 DIGITAL SIGNATURE ASSUMPTIONS

This section defines assumptions related to the Digital Signature application as stated in PP SSCD and as stated in [PP/BSI-0002] for composite evaluation.

A.CGA	*Trustworthy certification-generation application* The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.
A.SCA	*Trustworthy signature-creation application* The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.
A.SCD_Generate (type2)	*Trustworthy SCD/SVD generation.* If a party other than the signatory generates the SCD/SVD-pair of a signatory, then (a) this party will use a SSCD for SCD/SVD-generation, (b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and (c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory. (d) The generation of the SCD/SVD is invoked by authorised users only (e) The SSCD Type1 ensures the authenticity of the SVD it has created and exported.

3.5 ORGANIZATIONAL SECURITY POLICIES

This section defines OSPs related to the Digital Signature application as stated in PP SSCD3.

P.CSP_Qcert	*Qualified certificate.* The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive [DIRECTIVE], i.e., inter alias the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.
P.Qsign	*Qualified electronic signatures.* The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate and is created by a SSCD.
P.Sigy_SSCD	*TOE as secure signature-creation device.* The TOE stores the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

4 SECURITY OBJECTIVES

The security objectives in this Security Target are those named and described in [PP SSCD2] and [PP SSCD3].

They cover the following aspects:

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

The security objectives stated in [PP/BSI-0002] can be found in [IC-ST].

4.1 SECURITY OBJECTIVES FOR THE TOE

OT.EMSEC_Design	*Provide physical emanations security* Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.
OT.Lifecycle_Security	*Lifecycle security.* The TOE shall detect flaws during the initialization, personalization and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-generation or re-import.
OT.SCD_Secrecy	*Secrecy of the signature-creation data.* The secrecy of the SCD (used for signature generation) is reasonably assured against attacks with a high attack potential.
OT.SCD_SVD_Corresp	*Correspondence between SVD and SCD.* The TOE shall ensure the correspondence between the SVD and the SCD. The TOE shall verify on demand the correspondence between the SCD stored in the TOE and the SVD if it has been sent to the TOE.
OT.SVD_Auth_TOE	*TOE ensures authenticity of SVD.* The *TOE* provides means to enable the CGA to verify the authenticity SVD that has been exported by that TOE.
OT.Tamper_ID	*Tamper detection.* The TOE shall provide system features that detect physical tampering of a system component, and use those features to limit security breaches.
OT.Tamper_Resistance	*Tamper resistance.* The **TOE** shall prevent or resist physical tampering with specified system devices and components.
OT.Init (type 3)	*Secure SCD SVD generation.* The **TOE** provides security features to ensure that the generation of the SCD and the SVD is invoked by authorized users only.
OT.SCD_Unique (type 3)	*Uniqueness of the signature-creation data* The TOE shall ensure the cryptographic quality of the SCD/ SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible low.
OT.SCD_Transfer (Type 2)	*Secure transfer of SCD between SSCD.* The TOE shall ensure the confidentiality of the SCD transferred between SSCDs.

OT.DTBS_Integrity_TOE	*Verification of the DTBS-representation integrity* The TOE shall verify that the DTBS-representation received from the SCA has not been altered in transit between the SCA and the TOE. The TOE itself shall ensure that the DTBS-representation is not altered by the TOE as well. Note, that this does not conflict with the signature-creation process where the DTBS itself could be hashed by the TOE.
OT.Sigy_SigF	*Signature generation function for the legitimate signatory only.* The TOE provides the signature generation function for the legitimate signatory only and protects SCD against the use of others. The TOE shall resist attacks with high attack potential.
OT.Sig_Secure	*Cryptographic security of the electronic signature* The TOE generates electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the electronic signatures. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section describes the security objectives for the environment.

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

Security Objectives	Description
OE.SCD_SVD_Corresp (type 2)	*Correspondence between SVD and SCD* The SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSVD Type1 shall prove the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.
OE.SCD_Transfer (type 2)	*Secure transfer of SCD between SSCD* The SSCD Type1 shall ensure the confidentiality of the SCD transferred to the TOE. The SSCD Type1 shall prevent the export of a SCD that already has been used for signature generation by the SSCD Type1. The SCD shall be deleted from the SSCD Type1 whenever it is exported into the TOE.
OE.SCD_Unique (type 2)	*Uniqueness of the signature-creation data* The SSCD Type1 shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible low.
OE.CGA_Qcert	*Generation of qualified certificates* The CGA generates qualified certificates which include inter alias the name of the signatory controlling the TOE, the SVD matching the SCD implemented in the TOE under sole control of the signatory, the advanced signature of the CSP.
OE.SVD_AUTH_CGA	*CGA verifies the authenticity of the SVD* The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between

	the SCD in the SSCD of the signatory and the SVD in the qualified certificate.
OE.HI_VAD	*Protection of the VAD* If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.
OE.SCA_Data_Intend	*Data intended to be signed* The SCA (a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE, (b) sends the DTBS-representation to the TOE and enables verification of the integrity of DTBS-representation by the TOE, (c) attaches the signature produced by the TOE to the data or provides it separately .

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 Threats

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

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

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

OT.SCD_Transfer and OE.SCD_Transfer ensure the confidentiality of the SCD transferred between SSCDs.

T.SCD_Derive (Derive the signature-creation data) deals with attacks on the SCD via public known data produced by the TOE. This threat is countered by OE.SCD_Unique that provides cryptographic secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographic secure electronic signatures.

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. This threat is in general addressed by OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.SCD_Transfer (Secure transfer of SCD between SSCD), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance) and OT.Lifecycle_Security (Lifecycle security), as follows.

OT.Sig_Secure ensures by means of robust encryption techniques that the signed data and the electronic signature are securely linked together. OE.SCA_Data_Intend provides that the methods used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation is appropriate for the cryptographic methods employed to generate the electronic signature. The combination of OE.CGA_QCert, OT.SCD_SVD_Corresp, OT.SVD_Auth_TOE, and OE.SVD_Auth_CGA provides the

integrity and authenticity of the SVD that is used by the signature verification process. OT.Sig_Secure, OT.SCD_Secrecy, OT.SCD_Transfer, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

T.Sig_Repud (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGA_QCert (Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signature creation data), OT.SCD_Transfer (Secure transfer of SCD between SSCD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed) and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity).

OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. OE.CGA_QCert and OT.SCD_SVD_Corresp ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OT.SCD_Unique provides that the signatory's SCD can practically occur just once. OT.Sig_Secure, OT.SCD_Transfer, OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD. OT.Sigy_SigF provides that only the signatory may use the TOE for signature generation. OT.Sig_Secure ensures by means of robust cryptographic techniques that valid electronic signatures may only be generated by employing the SCD corresponding to the SVD that is used for signature verification and only for the signed data. OE.SCA_Data_Intend and OT.DTBS_Integrity_TOE ensure that the TOE generates electronic signatures only for DTBS-representations that the signatory has decided to sign.

T.SVD_Forgery (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.SVD_Auth_TOE, which ensures that the TOE sends the SVD in a verifiable form to the CGA, as well as by OE.SVD_Auth_CGA, which provides verification of SVD authenticity by the CGA.

T.DTBS_Forgery (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which then does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by verifying the integrity of the DTBS-representation. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.SCA_Data_Indent.

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 SDO for data the signatory has not decided to sign, as required by the Directive [1], Annex III, paragraph 1, literal (c). This threat is addressed by the OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OE.SCA_Data_Intend (Data intended to be signed), OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity), and OE.HI_VAD (Protection of the VAD) as follows:

OT.Sigy_SigF ensures that the TOE provides the signature-generation function for the legitimate signatory only. OE.SCA_Data_Intend ensures that the SCA sends the DTBS-representation only for data the signatory intends to sign. The combination of OT.DTBS_Integrity_TOE and OE.SCA_Data_Intend counters the misuse of the signature generation function by means of manipulation of the channel between the SCA

and the TOE. If the SCA provides the human interface for the user authentication, OE.HI_VAD provides confidentiality and integrity of the VAD as needed by the authentication method employed.

4.3.2 Assumptions

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

A.SCA (Trustworthy signature-creation application) establishes the trustworthiness of the SCA according to the generation of DTBS-representation. This is addressed by OE.SCA_Data_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS-representation of the data that has 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.SCD_Generate Trustworthy SCD/SVD generation establishes a trustworthy SCD/SVD pair. This means that the SCD must be unique, objective met by OE.SCD_Unique, that the SCD and the SVD must correspond, objective met by OE.SCD_SVD_Corresp. The secrecy of the SCD must be maintained while it is transferred to the TOE before being deleted, OE.SCD_Transfer. (Remark: type 2 only).

4.3.2.1 Additional

4.3.3 Organisational security policies

P.CSP_QCert (CSP generates qualified certificates) establishes the qualified certificate for the signatory and provides that the SVD matches the SCD that is implemented in the SSCD under sole control of this signatory. On SCD/SVD correspondence, this OSP is addressed by OT.SCD_SVD_Corresp and OE.SCD_SVD_Corresp. In the IT environment, this OSP is addressed by OE.CGA_QCert for generation of qualified certificates by the CGA, respectively.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with qualified electronic signatures, as defined by the Directive [1], article 5, paragraph 1. Directive [1], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The requirement of qualified electronic signatures being based on qualified certificates is addressed by OE.CGA_QCert. OE.SCA_Data_Intend ensures that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. OT.Sig_Secure and OT.Sigy_SigF address the generation of advanced signatures by the TOE.

P.Sigy_SSCD (TOE as secure signature-creation device) establishes the TOE as secure signature-creation device of the signatory with practically unique SCD. This OSP is addressed by OT.Sigy_SigF that ensures that the SCD is under sole control of the signatory, and OE.SCD_Unique that ensures that the cryptographic quality of the SCD/SVD pair for the qualified electronic signature.

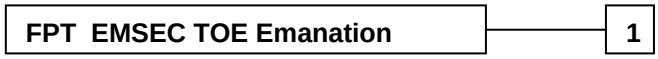
5 EXTENDED COMPONENTS DEFINITION

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE.

The TOE shall prevent attacks against the SCD 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.

FPT_EMSEC TOE Emanation
Family behavior
This family defines requirements to mitigate intelligible emanations.
Component leveling:



FPT_EMSEC.1 TOE Emanation has two constituents:

- FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMSEC.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

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

Audit: FPT_EMSEC.1
There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP.

FPT_EMSEC.1 TOE Emanation

- FPT_EMSEC.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].
- FPT_EMSEC.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

Hierarchical to: No other components.
Dependencies: No other components.

6 SECURITY REQUIREMENTS

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This chapter defines the security functional requirements for the TOE using functional requirements components as specified in [PP SSCD2] and [PP SSCD3].

[IC-ST] deals with the security functional requirements of [PP/BSI-0002].

6.1.1 Security functional requirements list

Identification	Description
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP	**User data protection**
FDP_ACC.1	Subset Access control
FDP_ACF.1	Security attributes based access control
FDP_ETC.1	Export of user data without security attributes
FDP_ITC.1	Import of User Data without security attributes
FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Basic data exchange integrity
FIA	**Identification and Authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT	**Security management**
FMT_MOF.1	Management of security function behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT	**Protection of the TOE Security function**

FPT_AMT.1	Abstract machine testing [2]
FPT_EMSEC.1	TOE Emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing
FTP	**Trusted path/Channel**
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	TOE Trusted path

Table 5. *IAS Classic security functional requirements list*

6.1.2 FCS – Cryptographic support

Remark: To be in the context of the French qualification RSA key shall use 1536 or 2048 bits.

6.1.2.1 FCS_CKM cryptographic key management

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1/RSA

FCS_CKM.1/RSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[RSA key generation]** and specified cryptographic key sizes **[1024, 1536 and 2048 bits]** that meet the following: **[no standard]**.

Application note: Type 3 only.

Remark: Link with Initialization SFP.

FCS_CKM.1.1/DH

FCS_CKM.1/DH	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Diffie-Helman 1024, 1536, 2048]** and specified cryptographic key sizes **[160 bits]** that meet the following: **no standard**.

Remark: DH authentication scheme see chapter 5.2.3 of [SRS];

FCS_CKM.1.1/ TDES

FCS_CKM.1/ TDES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[SRS chapter 7.1]** and specified cryptographic key sizes [**112 bits]** that meet the following: [**no standard].**

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4/SCD

[2] This CC2.3 SFR is removed from CC3.1 SFR (no dependencies with FPT_TST in CC 3.1).

FCS_CKM.4.1/SCD	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[overwrite the keys]** hat meets the following: **[no standard]**.

Application note (refined):
The cryptographic key SCD will be destroyed on demand of the Signatory.
The destruction of the SCD is mandatory before the SCD/SVD pair is re-imported into the TOE.(Type 2)
The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.(Type 3)

Remark: Link with SCD destruction SFP.

6.1.2.2 FCS_COP Cryptographic operation

FCS_COP.1 Cryptographic operation

FCS_COP.1/CORRESP

FCS_COP.1.1/ CORRESP	The TSF shall perform **[SCD / SVD correspondence proof]** in accordance with a specified cryptographic algorithm **[RSA key generation]** and cryptographic key sizes **[1024, 1536 and 2048 bits]** that meet the following: **[no standard]**.

Application note:

When the key pair is generated on card, the key generation process ensures that the public key corresponds to the private key.(Link with Initialization SFR)

When the SCD is input in the card, the card does not manage the SVD. The SVD or the corresponding certificate can be input in a standard file for future use by the application. But the card does not even know the content of the file. (Link with SVD transfer SFP)

FCS_COP.1/SIGNING

FCS_COP.1.1/ SIGNING	The TSF shall perform **[Digital signature-generation]** in accordance with a specified cryptographic algorithm **[RSA_SHA_PKCS#1]** and cryptographic key sizes **[1024, 1536 and 2048 bits]]** that meet the following: **[RSA PKCS #1, using SHA-1 or SHA-256]**.

Remark: Link with Signature creation SFP

FCS_COP.1/MAC

FCS_COP.1.1/ MAC	The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **ANSI X9.19 (Retail MAC)** and cryptographic key sizes **112 bits** that meet the following: **[SRS chapter 7.1]**

FCS_COP.1/TDES Cryptographic operation

FCS_COP.1.1/ TDES	The TSF shall perform [**TDES encryption and decryption]** in accordance with a specified cryptographic algorithm [**TDES-CBC]** and cryptographic key sizes [**112 bits for TDES 2 keys]** that meet the following: **[FIPS 46-3]**.

Application note:

The TOE can also encrypt and decrypt using DES algorithm with 56 bits key, but this is to be considered as a service. The DES algorithm is no longer considered as resistant to high level attacks.

FCS_COP.1/SHA Cryptographic operation

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

Application note:

This cryptographic operation does not use key.

FCS_COP.1/RNG Cryptographic operation

FCS_COP.1.1/ RNG	The TSF shall perform **Random Number Generation** in accordance with a specified cryptographic algorithm **Random Number Generator** and cryptographic key sizes **None** that meet the following: **ANSI X9.17 Appendix C.**

Application note:

This cryptographic operation does not use key.

6.1.3 FDP: User data protection

6.1.3.1 FDP_ACC Access Control policy

FDP_ACC.1 Subset access control

FDP_ACC.1/Initialization SFP

FDP_ACC.1.1/ Initialization SFP	The TSF shall enforce the **[Initialization SFP]** on [**Generation of SCD/SVD pair by User**].

Application note: Type 3 only.

FDP_ACC.1/SVD Transfer SFP

FDP_ACC.1.1/ Transfer SFP	**SVD**	The TSF shall enforce the [**SVD Transfer SFP**] on [**import and export of SVD by User**].

Application note:

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

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

FDP_ACC.1/SCD Import SFP

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

Application note: Type 2 only.

FDP_ACC.1/Personalization SFP

FDP_ACC.1.1/ Personalization SFP	The TSF shall enforce the [**Personalization SFP**] on [**Creation of RAD by Administrator**].

FDP_ACC.1/Signature-creation SFP

FDP_ACC.1.1/ Signature-creation SFP	The TSF shall enforce the [**Signature-creation SFP**] on [**Sending of DTBS-representation by SCA**] and [**Signing of DTBS-representation by Signatory**].

6.1.3.2 FDP_ACF access control function

FDP_ACF.1 Security attributes based access control

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

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

Refinement:

The rules for specific functions that implement access control SFP defined in FDP_ACC.1 are the following:

FDP_ACF.1/Initialization SFP

FDP_ACF.1.1/ Initialization SFP	The TSF shall enforce the [**Initialization SFP**] to objects based on [**General attribute group**] and [**Initialization attribute group**].
FDP_ACF.1.2/ Initialization SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "authorized" is allowed to generate SCD/SVD pair.
FDP_ACF.1.3/ Initialization SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**]
FDP_ACF.1.4/ Initialization SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "not

authorized" is not allowed to generate SCD/SVD pair.

Application note: Type 3 only.

FDP_ACF.1/SVD Transfer SFP

FDP_ACF.1.1/ SVD Transfer SFP	The TSF shall enforce the [**SVD Transfer SFP**] to objects based on [**General attribute group**]
FDP_ACF.1.2/ SVD Transfer SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute "role" set to "Administrator" or to "Signatory" is allowed to export SVD.
FDP_ACF.1.3/ SVD Transfer SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules [**none**].
FDP_ACF.1.4/ SVD Transfer SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: [**none**].

Application note:

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

FDP_ACF.1/SCD Import SFP

FDP_ACF.1.1/ Import SFP	**SCD**	The TSF shall enforce the [**SCD Import SFP**] to objects based on [**General attribute group**] and [**Initialization attribute group**].
FDP_ACF.1.2/ SCD Import SFP		The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorized" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".
FDP_ACF.1.3/ Import SFP	**SCD**	The TSF shall explicitly Authorize access of subjects to objects based on the following additional rules [none].
FDP_ACF.1.4/ Import SFP	**SCD**	The TSF shall explicitly deny access of subjects to objects based on the rule: The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorized" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes". The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorized" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no".

Application note: Type 2 only.

FDP_ACF.1/Personalization SFP

FDP_ACF.1.1/ Personalization SFP	The TSF shall enforce the [**Personalization SFP**] to objects based on [**General attribute group**]
FDP_ACF.1.2/ Personalization SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute "role" set to "Administrator" is allowed to create

	the RAD.
FDP_ACF.1.3/ Personalization SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules [**none**].
FDP_ACF.1.4/ Personalization SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: [**none**].

FDP_ACF.1/Signature Creation SFP

FDP_ACF.1.1/ Signature-creation SFP	The TSF shall enforce the [**Signature-creation SFP**] to objects based on [**General attribute group**] and [**Signature-creation attribute group**].
FDP_ACF.1.2/ Signature-creation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".
FDP_ACF.1.3/ Signature-creation SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4/ Signature-creation SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS which is not sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes". User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no".

6.1.3.3 FDP_ETC :Export to outside TSF control

FDP_ETC.1: Export of user data without security attributes

FDP_ETC.1/ SVD Transfer

FDP_ETC.1.1/ Transfer	**SVD**	The TSF shall enforce the [**SVD Transfer SFP**] when exporting user data, controlled under the SFP(s), outside of the TSC.
FDP_ETC.1.2/ Transfer	**SVD**	The TSF shall export the user data without the user data's associated security attributes.

Application note:

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

6.1.3.4 FDP_ITC Import From outside TSF control

FDP_ITC.1: Import of user data without security attributes

FDP_ITC.1/SCD

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

FDP_ITC.1.3/SCD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **[SCD shall be sent by an Authorized SSCD]**.

Application note:

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

Type 2 only.

Remark: Link with trusted channel SFP.

FDP_ITC.1/DTBS

FDP_ITC.1.1/DTBS	The TSF shall enforce the **[Signature-creation SFP]** when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2/DTBS	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3/DTBS	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **[DTBS-representation shall be sent by an Authorized SCA]**.

Application note:

A SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature and able to establish a trusted channel to the SSCD as required by FTP_ITC.1.3/SCA DTBS.

Remark: Link with trusted channel and authenticate SFP.

6.1.3.5 FDP_RIP Residual information protection

FDP_RIP.1: Subset residual information protection

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

Remark: Link with SCD destruction SFP.

6.1.3.6 FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2/Persistent

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

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

FDP_SDI.2.1/ Persistent	The TSF shall monitor user data stored within the TSC for [**integrity error**] on all objects, based on the following attributes: [**integrity checked persistent**

	stored data].
FDP_SDI.2.2/ Persistent	Upon detection of a data integrity error, the TSF shall: [**1. prohibit the use of the altered data** **2. inform the Signatory about integrity error**.]

FDP_SDI.2/DTBS

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

FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored within the TSC for **[integrity error**] on all objects, based on the following attributes: [**integrity checked stored data].**
FDP_SDI.2.2/DTBS	Upon detection of a data integrity error, the TSF shall: [**1. prohibit the use of the altered data** **2. inform the Signatory about integrity error.**]

Application note:

The DTBS-representation temporarily stored by TOE has the user data attribute "integrity checked stored data".

6.1.3.7 FDP_UCT Inter-TSF user data confidentiality transfer protection

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1/Receiver

FDP_UCT.1.1/Receiver	The TSF shall enforce the [**SCD Import SFP**] to be able to [**receive**] user data in a manner protected from unauthorized disclosure.

Application note: Type 2 only.

6.1.3.8 FDP_UIT Inter-TSF user data integrity transfer protection

FDP_UIT.1: Data exchange integrity

FDP_UIT.1/SVD Transfer

FDP_UIT.1.1/ Transfer	**SVD**	The TSF shall enforce the [**SVD Transfer SFP**] to be able to [**transmit**] user data in a manner protected from [**modification and insertion**] errors.
FDP_UIT.1.2/ Transfer	**SVD**	The TSF shall be able to determine on receipt of user data, whether [**modification and insertion]** has occurred.

FDP_UIT.1/TOE DTBS

FDP_UIT.1.1/TOE DTBS	The TSF shall enforce the [**Signature-creation SFP**] to be able to [**receive**] user data in a manner protected from [**modification, deletion and insertion**] errors.
FDP_UIT.1.2/TOE DTBS	The TSF shall be able to determine on receipt of user data, whether

[**modification, deletion and insertion**] has occurred.

Refinement: The mentioned user data is the DTBS-representation.

6.1.4 FIA: Identification and authentication

6.1.4.1 FIA_AFL Authentication failure

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1	The TSF shall detect when [**3(for 5-digit RAD) or 5 (for 6-digit RAD)**] **unsuccessful authentication attempts** occur related to [**consecutive failed authentication attempts**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been **[met]** the TSF shall **[block RAD**]

Refinement:

When the RAD is blocked, any attempt of authentication fails.

Remark: Link with Authenticate SFP.

6.1.4.2 FIA_ATD User attribute definition

FIA_ATD.1User attributes definition

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users [**RAD**]

6.1.4.3 FIA_UAU User authentication

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1	The TSF shall allow **1 [Identification of the user by means of TSF required by FIA_UID.1]** **2 [Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP_ITC.1/SCD import]** **3 [Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE]** **4 [Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:

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

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.

Dependencies: FIA_UID.1 Timing of identification.

6.1.4.4 FIA_UID User Identification

FIA_UID.1Timing of identification

FIA_UID.1.1	The TSF shall allow **1 [Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP_ITC.1/SCD import]** **2 [Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE]** **3 [Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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

6.1.5 FMT: Security management

6.1.5.1 FMT_MOF Management of functions in TSF

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1	The TSF shall restrict the ability to [**enable**] the [**signature-creation function**] to [**Signatory**].

6.1.5.2 FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes

FMT_MSA.1/Administrator

FMT_MSA.1.1/ Administrator	The TSF shall enforce the [**Initialization SFP**] and [**SCD Import SFP**] to restrict the ability to [**modify**] the security attributes [**SCD / SVD management and secure SCD import allowed**] to [**Administrator**].

Application note:

The SCD Import SFP enforcing comes from Type 2.

The Initialisation SFP enforcing comes from Type 3.

FMT_MSA.1/Signatory

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

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for **[All security attributes (see FDP_ACF.1)]**

FMT_MSA.3 Static attribute initialization

FMT_MSA.3/Type 2

FMT_MSA.3.1/Type 2 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.

Refinement

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

FMT_MSA.3.2/Type 2 The TSF shall allow the [**Administrator**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/Type 3

FMT_MSA.3.1/Type 3 The TSF shall enforce the [**Initialization SFP**] and [**Signature-creation SFP**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

Refinement

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

FMT_MSA.3.2/Type 3 The TSF shall allow the [**Administrator**] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.3 FMT_MTD Management of TSF data

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [**modify**] the [**RAD**] to [**Signatory**].

Note: RAD being the PIN code, RAD and VAD are the same data.

6.1.5.4 FMT_SMF Specification of Management Functions

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following functions [**Identification and authentication management]**.

Additional SFR

6.1.5.5 FMT_SMR Security management roles

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [**Administrator**] and [**Signatory**].
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6 FPT: Protection of the TSF

6.1.6.1 FPT_EMSEC TOE Emanation

FPT_EMSEC.1.1 TOE Emanation

FPT_EMSEC.1.1 The TOE shall not emit [**Side channel current**] in excess of [**State of the art limits**] enabling access to [**RAD and SCD**].

Notes:

This SFR is an extension to [CCPART 2].

State of the art limits are the limits currently expected for IC meeting EAL4+ level of security.

FPT_EMSEC.1.2 The TSF shall ensure [**all users**] are unable to use the following interface [**external contacts**] emanations to gain access to [**RAD and SCD**].

Notes:

This SFR is an extension to [CCPART 2].

State of the art limits are the limits currently expected for IC meeting EAL4+ level of security.

Remark: Link with Protection SFP.

6.1.6.2 FPT_FLS Failure secure

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**power shortage, over and under voltage, over and under clock frequency, over and under temperature, integrity problems**, **unexpected abortion of the execution of the TSF due to external events.**].

Remark: Link with Protection SFP.

6.1.6.3 FPT_PHP TSF physical Protection

FPT_PHP.1 Passive detection of physical attack

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

FPT_PHP.3.1	The TSF shall resist [**voltage, clock frequency and temperature out of bounds as well as penetration attacks**] to the **[integrated circuit**] by responding automatically such that the TSP is not violated

Remark: Link with Protection SFP.

6.1.6.4 FPT_TST TSF self test

FPT_TST.1 TSF testing

FPT_TST.1.1	The TSF shall run a suite of self-tests [**during initial start-up]** 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 stored TSF executable code.

Remark: Link with Protection SFP.

6.1.7 FTP: Trusted Path / Channel

6.1.7.1 FTP_ITC Inter-TSF trusted channel

FTP_ITC.1 Inter-TSF trusted Channel

FTP_ITC.1/SCD import

FTP_ITC.1.1/SCD import	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/SCD import	The TSF shall permit **[another trusted IT product]** to initiate communication via the trusted channel.
FTP_ITC.1.3/SCD import	The TSF shall initiate communication via the trusted channel for [**SCD import**]

Refinement: The mentioned remote trusted IT product is a SSCD of type 1.

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

Remark: Link with SCD import SFP.

FTP_ITC.1/SVD Transfer

FTP_ITC.1.1/SVD Transfer	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/SVD Transfer	The TSF shall permit **[another trusted IT product]** to initiate communication via the trusted channel.
FTP_ITC.1.3/SVD Transfer	The TSF shall initiate communication via the trusted channel for [**SVD Transfer]**

Refinement: The mentioned remote trusted IT product is a CGA or the SCA application that will transmit the SVD to the CGA.

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

Remark: Link with SVD transfer SFP.

FTP_ITC.1/ DTBS import

FTP_ITC.1.1/DTBS import	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/DTBS import	The TSF shall permit **[another trusted IT product]** to initiate communication via the trusted channel.
FTP_ITC.1.3/DTBS import	The TSF shall initiate communication via the trusted channel for [**signing DTBS-representation**]

Refinement: The mentioned remote trusted IT product is a SCA.

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

Remark: Link with Signature creation SFP.

6.1.7.2 FTP_TRP Trusted path

FTP_TRP.1 Trusted path

FTP_TRP.1.1	The TSF shall provide a communication path between itself and [**local**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **[modification, disclosure**].
FTP_TRP.1.2	The TSF shall permit [**local users**] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [**initial user authentication**][**no other service**].

Application note:

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

6.2 SECURITY ASSURANCE REQUIREMENTS

The TOE security assurance requirements define the assurance requirements for the TOE using only assurance components drawn from [CCPART3].

The assurance level is **EAL4** augmented on:

- ALC_DVS.2: Sufficiency of security measures.
- AVA_VAN.5: Advanced methodical vulnerability analysis

6.2.1 TOE security assurance requirements list

Table below shows equivalence between SAR in CC V2.3 and SAR CC V3.1.

CC V3.1 will be followed on this part.

Assurance class	Assurance Family CC2.x	Assurance Family CC3.1
Configuration Management	ACM_AUT	--
	ACM_CAP	ALC_CMC
	ACM_SCP	ALC_CMS
Delivery and operation	ADO_DEL	ALC_DEL partially AGD_PRE [1.1C]
	ADO_IGS	installation: AGD_PRE [1.2C] start-up: part of ADV_ARC [1.3C]
Development	ADV_LLD	ADV_TDS partially ADV_ARC [1.2C, 1.4C, 1.5C]
	ADV_FSP	ADV_FSP
	ADV_IMP	ADV_IMP
	ADV_HLD	ADV_TDS
Guidance documents	AGD_USR	AGD_OPE
	AGD_ADM	AGD_OPE

Assurance class	Assurance Family CC2.x	Assurance Family CC3.1
Life-cycle support	-- (ACM_CAP)	ALC_CMC
	-- (ACM_SCP)	ALC_CMS
	-- (ADO_DEL)	ALC_DEL
	ALC_DVC	ALC_DVS
	ALC_LCD	ALC_LCD
	ALC_TAT	ALC_TAT
Security Target evaluation	ASE	ASE
Tests	ATE_COV	ATE_COV
	ATE_DPT	ATE_DPT
	ATE_FUN	ATE_FUN
	ATE_IND	ATE_IND
Vulnerability assessment	AVA_CCA	AVA_VAN
	AVA_VLA	AVA_VAN
	AVA_SOF	AVA_VAN
	AVA_MSU	AGD_OPE [1.5C – 1.8C] AGD_PRE.1.2C (WU AGD_PRE.1-4) AGD_PRE.1.2E

Table 6. SAR CC V2.3 versus CC V3.1

Identification	**Description**
ADV	**Development**
ADV_ARC.1	Security architecture description

ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation representation of the TSF
ADV_TDS.3	Basic modular design
AGD	**Guidance documents**
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC	**Life cycle support**
ALC_CMC.4	Production support, acceptance procedures and automation
ALC_ CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE	**Tests**
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing : Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA	**Vulnerability assessment**
AVA_VAN.5	Methodical vulnerability analysis,

Table 7. TOE security assurance requirements list

7 TOE SUMMARY SPECIFICATION

The security functions provided by the IC are described in [IC-ST]. The TOE Security Functionalities are described below.

7.1 TOE SECURITY FUNCTIONALITIES PROVIDED BY PLATFORM

7.1.1 TSF_CARD_EMANATION: Emanation protection

This security functionality protects the electronic signature application data RAD and SCD against snooping. The security functionality ensures that:

- The TOE shall not emit electromagnetic radiation in excess of unintelligible emission enabling access to RAD and SCD.
- The TOE shall ensure that the attacker S.OFFCARD is not able to use I/O, VCC or Ground interface to gain access to RAD and SCD.

This security function is supported by the IC security function F.LOG: Logical Protection (see [IC-ST]).

7.1.2 TSF_CARD_PROTECT: Card operation protection

This security functionality ensures the protection of the TSF and supports the following operations.

- Analyze potential violation on the card life-cycle inconsistency, the PIN and keys integrity error, the illegal access to Java objects, and the unavailability of resources.
- Take action upon violation detection: reset the card, block the action, terminate or mute the card.
- Check start-up security conditions: the consistency of life-cycle, the integrity of specific data area.
- Check operating conditions periodically by listening the IC sensors.
- Resist to physical attacks (such as out-of-bound voltage, clock frequency and temperature, etc)

In case of error detections this function returns an error or an exception and takes appropriate shield action. If during the TSF execution an unexpected error or an abortion occurs, a secure state will be preserved by resetting security attributes to secure values and if necessary recover the persistently stored data to a secure consistent state.

This security function ensures the atomicity of Java objects update in EEPROM:

- The content of the data that are modified within a transaction is copied in the transaction dedicated EEPROM area. The TSF manages an optimistic backup: the optimistic backup mechanism includes a backup of the previous data value at first data modification, and previous value restoring at abort.
- Commit operation closes the transaction, and de-activates the dedicated transaction area.
- Rollback operation restores the original values of the objects (modified during the transaction) and de-activates the dedicated transaction area.
- The security function ensures that the EEPROM containing sensitive data is in a consistent state whatever the time when EEPROM programming sequence stops, either during copying, invalidating, restoring data to or from the backup dedicated EEPROM area or updating sensitive data in EEPROM.

This TSF is supported by the IC security function F.PHY: Protection against Physical Manipulation (see [IC-ST]).

7.2 TOE SECURITY FUNCTIONALITIES PROVIDED BY IAS ECC APPLET

7.2.1 TSF_ AUTHENTICATION: Authentication management

This security functionality manages the authentication mechanisms such as:

- Authentication operations for role management (i.e. PIN verification)

– Authentication operations for secure channel management (i.e. mutual authentication with symmetric and asymmetric schemes).

This security function:

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

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

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

7.2.2 TSF_CRYPTO: Cryptography management

This security functionality manages the cryptographic operations of the electronic signature application:

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

Cryptographic algorithms TDES, RSA and RNG and provided by the platform and ensures that D.SCD information is made unavailable after use (key destruction).

- TDES algorithm only support 112-bit key
- RSA algorithm supports 1024, 1536, 2048 bits keys. The RSA algorithm is SW and does not use the IC cryptographic library, only the IC cryptographic co-processor is used. The platform supports CRT RSA.
- Random generator uses the certified Hardware Random Generator that fulfils the requirements of AIS31 (see [IC-ST]).
- SHA-1 and SHA-256 algorithms

This security function controls all the operations relative to the card keys management (provided also by the platform)

- Key generation: The TOE provides the following:
  RSA key generation manages 1024, 1536, 2048 bits long keys. The RSA key generation is SW and does not use the IC cryptographic library.
  The TDES key generation (for session keys) uses the random generator.
- Key destruction: the TOE provides a specified cryptographic key destruction method that makes Key unavailable.

This security functionality ensures the confidentiality of keys during manipulation and ensures the de-allocation of memory after use.
This security functionality is supported by the IC security function F.RNG (Random Generator), F.HW_DES (Triple-DES Co-processor), (see [IC-ST]).

7.2.3 TSF_INTEGRITY: Integrity monitoring

This security functionality monitors the integrity of sensitive user data and the integrity of the DTBS. The integrity of persistently stored data such as D.SCD, D.RAD and D.SVD is monitored using the platform features.
In case of integrity error this TSF will

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

This TSF also monitors the integrity of the access conditions of created data objects and also ensures that no residual information is available after a PIN update or clearance.

7.2.4 TSF_MANAGEMENT: operation management and access control

This security functionality provides application operation management and access control.

Operation management

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

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

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

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

Access control

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

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

This security functionality provides access control to data objects.

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

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

7.2.5 TSF_SECURE_MESSAGING: secure messaging management

This security functionality ensures the integrity and the confidentiality of exchanged user data.

This security functionality ensures that the TSF is able to

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

This security functionality manages four modes of secure channel during the personalization phase

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

During the application personalization phase secure messaging provided by the platform is used. This ensures the integrity and/or the confidentiality of command/message transmission in a secure channel. The integrity is achieved by adding a message authentication code to the message. The confidentiality is achieved by APDU message data field encryption. These features are used in accordance with the security mode applied to the secure channel.