IAS Classic V3 on MultiApp ID V2.1

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

TABLE OF CONTENTS

FIGURES

TABLES

1 REFERENCE DOCUMENTS

1.1 EXTERNAL REFERENCES [ER]

[CC]	Common Criteria references
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2009-07-001, version 3.1 rev 3, July 2009
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2009-07-002, version 3.1 rev 3, July 2009
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2009-07-003, version 3.1 rev 3, July 2009
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology, CCMB-2009-07-004, version 3.1 rev 3, July 2009
[CCDB]	Common Criteria mandatory technical document – Composite product evaluation for smart cards and similar devices, CCDB-2007-09-001, Version 1.0 Revision 1, September 2007.
[PP]	**Protection profiles**
[PP/0035]	Security IC platform protection profile, version 1.0, 15th June 2007. Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035.
[PP-JCS-Open]	Java Card System Protection Profile – Open Configuration ANSSI-PP-2010-03, Version 2.6, April 19th 2010
[DIRECTIVE]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures
[PP-SSCD /T1]	Protection Profile – Secure Signature-Creation Device Type 1 BSI-PP-0004-2002, Version 1.05, April 3rd 2002
[PP-SSCD /T2]	Protection Profile – Secure Signature-Creation Device Type 2 BSI-PP-0005-2002, Version 1.04, April 3rd 2002
[PP-SSCD /T3]	Protection Profile – Secure Signature-Creation Device Type 3 BSI-PP-0006-2002, Version 1.05, April 3rd 2002
[NXP]	**NXP references**
[ST-P5CC081]	NXP Secure Smart Card Controllers P5CD016/021/041V1A and P5Cx081V1A - Security Target Lite — Rev. 1.3 — 21 September 2009
[ST-P5CC145]	NXP Secure Smart Card Controllers P5Cx128V0A / P5Cx145V0A, MSO – Security Target Lite – Rev 1.6 – 07 June 2010
[CR-P5CC081]	Certification Report for NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A, each with IC dedicated software BSI-DSZ-CC-0555-2009, November 10th 2009
[CR-P5CC145]	Certification Report for NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software BSI-DSZ-CC-0645-2010, July 23rd 2010
[ISO]	**ISO references**
[ISO7816]	Identification cards – Integrated circuit(s) cards with contacts - Books 1 to 9
[JCS]	**Javacard references**
[JCRE222]	Java Card 2.2.2 Runtime Environment (JCRE) Specification – 15 March 2006 - Published by Sun Microsystems, Inc.
[JCVM222]	Java Card 2.2.2 Virtual Machine (JCVM) Specification – 15 March 2006 - Published by Sun Microsystems, Inc.

[JCAPI222]	Java Card 2.2.2 Application Programming Interface - March 2006 - Published by Sun Microsystems, Inc.
[GP]	**Global Platform references**
[GP211]	Global Platform Card Specification v 2.1.1 - March 2003

1.2 INTERNAL REFERENCES [IR]

[AGD]	**MultiApp ID V2.1 Software – Guidance documentation**
[AGD_TopLev]	MultiApp ID V2.1 Software – AGD top-level document – IAS Classic V3 Application Ref: R0A21037_036_CCD_AGD-IASClassic

2 ACRONYMS & GLOSSARY

2.1 ACRONYMS

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

2.2 GLOSSARY

The 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]
Administrator user who performs TOE initialization, TOE personalization, or other TOE administrative functions
Advanced electronic signature digital signature which meets specific requirements in **The Directive: 2.2** Note: according to **The Directive** a digital signature qualifies as an advanced electronic signature if it: • is uniquely linked to the signatory; • is capable of identifying the signatory; • is created using means that the signatory can maintain under his sole control, and • is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Authentication data information used to verify the claimed identity of a user
Certificate digital signature used as electronic attestation binding signature-verification data to a person confirming the

identity of that person as legitimate signer (**The Directive: 2.9**)
Certificate info information associated with an SCD/SVD pair that may be stored in a secure signature creation device NOTE 1: Certificate info is either • a signer's public key certificate or, • one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values. NOTE 2: Certificate info may contain information to allow the user to distinguish between several certificates.
Certificate-generation application (CGA) collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate
Certification service provider (CSP) entity that issues certificates or provides other services related to electronic signatures (**The Directive: 2.11**)
Data to be signed (DTBS) all of the electronic data to be signed including a user message and signature attributes
Data to be signed or its unique representation (DTBS/R) data received by a secure signature creation device as input in a single signature-creation operation NOTE: DTBS/R is either • a hash-value of the data to be signed (DTBS), or • an intermediate hash-value of a first part of the DTBS complemented with a remaining part of the DTBS, or • the DTBS.
Legitimate user user of a secure signature creation device who gains possession of it from an SSCD-provisioning service provider and who can be authenticated by the SSCD as its signatory
Qualified certificate public key certificate that meets the requirements laid down in Annex I and that is provided by a CSP that fulfils the requirements laid down in **Annex II** (**The Directive: 2.10**)
Qualified electronic signature advanced electronic signature that has been created with an SSCD with a key with a qualified certificate (**The Directive: 5.1**)
Reference authentication data (RAD) data persistently stored by the TOE to authenticate a user as authorized for a particular role by cognition or by data derived from a user's biometric characteristics
Secure signature-creation device (SSCD) personalized device that meets the requirements laid down in **Annex** III by being evaluated according to a security target conforming to a PP in this series of European standards (**The Directive: 2.5** and **2.6**)
Signatory legitimate user of an SSCD associated with it in the certificate of the signature-verification data and who is authorized by the SSCD to operate the signature-creation function (**The Directive**: **2.3**)
Signature attributes additional information that is signed together with a user message
Signature-creation application (SCA) application complementing an SSCD with a user interface with the purpose to create an electronic signature Note: A signature creation application is software consisting of a collection of application components configured to: • present the data to be signed (DTBS) for review by the signatory, • obtain prior to the signature process a decision by the signatory, • if the signatory indicates by specific unambiguous input or action its intent to sign send a DTBS/R to the TOE • process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.
Signature-creation data (SCD) private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature (**The Directive: 2.4**)
Signature-creation system (SCS) complete system that creates an electronic signature consisting of an SCA and an SSCD
Signature-verification data (SVD) public cryptographic key that can be used to verify an electronic signature (**The Directive: 2.7**)
SSCD-provisioning service service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD
User entity (human user or external IT entity) outside the TOE that interacts with the TOE
User Message data determined by the signatory as the correct input for signing

Verification authentication data (VAD) data provided as input to a secure signature creation device for authentication by cognition or by data derived from a user's biometric characteristics

3 SECURITY TARGET INTRODUCTION

3.1 SECURITY TARGET IDENTIFICATION

Title:	IAS Classic V3 on MultiApp ID V2.1: Security Target, public version
Version:	1.1
Author:	Gemalto
Reference:	R0A21037_012_CCD_ASE-IASClassic
Publication date:	23/08/2012

3.2 TOE IDENTIFICATION

Product:	MultiApp ID V2.1 smartcard
TOE name:	IAS Classic V3 part of the MultiApp ID V2.1 smartcard software
TOE version:	MPH117 (Mask reference on P5CC081 security controller)
	MPH119 (Mask reference on P5CC145 security controller)
TOE documentation:	Guidance [AGD]
TOE hardware part:	P5CC081 security controller
	P5CC145 security controller
Developer:	Gemalto

3.3 TOE OVERVIEW

The MultiApp ID V2.1 product is a smartcard addressing the identity market. Built upon an opened javacard[1] platform, the smartcard application software implements identification, authentication and signature (IAS) services, as well as secure data storage and biometry features.

These services are enabled through the personalization of one or several corresponding applets:

- **IAS XL**: digital signature application compatible with IAS ECC v1.01 specification defined by Gixel (French smartcard industry association)
- **IAS Classic V3**: digital signature application with RSA up to 2048 and SHA256
- **MPCOS**: secure data storage 3DES based and PIN protection
- **MOCA server**: offers a match on card services to applications
- **MOCA client**: match on card application using MOCA server
- **Crypto Manager**: additional Match on Card application from Precise Biometrics Company.

Additionally, the two following applications may be embedded in the MultiApp V2.1 smartcard:

- **Custom EMV CAP**: Custom implementation of the MCHIP4 Lite applet used in the banking business, and containing only features used to generate the data necessary for CAP token computation.

[1] The Java Card technology combines a subset of the Java programming language with a runtime environment optimized for smart cards and similar small-memory embedded devices [JCVM222]. The Java Card platform is a smart card platform enabled with Java Card technology (also called a “Java card”). This technology allows for multiple applications to run on a single card and provides facilities for secure interoperability of applications. Applications for the Java Card platform (“Java Card applications”) are called applets.

- **ZZZS HIC/HPC**: Applet used in Slovenian health care cards. HIC stands for the patient card whereas HPC is the professional one. HIC/HPC specificities are activated through applet install parameters.

The MultiApp ID V2.1 product is a “contact-only” smartcard compliant with [ISO7816], and supporting T=0 and T=1 communication protocols.

For the present ST, the Target of Evaluation (TOE) is the IAS Classic V3 applet and the underlying platform which supports its functionality. Therefore, the TOE boundaries encompass:

- **The IAS Classic V3 application software made of the following parts:**
  - The IAS Classic V3 Applet Software
  - The MultiApp ID V2.1 javacard platform, based on [SUN] and [GP], which supports the execution of the personalized applets and provides card administration services
- **The associated smart card data, made of :**
  - The IAS Classic V3 applet data
  - The data stored by the MultiApp ID V2.1 platform (smartcard-related data)
- **The Integrated Circuit (either P5CC081 or P5CC145)**
- **The guidance documentation [AGD]**

Notes:

- Only the parts and features of the MultiApp ID V2.1 javacard platform, which support the installation and execution of the IAS Classic V3 applet, are within the TOE scope. Other javacard platform parts and features are out of the TOE.
- The IAS-XL, MPCOS 4.1, MOCA Server 1.0, MOCA Client 1.0, Crypto Manager, Custom EMV CAP and ZZZS HIC/HPC applets’ software is also embedded in the MultiApp ID V2.1 smartcard, but is not in the TOE scope for the present ST.
- The smartcard product includes a plastic body and associated security elements (such as holograms, security printing…) which are also outside the TOE scope.

4 TOE DESCRIPTION

4.1 ARCHITECTURE OF THE SMARTCARD CONTAINING THE TOE

The TOE is part of the MultiApp ID V2.1 smartcard. This smartcard contains the software dedicated to the operation of:

- The MultiApp ID V2.1 javacard opened platform, which supports the execution of the personalized applets and provides the smartcard administration services.
- The personalized applets: IAS XL, IAS Classic V3, MPCOS 4.1, MOCA Server 1.0, MOCA Client 1.0, Crypto Manager, Custom EMV CAP and ZZZS HIC/HPC.
- Additionally, other applets – not determined at the moment of the present evaluation – may be loaded on the smartcard before or after issuance.

Therefore, the architecture of the smartcard software and application data can be represented as follows:

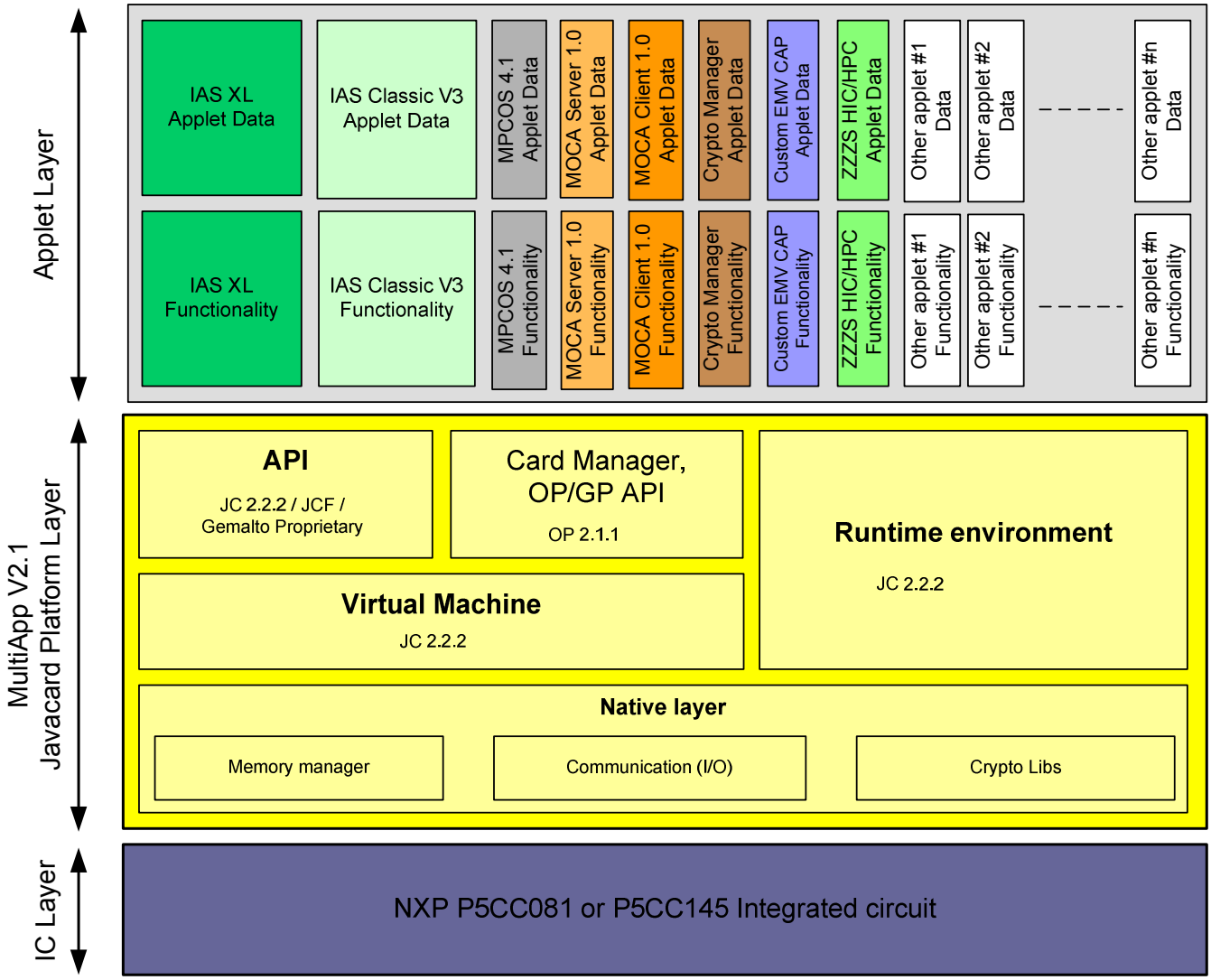


Figure 1: MultiApp ID V2.1 smartcard architecture

Actually, the IAS XL & Classic V3 functionalities[2], as well as the MPCOS 4.1 functionality, the MOCA Server/Client functionalities and the MultiApp V2.1 javacard platform, are entirely located in ROM. The Crypto Manager, Custom EMV CAP and ZZZS HIC/HPC functionalities are located in EEPROM, and any additional applet's executable code (loaded before or after issuance) would also be located in EEPROM, which might also contain any software patch that would be needed in the future.

All the data (related to the applets or to the javacard platform) are located in EEPROM. The separation between these data is ensured by the javacard firewall as specified in [JCRE222].

4.2 TOE BOUNDARIES

As illustrated by figure 2, the Target of Evaluation (TOE) is the IAS Classic V3 applet, supported by the MultiApp ID V2.1 javacard platform and the underlying integrated circuit. The [AGD] documentation is also part of the TOE.

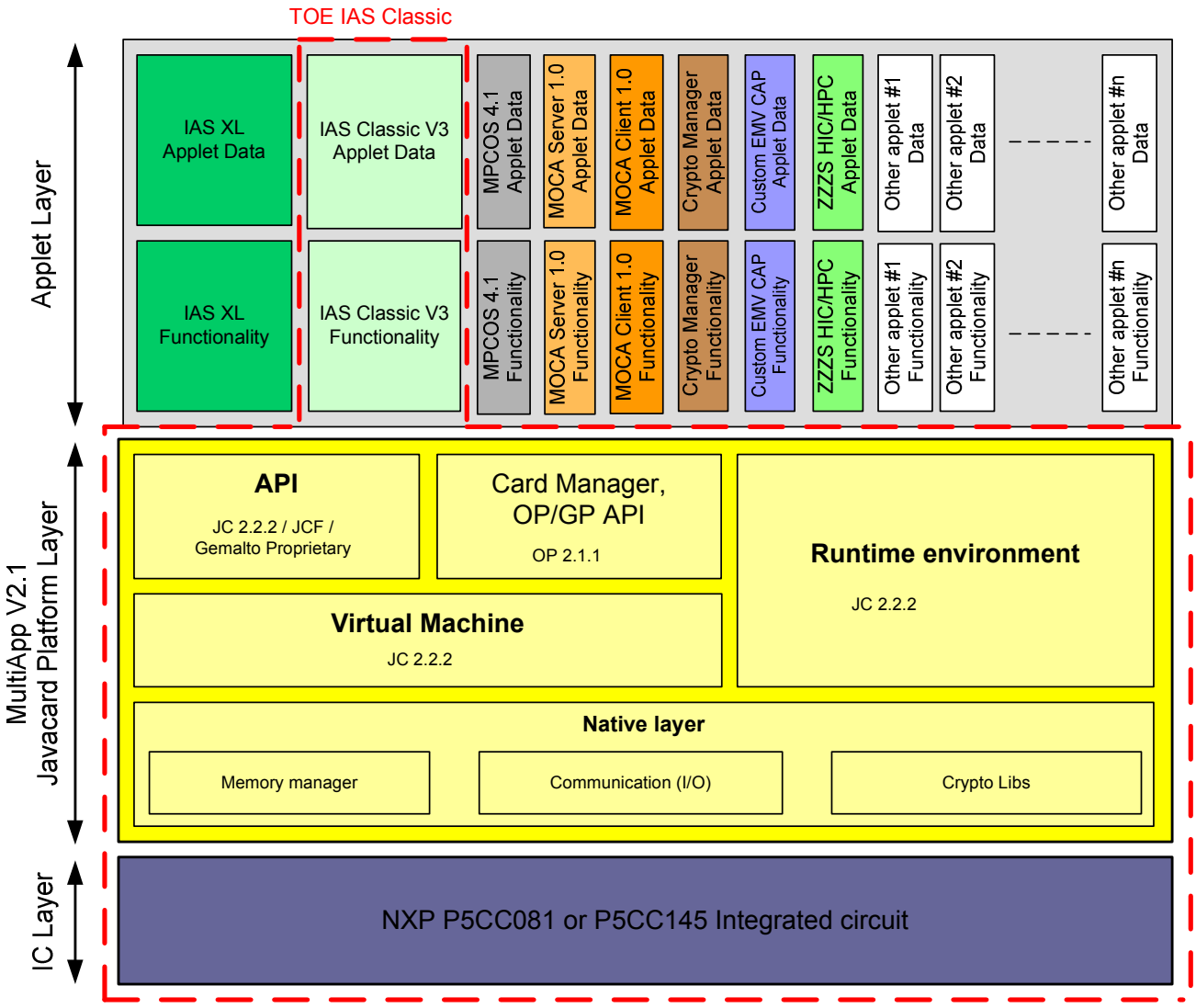


Figure 2: IAS Classic TOE boundaries

[2] What is meant here by « functionality » is the applet executable code

The other applets running on top of the javacard platform (IAS-XL, MPCOS 4.1, MOCA Server/Client, Crypto Manager, Custom EMV CAP and ZZZS HIC/HPC as well as any other applet loaded pre or post issuance) are outside the boundaries of the TOE - but are part of its IT environment.

Other smart card product elements (such as holograms, magnetic stripes, security printing etc.) are outside the scope of this Security Target.

4.3 MULTIAPP ID V2.1 JAVACARD PLATFORM DESCRIPTION

The MultiApp ID V2.1 platform is a smart card operating system that complies with two major industry standards:

- Sun's Java Card 2.2.2, which consists of the Java Card 2.2.2 Virtual Machine [JCVM222], the Java Card 2.2.2 Runtime Environment [JCRE222] and the Java Card 2.2.2 Application Programming Interface [JCAPI222].
- The Global Platform Card Specification version 2.1.1 [GP211].

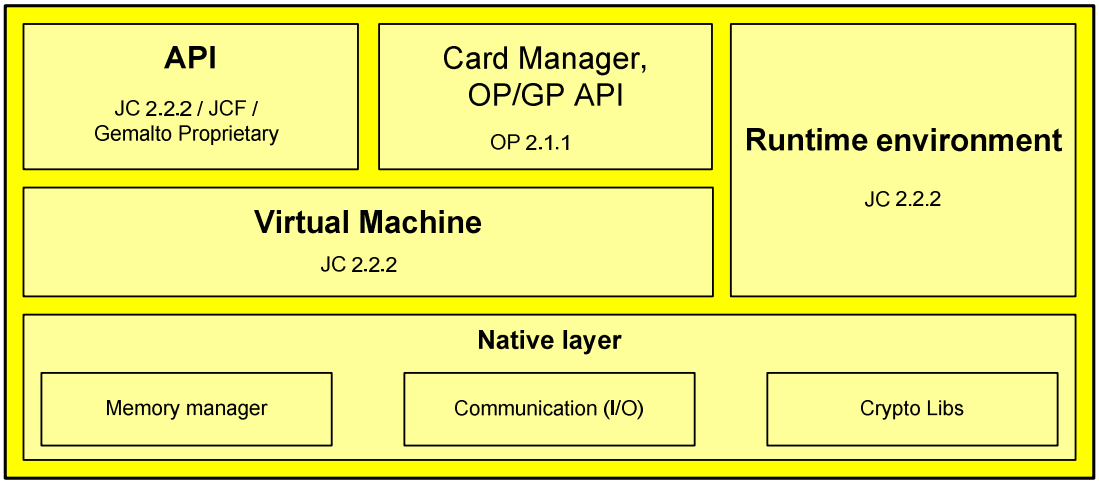


Figure 3: MultiApp ID V2.1 javacard platform architecture

As described in figure 3, the MultiApp ID V2.1 platform contains the following components:

- The **Native Layer**

  It provides the basic card functionalities (memory management, I/O management and cryptographic primitives) with native interface with the underlying IC. The cryptographic features implemented in the native layer, and which support the IAS Classic V3 functionality, are:

  - DES, Triple-DES
  - RSA 1024, 1152, 1280, 1536, 2048 - Standard and CRT methods
  - OBKG (RSA key pair)
  - SHA1, SHA256
  - Pseudo-Random Number Generation (PRNG).

- The **Javacard Runtime Environment**

  It conforms to [JCRE222] and provides a secure framework for the execution of the Java Card programs and data access management (firewall).

  Among other features, multiple logical channels are supported, as well as extradition, DAP, Delegated management, SCP01, SCP02 and SCP03.

- The **Javacard Virtual Machine**

  It conforms to [JCVM222] and provides the secure interpretation of bytecodes.

- The **API**

  It includes the standard javacard API [JCAPI222] and the Gemalto proprietary API.

- The **Open Platform Card Manager**

  It conforms to [GP211] and provides card, key and applet management functions (contents and life-cycle) and security control.

The MultiApp ID V2.1 platform provides the following services:

- Initialization of the Card Manager and management of the card life cycle
- Secure loading and installation of the applets under Card Manager control
- Deletion of applications under Card Manager control
- Extradition services to allow several applications to share a dedicated security domain
- Secure operation of the applications through the API
- Management and control of the communication between the card and the CAD
- 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 and cryptographic key objects
  - Generating random numbers
  - Handling secure data object and backup mechanisms
  - Managing memory content
  - Ensuring Java Card firewall mechanism

4.4 IAS CLASSIC V3 APPLET DESCRIPTION

IAS Classic V3 is a Javacard application that provides a Secure Signature Creation Device (SSCD) as defined in the DIRECTIVE 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures.

The IAS Classic V3 applet provides the following services related to electronic signature:

- Trusted channel services to secure the communications with CGA and SCA entities
- Key pair (SCD/SVD) generation
- SCD key import (if SCD was generated outside the TOE)
- SVD key export to a CGA (if SVD was generated inside the TOE), and reception/storage of certificate information.
- Reference authentication data (RAD) initialization
- Switch from a non-operational state to an operational state
- Signatory authentication (by means of PIN)
- Electronic signature creation
- Certificate verification.

The signature key material is composed of RSA key pairs. Each key pair is composed of a private key (the signature-creation data: SCD) and the associated public key (the signature-verification data: SVD). Key size is 1024, 1152, 1280, 1536 or 2048 bits.

The TOE is able to manage simultaneously several signature key pairs, which may be generated by the TOE itself, or imported from outside the TOE, or a combination thereof. In such cases the SCA shall allow the signatory to choose a given key pair before requesting any signature operation to the TOE.

If in an operational state, the TOE is able to create qualified electronic signatures with the following steps:

(a) Select an SCD if multiple are present in the SSCD
(b) Authenticate the signatory and determine its intent to sign,
(c) Receive data to be signed or a unique representation thereof (DTBS/R)
(d) Apply an appropriate cryptographic signature-creation function using the selected SCD to the DTBS/R.

The TOE shall only be switched to an operational state if it is properly prepared for the signatory's use and sole control by

— Generating (or importing) at least one SCD/SVD pair, and
— Personalizing for the signatory by storing in the TOE:
(a) The signatory's reference authentication data (RAD)
(b) Optionally, certificate info for at least one SCD in the TOE.

To authenticate himself as the legitimate user of the TOE, the signatory submits Verification Authentication Data (VAD) in the form of a PIN. The TOE compares the VAD with Reference Authentication Data (RAD) securely stored in the card. The authentication is successful if VAD and RAD are identical.

The TOE implements all IT security functionalities, which are necessary to ensure the SCD and RAD secrecy. 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 (i.e. CGA or SCA).

4.5 LIFE-CYCLES

4.5.1 Product life-cycle

The TOE life cycle is part of the product[3] life cycle, which is composed of the 7 phases described in [PP/0035] and recalled in the following table. The table also mentions the authority involved in each phase.

MultiApp ID V2.1 product life-cycle			
Phase n°	**Phase designation**	**Phase description**	**Comment**
1	SC embedded software development	The SC embedded software developer is in charge of the specification, development and validation of the MultiApp ID V2.1 software (SC operating system & applets). He also specifies the IC initialization data.	The SC embedded software developer is Gemalto.
2	IC development	The IC developer designs the IC, develops the IC dedicated software and provides information, software or tools to the SC embedded software developer. Then, the IC developer receives (from the SC embedded software developer through trusted delivery and verification procedures) the whole – or just a part – of the SC embedded software. From the IC design, the IC dedicated software and the delivered SC embedded software, he builds the Smart Card IC database needed for the IC photomask fabrication.	The IC designer is NXP
3	IC manufacturing and testing	The IC manufacturer is responsible for producing the IC through three main steps: IC manufacturing, IC testing, and IC initialisation.	The IC manufacturer is NXP
4	IC Packaging	The IC Packager is responsible for the smartcard module manufacturing and testing.	The IC Packager is NXP or Gemalto
5	Pre-personalization	The Prepersonalizer loads embedded software components within the smartcard module, builds the Smartcard profile, loads the data needed for card personalization and performs tests.	The Prepersonalizer is NXP or Gemalto

[3] i.e. the whole MultiApp ID V2.1 smartcard software and hardware.

6	Personalization	The Personalizer builds the card administration and application profiles (file creation and data loading) and performs final tests.	The Personalizer is Gemalto or another accredited company.
7	End-usage	The SC issuer is responsible for the SC product delivery to the SC end-user (cardholder), and the end of life process.	The cardholder is a customer of the SC issuer.

Table 1: MultiApp ID V2.1 product life-cycle

Two scenarios are to be considered for the present evaluation:

- The first scenario (LC1), which is the standard one, is described by figure 4. According to this scenario, the IC is manufactured at NXP site. It is then shipped to Gemalto site where it is initialized and pre-personalized and then shipped to the Personalizer. During the shipment from Gemalto to the Personalizer, the module is protected by a diversified key.

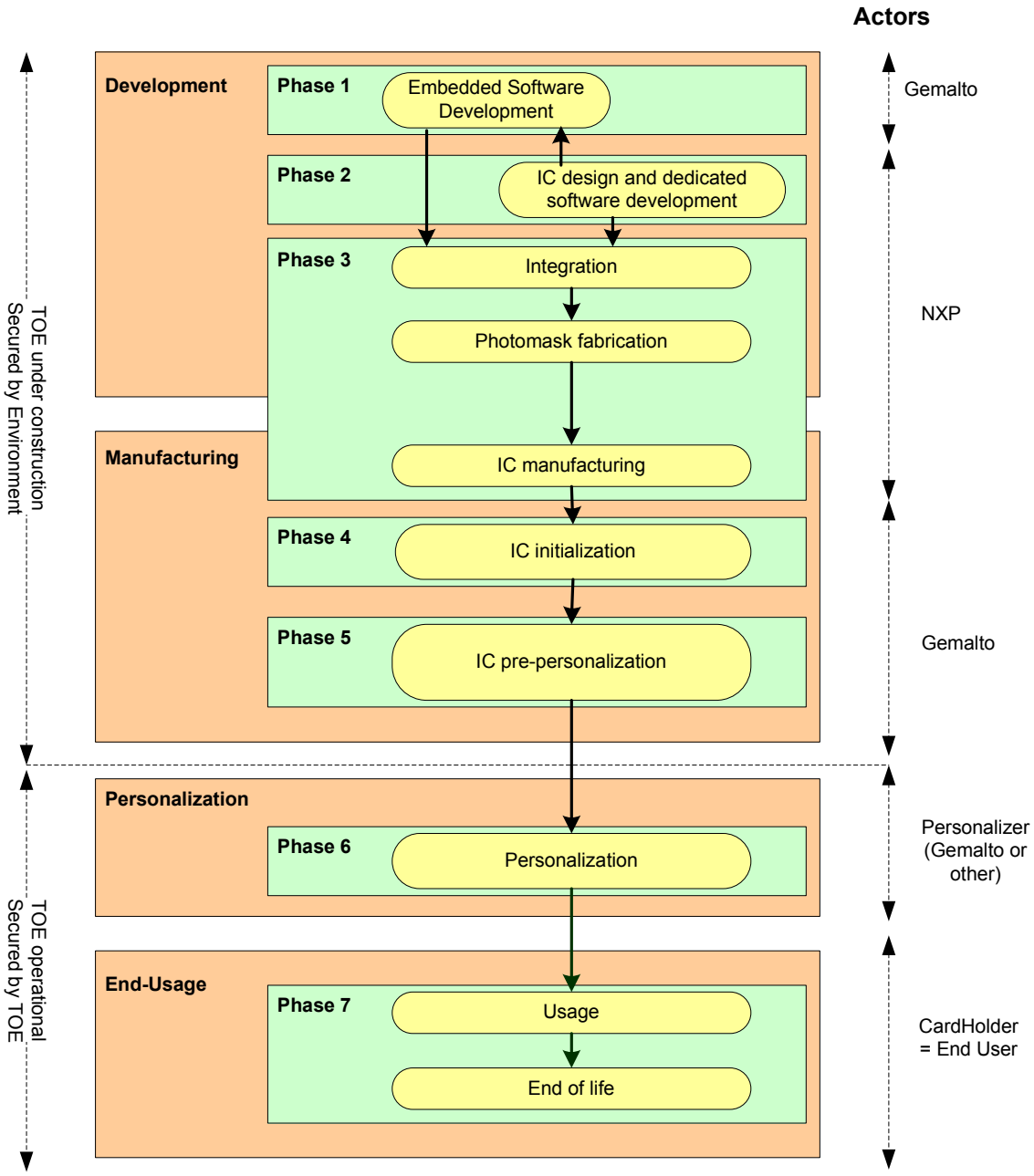


Figure 4: LC1: Init on module at Gemalto site

- The second scenario (LC2) is an alternative to LC1, and is described by figure 5. It corresponds to the situation where the customer whishes to receive wafers directly from the founder. In this case, initialization and pre-personalization, which include sensitive operations such as the loading of patches, take place at NXP site. The creation of files is started by the founder and completed by the personalizer. During the shipment from NXP to the Personalizer, the module is protected by a diversified key.

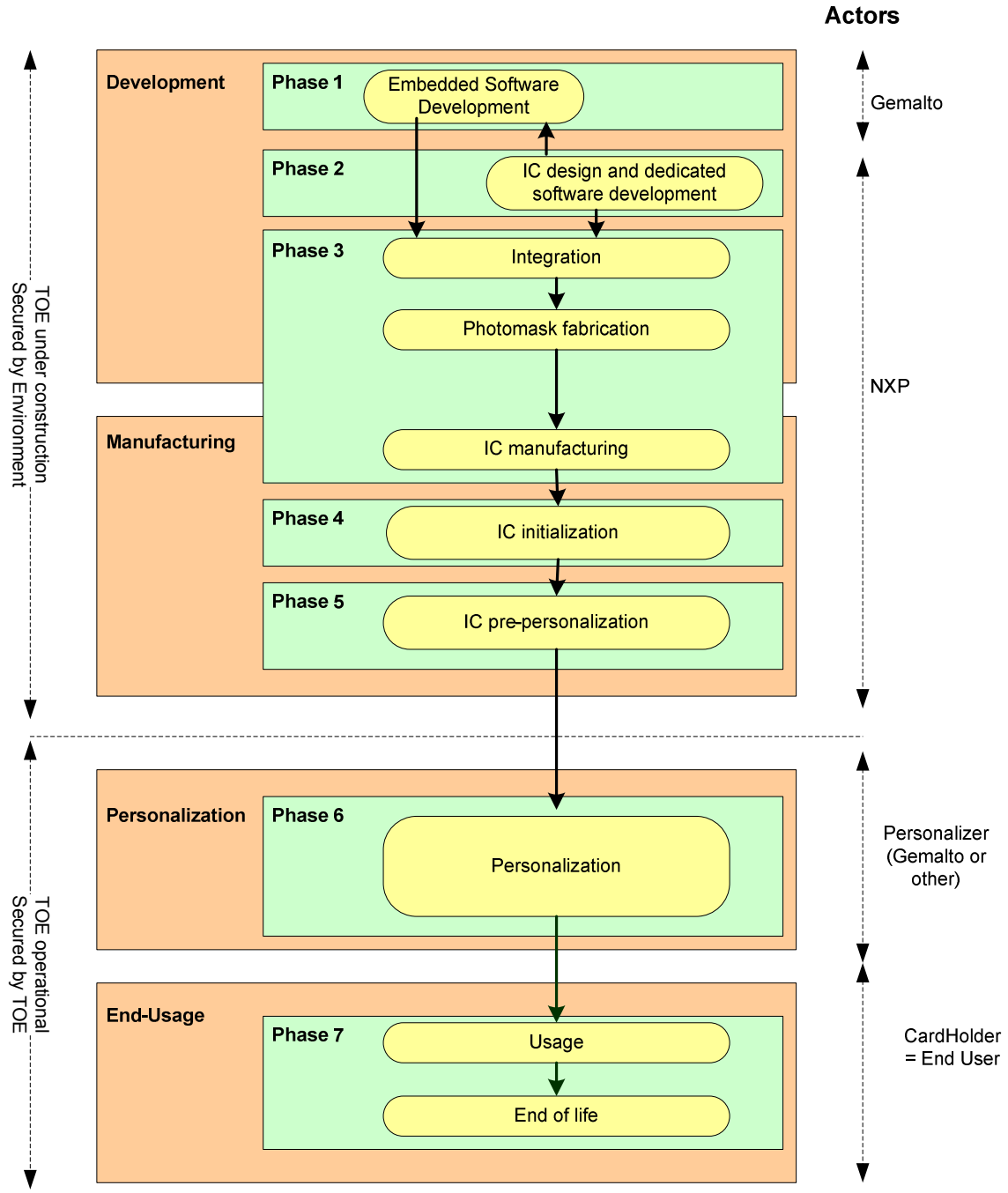


Figure 5: LC2 Init on module at Founder site

4.5.2 TOE life-cycle

The TOE life-cycle itself can be decomposed in four stages:

- Development
- Storage, pre-personalization and testing
- Personalization and testing
- Final usage

The TOE storage is not necessarily a single step in the life cycle since it can be stored in parts. The TOE delivery occurs before storage and may take place more than once if the TOE is delivered in parts.

These four stages map to the product life cycle phases as shown in Figure 6.

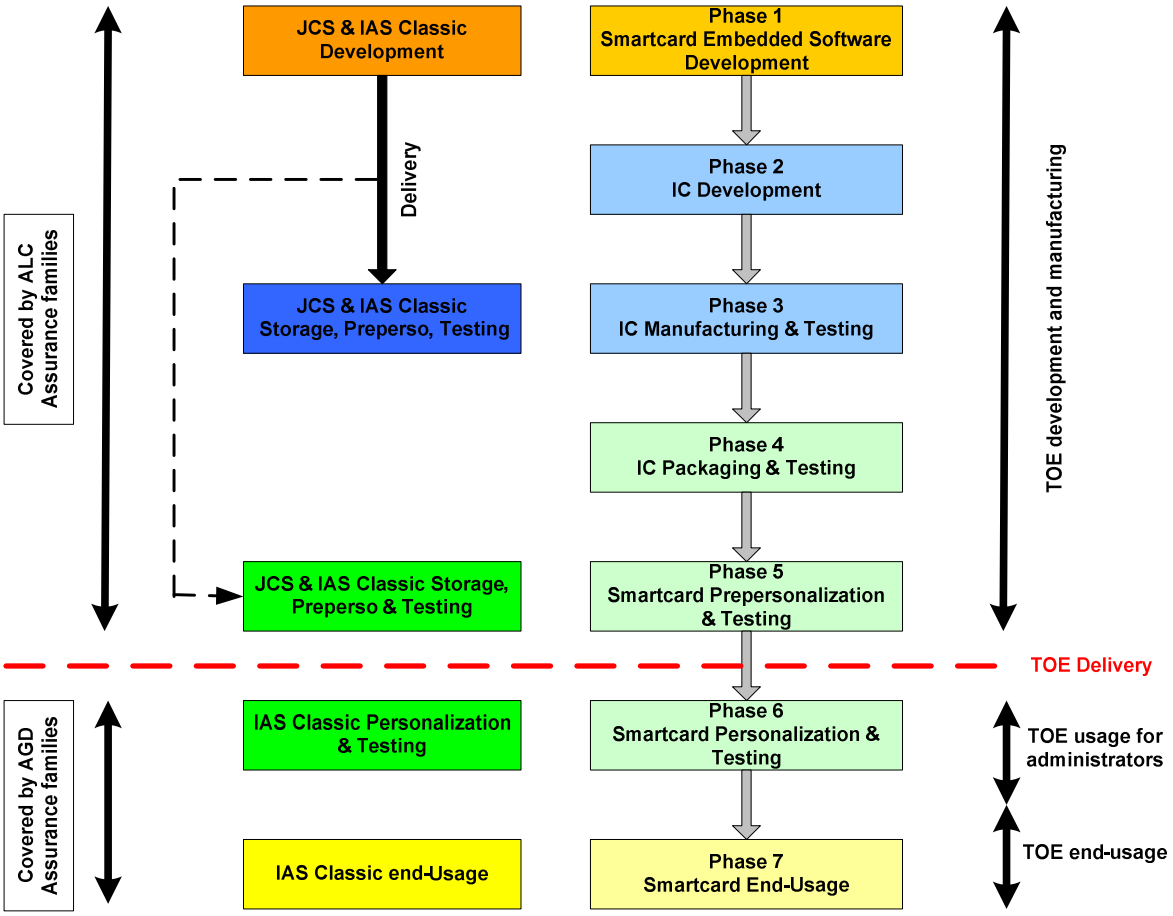


Figure 6: TOE Life Cycle within Product Life Cycle

The IAS Classic V3 & JCS development is performed during Phase 1. This includes IAS Classic V3 and JCS conception, design, implementation, testing and documentation. The development shall fulfill requirements of the final product, including conformance to Java Card Specifications, and recommendations of the SCP user guidance. The development shall occur in a controlled environment that avoids disclosure of source code, data and any critical documentation and that guarantees the integrity of these elements. The present evaluation includes the IAS Classic V3 & JCS development environment.
In Phase 3, the IC Manufacturer may store, initialize the TOE and potentially conduct tests on behalf of the TOE developer. The IC Manufacturing environment shall protect the integrity and confidentiality of the TOE and of any related material, for instance test suites. The present evaluation includes the whole IC Manufacturing environment, in particular those locations where the TOE is accessible for installation or testing. As the Security IC has already been certified against [PP/0035] there is no need to perform the evaluation again.

In Phase 5, the SC Pre-Personalizer may store, pre-personalize the TOE and potentially conduct tests on behalf of the TOE developer. The IAS Classic V3 applet installation, as well as the loading of any softmask, is performed during phase 5. The SC Pre-Personalization environment shall protect the integrity and confidentiality of the TOE and of any related material, for instance test suites.

(Part of) TOE storage in Phase 5 implies a TOE delivery after Phase 5. Hence, the present evaluation includes the SC Pre-Personalization environment. The TOE delivery point is placed at the end of Phase 5, since the entire TOE is then built and embedded in the Security IC.

The TOE is personalized in Phase 6: loading of the IAS Classic V3 applet data, SCD import (if any), SVD export for certificate. The SC Personalization environment is not included in the present evaluation. Appropriate security recommendations are provided to the SC Personalizer through the [AGD] documentation.

Phase 7 corresponds to the TOE end-usage. SCD/SVD generation (if any) and signature creation take place during phase 7. The SSCD destruction corresponds to the end of phase 7.

4.5.3 Involved sites

The following development and manufacturing sites are involved in the development and construction of the TOE, and shall therefore be included within the scope of the present evaluation:

Life cycle phase	Involved sites
Embedded software development (Phase 1)	**Gemalto Meudon** site (all development teams) **Gemalto La Ciotat** site (MKS servers) **Gemalto Gémenos** site (Component team[4])
IC development (Phase 2)	NXP development site(s) mentioned in [CR-P5CC081] and [CR-P5CC145]
IC Manufacturing & Testing (Phase 3)	NXP production site(s) mentioned in [CR-P5CC081] and [CR-P5CC145]
IC initialization, packaging & testing (Phase 4)	Scenario LC1: **Gemalto Gémenos** site **Gemalto Singapore** site Scenario LC2: NXP production site(s) mentioned in [CR-P5CC081] and [CR-P5CC145]
Prepersonalization & testing (Phase 5)	Scenario LC1: **Gemalto Gémenos** site **Gemalto Singapore** site **Gemalto Vantaa** site Scenario LC2: NXP production site(s) mentioned in [CR-P5CC081] and [CR-P5CC145]

Table 2: Sites involved in TOE development and manufacturing

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

4.6 TOE USERS

The TOE users (in the CC meaning, i.e. after TOE delivery) are described hereunder:

Personalizer

The Smart Card Personalizer personalizes the card by loading the cardholder data as well as cryptographic keys and PIN. For this TOE, the personalizer is the Card Issuer. At the end of this phase, the card is 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 and generate a new SCD/SVD pair.

From what precedes, two roles are identified for the present evaluation: the Administrator S.ADMIN (which is the card issuer) and the Signatory S.SIGY (which is the card end-user).

4.7 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 to 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.

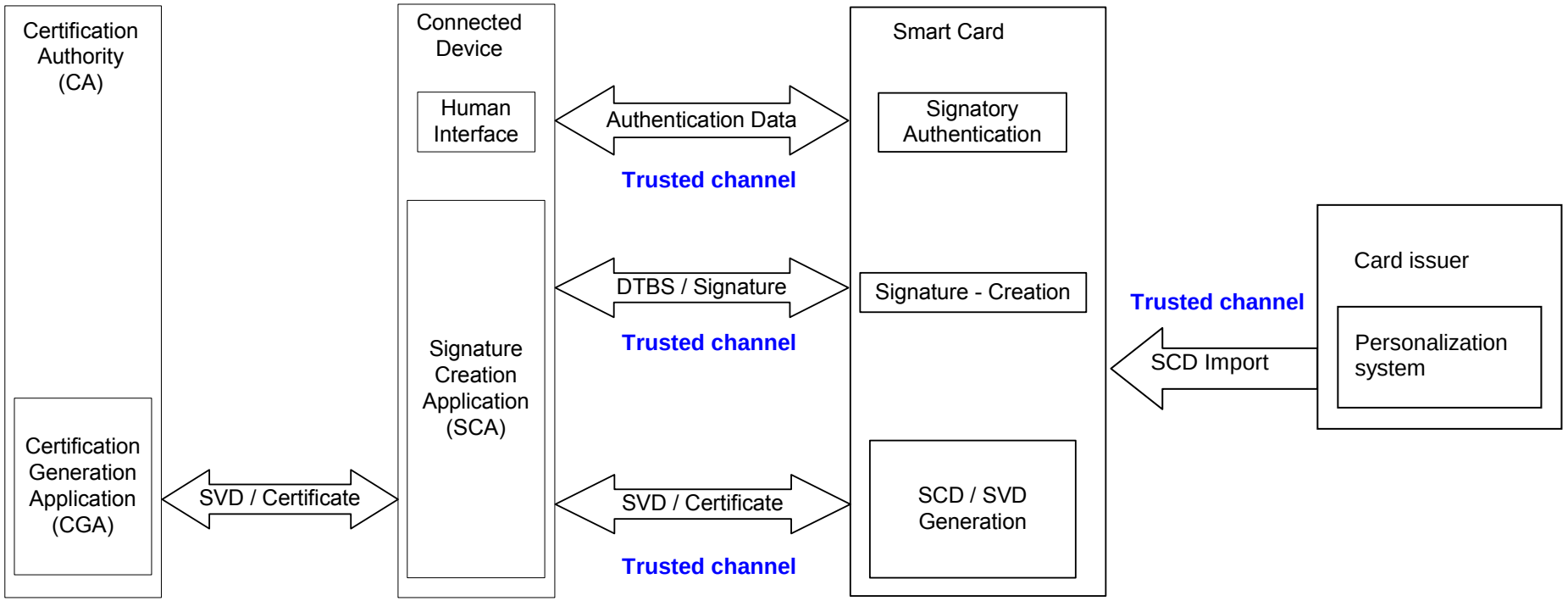


Figure 7 - TOE Usage

5 CONFORMANCE CLAIMS

Common criteria Version:

This ST conforms to CC Version 3.1 [CC-1] [CC-2] [CC-3]

Conformance to CC part 2 and 3:

- CC part 2 extended
- CC part 3 conformant

Assurance package conformance:

EAL4 augmented (EAL4+)

This ST conforms to the assurance package EAL4 augmented by ALC_DVS.2 and AVA_VAN.5.

Evaluation type

This is a composite evaluation, which relies on the P5CC081 and P5CC145 chip certificates and evaluation results.

P5CC081 and P5CC145 chip certificates:

- Certification done under the BSI scheme
- Certification reports [CR-P5CC081] and [CR-P5CC145]
- Security Targets [ST-P5CC081] and [ST-P5CC145] strictly conformant to IC Protection Profile [PP/0035]
- Common criteria version: 3.1
- Assurance level: EAL5 augmented by ASE_TSS.2, ALC_DVS.2 and AVA_VAN.5

Consequently, the composite product evaluation (i.e. the present evaluation) includes the additional composition tasks defined in the CC supporting document “Composite product evaluation for smart cards and similar devices” [CCDB].

Protection Profile conformance

This ST claims strict conformance to the SSCD Protection Profiles [PP-SSCD /T2] & [PP-SSCD /T3].

Remark: [PP-SSCD /T2] & [PP-SSCD /T3] are based on Common Criteria v2.3, whereas the present ST is based on Common Criteria v3.1. The following equivalence between CC v2.3 EAL4+ and CC v3.1 EAL4+ shall be taken into account in further sections of the present document:

- ADV_IMP.2 (Development – Implementation of the FSP) in CC v2.3 EAL4 is equivalent to ADV_IMP.1 in CC v3.1 EAL4
- ALC_DVS.2 (Sufficiency of security measures) augmentation is maintained in CC v3.1 EAL4+
- AVA_MSU.3 (Analysis and testing for insecure states) in CC v2.3 EAL4 moved in AGD families in CC v3.1 EAL4
- AVA_VLA.4 (Highly resistant) en CC v2.3 EAL4+ is equivalent to AVA_VAN.5 in CC v3.1 EAL4+

6 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 /T2] [PP-SSCD /T3].

6.1 DIGITAL SIGNATURE ASSETS

The assets of the TOE are those defined in [PP-SSCD /T2], [PP-SSCD /T3] and [PP/0035].

The present Security Target deals with the assets mentioned in [PP-SSCD /T2] and [PP-SSCD /T3]. The assets of [PP/0035] are studied in [ST-P5CC081] and [ST-P5CC145].

Asset	Description
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).

6.2 DIGITAL SIGNATURE SUBJECTS

Subject	Description
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.**

6.3 DIGITAL SIGNATURE THREATS

Threat	Description
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 Signed-data objects (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.

6.4 DIGITAL SIGNATURE ASSUMPTIONS

This section defines assumptions related to the Digital Signature application as stated in PP SSCD and as stated in [PP/0035] for composite evaluation.

Assumption	Description
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.

6.5 ORGANIZATIONAL SECURITY POLICIES

This section defines OSPs related to the Digital Signature application as stated in [PP-SSCD /T2] and [PP-SSCD /T3].

OSP	Description
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.

7 SECURITY OBJECTIVES

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

They cover the following aspects:
- The security objectives for the TOE,
- The security objectives for the environment.

The security objectives stated in [PP/0035] can be found in [ST-P5CC081] and [P5CC145].

7.1 SECURITY OBJECTIVES FOR THE TOE

TOE security objective	Description
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.

TOE security objective	Description
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.

7.2 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 Objective	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.

Security Objective	Description
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 .

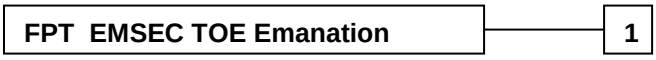
8 EXTENDED COMPONENTS DEFINITION

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.

9 SECURITY REQUIREMENTS

9.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This chapter defines the security functional requirements for the TOE using functional requirements components as specified in [PP-SSCD /T2] and [PP-SSCD /T3].

[ST-P5CC081] and [ST-P5CC145] deal with the security functional requirements of [PP/BSI-0002].

9.1.1 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 [5]
FPT_EMSEC.1	TOE Emanation

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

Identification	Description
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 3. *IAS Classic security functional requirements list*

9.1.2 FCS – Cryptographic support

Remark: To be in the context of the French qualification RSA keys shall be 2048-bits long.

9.1.2.1 FCS_CKM cryptographic key management

FCS_CKM.1 Cryptographic key generation

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, 1152, 1280, 1536 and 2048 bits]** that meet the following: **[no standard]**.

Application note: Type 3 only.

Remark: Link with Initialization SFP.

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

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

FCS_CKM.4 Cryptographic key destruction

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]**.

Remark: Link with SCD destruction SFP.

9.1.2.2 FCS_COP Cryptographic operation

FCS_COP.1 Cryptographic operation

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, 1152, 1280, 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.1.1/ SIGNING	The TSF shall perform **[Digital signature-generation]** in accordance with a specified cryptographic algorithm **[RSA_SHA_PKCS#1]** and cryptographic key sizes **[1024, 1152, 1280, 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.1.1/MAC	The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **TDES** and cryptographic key sizes **112 bits** that meet the following: **GP Secure Messaging.**

FCS_COP.1.1/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.1.1/ SHA	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.1.1/ 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.

9.1.3 FDP: User data protection

9.1.3.1 FDP_ACC Access Control policy

FDP_ACC.1 Subset access control

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

Application note: Type 2 only.

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

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

9.1.3.2 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.1.1/ 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 following additional rules: The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorized" is not allowed to generate SCD/SVD pair.

Application note: Type 3 only.

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

FDP_ACF.1.1/ Signature-creation SFP	The TSF shall enforce the [**Signature-creation SFP**] to objects based on [**General attribute group**] and [**Signature-creation attribute group**].
FDP_ACF.1.2/ Signature-creation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".

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

9.1.3.3 FDP_ETC :Export to outside TSF control

FDP_ETC.1: Export of user data without security attributes

FDP_ETC.1.1/ SVD Transfer	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/ SVD Transfer	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.

9.1.3.4 FDP_ITC Import From outside TSF control

FDP_ITC.1: Import of user data without security attributes

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.1.1/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.

9.1.3.5 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.

9.1.3.6 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 in containers controlled by the TSF for [**integrity error**] on all objects, based on the following attributes: [**integrity checked persistent stored data**].
FDP_SDI.2.2/ Persistent	Upon detection of a data integrity error, the TSF shall: [**1. prohibit the use of the altered data** **2. inform the Signatory about integrity error**.]

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 in containers controlled by the TSF for **[integrity error**] on all objects, based on the following attributes: [**integrity checked stored data].**
FDP_SDI.2.2/DTBS	Upon detection of a data integrity error, the TSF shall: [**1. prohibit the use of the altered data** **2. inform the Signatory about integrity error.**]

Application note:

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

9.1.3.7 FDP_UCT Inter-TSF user data confidentiality transfer protection

FDP_UCT.1 Basic data exchange confidentiality

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

Application note: Type 2 only.

9.1.3.8 FDP_UIT Inter-TSF user data integrity transfer protection

FDP_UIT.1: Data exchange integrity

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

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.

9.1.4 FIA: Identification and authentication

9.1.4.1 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.

9.1.4.2 FIA_ATD User attribute definition

FIA_ATD.1 User attributes definition

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

9.1.4.3 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.

9.1.4.4 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.

9.1.5 FMT: Security management

9.1.5.1 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**].

9.1.5.2 FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes

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.1.1/ 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.3.1/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.3.1/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.

9.1.5.3 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.

9.1.5.4 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

9.1.5.5 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.

9.1.6 FPT: Protection of the TSF

9.1.6.1 FPT_EMSEC 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.

9.1.6.2 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.

9.1.6.3 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 SFRs are always enforced.

Remark: Link with Protection SFP.

9.1.6.4 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.

9.1.7 FTP: Trusted Path / Channel

9.1.7.1 FTP_ITC Inter-TSF trusted channel

FTP_ITC.1 Inter-TSF trusted Channel

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.1.1/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.1.1/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.

9.1.7.2 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”.

9.2 SECURITY ASSURANCE REQUIREMENTS

The TOE security assurance requirements define the assurance requirements for the TOE using only assurance components drawn from [CC-3].

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

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

9.2.1 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
Life-cycle support	-- (ACM_CAP)	ALC_CMC
	-- (ACM_SCP)	ALC_CMS

Assurance class	Assurance Family CC2.x	Assurance Family CC3.1
	-- (ADO_DEL)	ALC_DEL
	ALC_DVS	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 4. 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 5. TOE security assurance requirements list

10 TOE SUMMARY SPECIFICATION

The security functions provided by the IC are described in [ST-P5CC081] and [ST-P5CC145]. The TOE Security Functionalities are described below.

10.1 TOE SECURITY FUNCTIONALITIES PROVIDED BY PLATFORM

10.1.1 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 SF.LOG: Logical Protection (see [ST-P5CC081] and [P5-CC145]).

10.1.2 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 SF.PHY: Protection against Physical Manipulation (see [ST-P5CC081] and [ST-P5CC145]).

10.2 TOE SECURITY FUNCTIONALITIES PROVIDED BY IAS CLASSIC V3 APPLET

10.2.1 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

10.2.2 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, 1152, 1280, 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.
- 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. It is supported by the IC security services SS.RNG (Random Number Generator) and SS.HW_DES (Triple-DES Co-processor), see [ST-P5CC081] and [ST-P5CC145].

10.2.3 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.

10.2.4 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.

10.2.5 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.

Security Function/ SFRs	TSF_AUTHENTICATION	TSF_CRYPTO	TSF_INTEGRITY	TSF_MANAGEMENT	TSF_SECURE_MESSAGING	TSF_CARD_EMANATION	TSF_CARD_PROTECT
FCS_CKM.1/RSA		X					
FCS_CKM.1/DH	X						
FCS_CKM.1/TDES	X						
FCS_CKM.4		X					
FCS_COP.1/CORRESP		X					
FCS_COP.1/SIGNING		X					
FCS_COP.1/MAC	X				X		
FCS_COP.1/TDES	X				X		
FDP_ACC.1				X			
FDP_ACF.1				X			
FDP_ETC.1				X			
FDP_ITC.1				X			
FDP_RIP.1		X	X				
FDP_SDI.2/Persistent			X				
FDP_SDI.2/DTBS			X				
FDP_UCT.1					X		
FDP_UIT.1					X		
FIA_AFL.1	X						
FIA_ATD.1	X						
FIA_UAU.1	X						
FIA_UID.1	X						
FMT_MOF.				X			
FMT_MSA.1/ Administrator				X			
FMT_MSA.1/ Signatory				X			
FMT_MSA.2	X			X			
FMT_MSA.3				X			
FMT_MTD.1				X			
FMT_SMF.1	X			X			
FMT_SMR.1				X			
FPT_EMSEC.1						X	

Security Function/ SFRs	TSF_AUTHENTICATION	TSF_CRYPTO	TSF_INTEGRITY	TSF_MANAGEMENT	TSF_SECURE_MESSAGING	TSF_CARD_EMANATION	TSF_CARD_PROTECT
FPT_FLS.1							X
FPT_PHP.1							X
FPT_PHP.3							X
FPT_TST.1							X
FTP_ITC.1					X		
FTP_TRP.1					X		

Table 6. *Coverage of PP SSCD SFRs by TOE security functionalities*

END OF DOCUMENT