Sagem Défense Sécurité
SAFRAN Group

:

SECURITY TARGET FOR THE

MORPHO-CITIZ 32 CARD

PHILIPS COMPONENT

Common Criteria version 2.2
Augmented EAL 4

(ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4)

Public Version

Version 1.1
2007

TABLE OF CONTENTS

Courtesy translation

1. INTRODUCTION OF THE SECURITY TARGET

1.1 IDENTIFICATION OF THE SECURITY TARGET

Document Identification:

Title	: Lite Security target Morpho-Citiz 32 card – Component PHILIPS
Version	: 1.1
Security Target Identifier	: SK-0000053756

TOE Identification:

Component Identifier	: PHILIPS Component: P5CC036V1 – Rev D
Masked Component Identifier	: MC32/P5CC036V1D/1.0.0
User Guide	: SK-0000051481 – 1.01 – MC32 - User Guide
Administrator Guide	: SK-0000051475 – 1.01 – MC32 - Administrator Guide
Installation and Start-Up Guide	: SK 0000051482 – 1.2 – Installation Procedure
Delivery Guide	: SK-0000057043 - 1.01 - PHILIPS Delivery Procedure

CC Compliance:

Assurance Level	: EAL4 augmented by assurance components ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.
Function Resistance Level	: SOF – High
CC Version	: 2.2
Component Certificate	: BSI-DSZ-CC-0293-2005
Crypto Librarian Certificate	: BSI-DSZ-CC-0296-2006

1.2 OVERALL VIEW OF THE SECURITY TARGET

This security target specifies the functional and security assurance requirements applicable to the electronic administration application in compliance with IAS of the Morpho-Citiz 32 card referred to hereafter as the IAS-eGOV application .

The TOE described in the framework of this security target is composed of embedded software on a component type smart card, reference P5CC036V1, with a cryptographic library called "Crypto Library on SmartMX."

The reference component P5CC036V1 and the cryptographic library "Crypto Library on SmartMX“ were assessed separately:

- The component reference P5CC036V1 was assessed according to the protection profile **[R5 – BSI0002]** and has received reference certificate BSI-DSZ-CC-0293-2005.
- The cryptographic library "Crypto Library on SmartMX“ on component P5CC036V1 has received reference certificate BSI-DSZ-CC-0296-2006.

The assessment of the TOE is thus a composition of the assessment of the embedded software on component P5CC036V1 with the library “Crypto Library on SmartMX.”

Courtesy translation

In its operating environment, IAS-eGOV application performs the electronic administration services as defined in documents **[R10 – AREAK1]** and **[R11 – AREAK2]**.

The IAS-eGOV application is an electronic administration (e-administration) development support through the available services responding essentially to the new needs of the electronic administration (as defined by the AEAD).

Within the framework of electronic administration contexts, IAS-eGOV application offers electronic signature services responding to the characteristics of a secure signature creation device (SSCD) that allow the implementation of so-called “qualifying,” certificates.

This security target thus specifies the functional security requirements and the security assurance requirements applicable to “secure” electronic signature services of the IAS-eGOV application.

In its operating environment, the IAS-eGOV application performs the secure electronic signature services in compliance with the European directive **[R6 – Directive]** transcribed in protection profile **[R4 – SSCD T3]**. These functions are:

- Generation of an electronic signature bi-key (SCD/SVD);
- Destruction of the electronic signature bi-key (SCD/SVD);
- Loading of electronic signature private key (SCD);
- Electronic signature creation.

The assurance level specified in the present security target and in its documentation is EAL 4 augmented by assurance components ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

The resistance level for functional security requirements is “high” (High SOF).

1.3 CC COMPLIANCE

This security target complies with Common Criteria V2.2 **[R1 – CC]**.

This security target complies with protection profile **[R3 – SSCD T2]** and **[R4 – SSCD T3]**. It is also based on protection profile **[R2 – 9911]** and on the target **[R15 – CLST]**.

The security target is in itself compliant with part 2 of the Common Criteria V2.2 expanded by requirement FPT_EMSEC defined in protection profiles **[R3 – SSCD T2]** and **[R4 – SSCD T3]**, by requirement FCS_RND.1 defined in protection profile **[R5 – BSI0002]** and by requirements FCS_RND.2 and FPT_TST.2 defined in target **[R15 – CLST]**.

The security target is in compliance with part 3 of the CC.

1.4 DOCUMENT ORGANISATION

The present security target is organized in 8 chapters in the following manner:

Chapter 1: Present introduction;
Chapter 2: General description of the TOE providing general information on the TOE that allows for introduction of the choices regarding security requirements;
Chapter 3: Presentation of the TOE security environment in which the TOE is used. It particularly describes

the property to protect, the users intervening on the TOE, the assumptions as well as the applicable threats and the organizational security policies;

Chapter 4: Presentation of security objectives satisfied by the TOE in its operating environment.

Chapter 5: Presentation of the security requirements satisfied by the TOE and its environment, in terms of functional requirements on the one hand and security assurance requirements on the other;

Chapter 6: Presentation of the general definitions of the security functions and assurance measures implemented by the TOE responding to the functional and assurances requirements;

Chapter 7: Presentation of existing protection profiles to which the present security target refers;

1.5 REFERENCE DOCUMENTS

[R1 – CC]: Common Criteria for Information Technology Security Evaluation- Version 2.2, January 2004.

[R2 – 9911]: Eurosmart Protection Profile, Smart Card Integrated Circuit With Embedded Software, PP/9911, v2.0, June 1999

[R3 – SSCD T2]: Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001.

[R4 – SSCD T3]: Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001.

[R5 – BSI0002]: Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001

[R6 – Directive]: DIRECTIVE 1999/93/EC of the EUROPEAN PARLIAMENT and COUNCIL of 13 December 1999 on a community framework for electronic signatures.

[R7 – Algo]: Algorithms and parameters of the algorithms, list of the algorithms and parameters eligible for the electronic signatures as defined in the directive 1999/93/EC, article 9 on the “Committee on Electronic Signatures” of the Directive.

[R8 – IPA]: SK - 0000020920 – 1.23 –Functional specifications of the IPA application
SK 0000053628 - Addendum to the Functional specifications of the IPA application

[R9 – E-ADMIN]: SK 0000020918 – 1.19 – Specification of the E-ADMINISTRATION application

[R10 – AREAK1]: CWA 14890-1: Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements – April 2004 (AREA-K-1)

[R11 – AREAK2]: CWA 14890-2: Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services – May 2004 (AREA-K-2)

[R12 – 7816 – 4]: ISO/IEC 7816 – 4: Identification cards Integrated circuits cards with contacts
Part 4 – Inter-industry commands for interchange

[R13 – ERRATUM]: eADMINISTRATION Common Platform
Technical Specification: Erratum to version 1.01

[R14 – HWST]: Security Target, BSI-DSZ-CC-0293, Evaluation of the P5CC036VID Secure Smart Card Controller, Version 1.0 – March 18th, 2005

[R15 – CLST]: Security Target lite, BSI-DSZ-CC-0296, Evaluation of the Secured Crypto Library on the P5CC036VID, Version 2.1.0 – December 6th, 2005

1.6 TERMINOLOGY

Administrator : A user who performs the initialisation of the target of evaluation (TOE), the personalization of the TOE or other TOE administrative functions.

Signature Creation Application (SCA) : Application used for creating an electronic signature, with exception to SSCD, i.e., the SCA is a group of application elements used for:

(a) Performing the DTBS presentation to the signatory prior to the signing process according to the signatory’s decision;

(b) Sending representation of the DTBS to the TOE if the signatory indicates his intention to sign by an entry or a non-interpretable action;

(c) Attach the qualified electronic signature generated by the TOE to the data or to provide the qualified electronic signature as separate data.

Certification Generation Application (CGA) : A group of application elements that request the data pertaining to the verification of the signature through SSCD for generation of the qualifying certificate. The CGA requests the generation of a corresponding SCD/SVD pair by the SSCD if the SVD requested have yet to be generated by the SSCD. The CGA verifies the authenticity of the SVD by (a) proof of the correspondence SSCD between the SCD and the SVD and; (b) a verification by the issuer and of the integrity of the SVD received.

Security Attribute : Information associated with subjects, users or objects, that is used for TSP application.

Signature Attributes : Supplementary information that is signed at the same time as the user message.

Property : Information or resources to be protected by the counter-measures of a TOE.

Certificate : Electronic certificate binding SVD to a person and confirming this latter's identity (defined in the Directive [1], article 2.9).

Qualifying Certificate : Certificate that fulfils requirements targeted at annexe I of the Directive [1] and provided by a CSP that fulfils requirements targeted annexe II of the Directive [1]. (defined in Directive [1], article 2.10)

Target of evaluation (TOE) : A product or IT system and the associated documentation for the administrator and for the user who is concerned by an assessment.

Security target (ST) : A group of security requirements and specifications to be used as a basis for assessing an identified TOE.

Directive : The 1999/93/EC directive of the European Parliament and Council of 13 December 1999 on a community framework for electronic signatures [1] is also named the 'Directive' in the rest of the PP.

Secure Signature Creation Device (SSCD) : Software device or material configured for applying SCD and that satisfies the requirements set forth in Annexe III of the Directive [1]. (defined in Directive [1], articles 2.5 and 2.6).

Reference Authentification Data (RAD) : Data permanently stored by the TOE for verification of the tentative authentification as an authorized user.

Signature Creation Data (SCD) : Unique data, such as private codes or cryptographic keys, that the signatory uses for creating an electronic signature (defined in Directive [1], article 2.4).

Signature Verification Data (SVD) : Data, such as public codes or cryptographic keys, that are used for verifying the electronic signature (defined in the Directive [1], article 2.7).

Authentification Data : Information used for verifying the identity announced by a user.

Verification Authentification Data (VAD) : Authentification data provided upon entry by the user or authentification data derived from the user's biometric characteristics.

Data To Be Signed (DTBS) : Electronic data to be signed (including both the user message and the signature attributes).

TSF Data (TSF data) : Data created by and for the TOE, that may affect TOE functioning.

User Data (User Data) : Data created by and for the user, that does not affect TSF functioning.

Invalidation : If a subject or an object is invalidated, it is no longer available in the system. It is logically destroyed.

Object : Entity upon which a subject performs operations. When a subject is the target of an operation, it is seen as an object.

Signed Data Object (SDO) : Electronic data to which the electronic signature was logically attached or associated as an authentification method.

Certification Service Providers (CSP) : Any entity or natural person or legal entity that delivers certificates or provides other services related to electronic signatures (defined in the Directive [1], article 2.11).

Refinement : The addition of details to a component.

Special Functions Registers : The registers used for accessing and configuring the functions for communication with an external interface, the cryptographic co-processor for the Triple-DES, the FameXE co-processor for the basic arithmetic functions for executing the asymmetrical cryptographic functions, the RNG and the chip configuration.

Representation of the data to be signed (Representation of the DTBS) : Data sent by the SCA to the TOE for signature and bearing:

(a) A DTBS hash value or;
(b) An intermediate hash value of a first DTBS portion and a remaining

DTBS portion or;

(c) The DTBS.

The SCA indicates to the TOE the case of DTBS representation notwithstanding implicit indication. The hash value in case (a) or the intermediate hash value of case (b) is calculated by the SCA. The hash value in case (b) or the intermediate hash value of case (c) is calculated by the TOE.

User Role : Defines the rights that are associated to a user shouldering a given role. The user is authentified according to his role.

Secret : Cryptographic keys or reference value for authentifying a user based on the verification of their PIN Code (i.e. RAD)

SSCD Supply Service : A service that prepares and provides an SSCD to its members.

Signatory : A person that holds an SSCD and who acts either on their own behalf or that of the legal entity or natural person that they represent (defined in Directive [1], article 2.3).

Advanced Electronic Signature : (defined in directive [1], article 2.2). An electronic signature that fulfils the following requirements, it:

(a) is linked solely to the signatory;
(b) allows for signatory identification;
(c) is created by means that the signatory may keep under his exclusive control;
(d) is linked to data to which it is linked in such a way that any subsequent data modification shall be detectable.

Qualified electronic signature : An advanced signature based on a qualified certificate and created by a secure signature creation device in compliance with Directive [1], article 5, paragraph 1.

SOF- High (SOF-high) : A level of the resistance of a TOE function such as the analysis displays that the function concerned provides adequate protection from a deliberately planned or organized TOE security violation by attackers with a high attack potential.

Subject : An active entity performing operations on the objects for the benefit of a user or as part of the TOE.

Signature Creation System (SCS) : A comprehensive system that creates an electronic signature. The signature creation system is comprised of the SCA and the SSCD.

User : An entity (human or external IT user entity) outside of the TOE that interacts with the TOE.

Domain Authority : User responsible for administration of a domain in the file architecture of the Morpho-Citiz 32 card.

1.7 GLOSSARY

CA	:	Certification Authority
AEAD	:	Agency for Electronic Administration Development
ADF	:	Application Directory File
ARR	:	Access Rules References
APDU	:	Application Protocol Data Unit
ATR	:	Answer To Reset
CC	:	Common Criteria
CGA	:	Certification Generation Application
CMD/RSP	:	Command / Response
CSP	:	Certification Service Provider
CVC	:	Certificate Verifiable by a Card
DAC	:	Data Access Conditions
DES	:	Data Encryption Standard
DF	:	Directory File
DFA	:	Differential Fault Analysis
DH	:	Diffie-Helmann
DPA	:	Differential Power Analysis
DRNG	:	Deterministic RNG
DTBS	:	Data To Be Signed
EAL	:	Evaluation Assurance Level
EF	:	Elementary File
EV	:	Electronic Value
FCI	:	File Control Information
IAS	:	Identification Authentification Signature
MF	:	Master File
OTP	:	One Time Programmable
PIN	:	Personal Identification Number
RAD	:	Reference Authentication Data
RNG	:	Random Number Generator
RSA	:	Rivest Shamir Adelman
SOF	:	Strength of function
SCA	:	Signature-Creation Application
SCD	:	Signature-Creation Data
SDO	:	Signed Data Object
SM	:	Secure Messaging
SPA	:	Simple Power Analysis
SSC	:	Secure Signature Creation
SSCD	:	Secure Signature-Creation Device
ST	:	Security Target
SVD	:	Signature-Verification Data
IT	:	Information Technology
TOE	:	Target Of Evaluation
TSF	:	TOE Security Functions
TSP	:	TOE Security Policy
VAD	:	Validation Authentication Data

2. TOE DESCRIPTION

2.1 PRODUCT TYPE

The Morpho-Citiz 32 card is a "smart card" type product composed of the following material and software elements:

- Embedded software designed by Sagem Défense Sécurité.
- An integrated circuit (IC) (dedicated material and software) designed by Philips Semiconductors Plc bearing reference P5CC036V1. This component was assessed according to German assessment methods and security certification of the information technology in compliance with protection profile **[R5 – BSI0002]**. The assurance level is EAL5 augmented by assurance requirements ALC_DVS.2, AVA_VLA.4 and AVA_MSU.3. The component security target is described in the document **[R14 – HWST]**.
- A cryptographic library designed by the Philips Semiconductors Plc. This library is identified by the name “Crypto Library on SmartMX.” It is assessed according to German assessment methods and security certification of the information technology in compliance with protection profile **[R5 – BSI0002]** and in composition with the component assessment. The assurance level is EAL4 augmented by assurance requirements ADV_IMP.2, ALC_DVS.2, AVA_VLA.4 and AVA_MSU.3. The cryptographic library security target is described in document **[R15 – CLST]**.

2.1.1 Embedded Software Architecture

The embedded software on the Morpho-Citiz 32 card is broken down into software blocks that perform the following functions:

- Data management functions ("user" and secrets data);
- Management functions for handling "user" authentifications;
- Management functions of secure electronic signature services;
- Initialisation and personalization function of the Morpho-Citiz 32 card.

The entire collection of block software is instantiated for performing the following applications:

- The initialisation and personalization application of the **[R8 – IPA]** card (noted hereinafter as “IPA”) in compliance with specifications **[R8 – IPA]**. This application is invalidated in the user phase;
- The IAS-eGOV application is present on the Morpho-Citiz 32 card in user phase (phase 7), in compliance with **[R9 – E-ADMIN]** specifications. It performs IAS type services responding to the electronic administration needs. The IAS-eGOV application may be instantiated several times;

Finally, the application manager dispatches the commands towards the application concerned and maintains the security function in the use of the card’s functions between the various pending applications that solicit it.

The general architecture of the Morpho-Citiz 32 card is displayed in Figure 1.

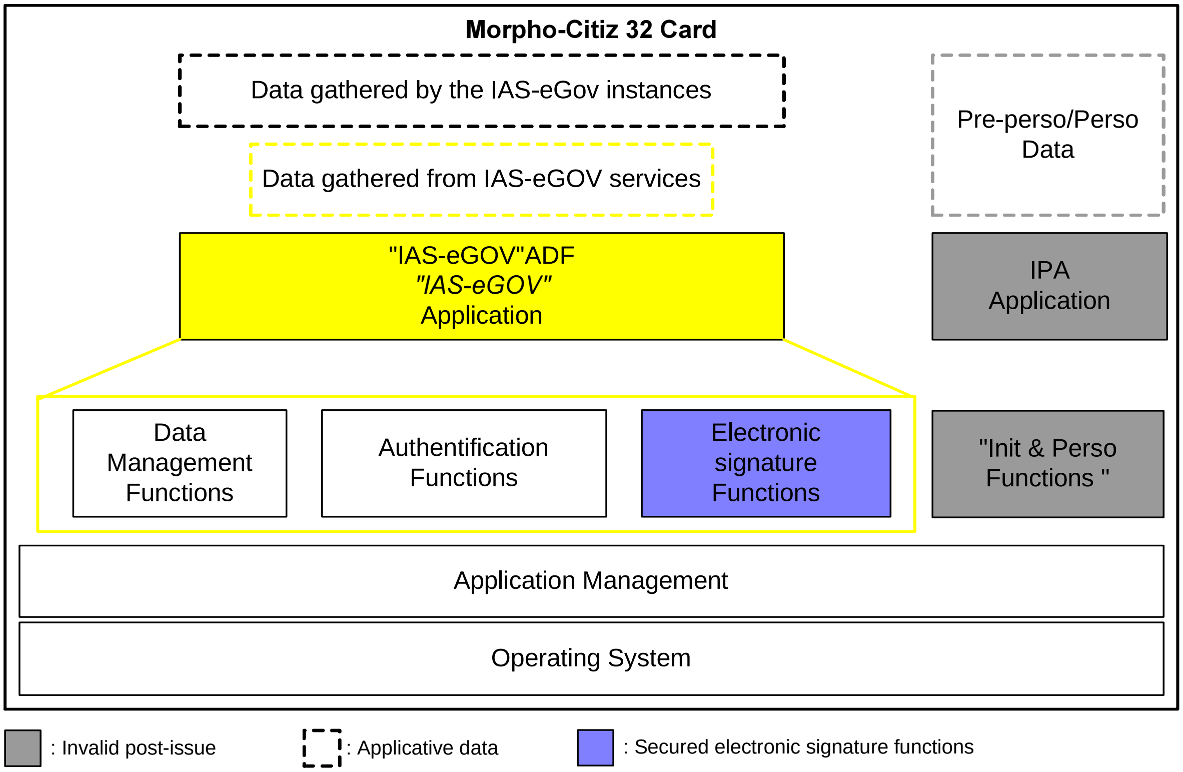
Morpho-Citiz 32 Card
Data gathered by the IAS-eGov instances
Data gathered from IAS-eGOV services
Pre-perso/Perso Data
"IAS-eGOV"ADF
"IAS-eGOV"
Application
IPA Application
Data Management Functions
Authentification Functions
Electronic signature Functions
"Init & Perso Functions "
Application Management
Operating System
: Invalid post-issue
: Applicative data
: Secured electronic signature functions

Figure 1: Description of the card Morpho-Citiz 32 architecture.

2.1.2 Services of the IAS-eGOV application

The IAS-eGOV application performs bundle services via the commands in compliance with **[R9 – E-ADMIN]** available solely in the user phase. The access to these services depends upon the user's role, the condition of the Morpho-Citiz 32 card and the condition of the application performing the service.

User Data Management Service:

This service is performed by the IAS-eGOV application on the data managed by the application. It performs all data management operations and manages the secrets accessible to an authorized user by relying on functions described in chapter 2.1.3.

User Authentification Service:

This service is performed by the IAS-eGOV application on data managed by the application.

The IAS-eGOV application performs the authentification service by relying on the authentification functions described in chapter 2.1.3.

Secure Electronic Signature Service:

This service is performed by IAS-eGOV application on the data managed by the application.

In order to perform the secure electronic signature service, IAS-eGOV application relies on the secure electronic signature functions described in chapter 2.1.3.

2.1.3 Functional Blocks

The following chapters describe the functions of the Morpho-Citiz 32 card that handle data management, electronic signature and authentification on behalf of the IAS-eGOV application.

2.1.3.1 Data Management

Data stored on the Morpho-Citiz 32 card is organized in a tree of directories and files, in compliance with standard **[R12 – 7816 – 4]**.

Objects supported by the Morpho-Citiz 32 card:

The Morpho-Citiz 32 card supports the following objects:

- **The directories and the files** creating the data structure;
- **The TLV objects** contained in the directories (in the same way as the files) but accessible by a name system;
- **The secrets** in which the cryptographic keys and the PIN codes are stored.

Access to objects:

Any object (directory, file, secret, TLV) subject to access conditions may only be accessed upon verification of these conditions.

The verification of access conditions is performed by comparing the access conditions defined in the DAC of the object with the current status of the security card.

Access conditions to an object are associated with authentification secrets (PIN Code, authentification key) or with the establishment of a channel of trust (SMC, SMI). Thus, when a user is authentified or a channel of trust is established, this information is memorized in the security card status. The security card status is updated when the user authentification is no longer valid or when the security canal is interrupted.

Data Management Functions:

Data management functions perform the management services of the data structure of the IAS-eGOV application.

- **Directory creation**: Allows directory creation (DF file type).
- **File creation**: Allows the creation of EF type files.
- **Directory deletion**: Allows directory deletion (DF file type).
- **File deletion**: Allows EF file type deletion.
- **Management of a file/directory life cycle:** Allows the authorized user to modify the status of a file/directory during its life cycle, except for MF.
- **Update / File data writing**: Allows writing of data into a selected file.
- **File data reading**: Allows reading of data in a selected file.
- **Creation of a TLV:** Allows TLV creation.
- **Update / Writing of data in a TLV**: Allows writing and deletion of data in a selected TLV object.
- **Reading of TLV data:** Allows reading of data in a selected TLV object.
- **Life cycle secret management:** Allows the authorized user to modify the status of a secret in its life cycle.

- **Secret release:** Allows release of a PIN Code or a cryptographic key found in the "Blocked," state.
- **Secret creation**: Allows secret creation.
- **Update / Secret writing**: Allows updating of a PIN Code or of a cryptographic key.
- **Reading of information linked to a secret**: Allows reading of information associated with a secret or to public keys.
- **Bi-key generation**: Allows generation of a bi-key for authentification, signature or asymmetrical confidentiality.

2.1.3.2 User Authentification

Nature of the authentification:

The authentification functions perform services of user authentification of the IAS-eGOV application User authentification is based on the role ensured by a user when accessing application services. User authentification operations are performed according to different types of secrets associated with the supported roles, i.e.:

- A so-called "PIN authentification code" for authentifying the bearer for access to data and to the creation of a qualified electronic signature;
- A so-called "PUK authentification code" for authentifying the user for the deblocking operation of the PIN Code to which the PUK code is associated;
- A symmetrical key for authentifying the user (without SM implementation) that allows access to data management;
- A symmetrical key (stored on the card) for mutual authentification allowing updating of card data via the establishment of a channel of trust;
- A CVC type certificate + response to a challenge provided to the card that authentifies the user via the verification of the certificate from a card root key for accessing data management;
- A CVC or X509 type certificate allowing card authentification;

Authentification functions:

These are user authentification functions of the IAS-eGOV application These functions help resolve the access conditions of objects of the Morpho-Citiz 32 card.

- **Verification of the PIN Code/PUK**: Allows authentification of the bearer or of the associated PUK code;
- **Mutual symmetrical authentification**: Allows mutual card/user authentification according to a symmetrical plan and based on the utilization of 112-bit TDES keys;
- **External symmetrical authentification**: Allows the authentification of a user on the basis of 112 bit TDES keys;
- **Mutual asymmetrical-DH authentification:** Allows mutual card/user authentification relying on a Diffie-Helmann (DH) protocol and based on CVC (RSA key up to 2048 bits) certificates;
- **External asymmetrical authentification**: Allows user authentification based on CVC user certificates (RSA key up to 2048 bits);

- **Internal asymmetrical authentification**: Allows card authentification based on a CVC or X509[1] "card" certificate (RSA key up to 2048 bits);

2.1.3.3 Electronic Signature

These functions create electronic signatures and manage data implemented within the framework of this electronic signature for the **IAS-eGOV application** user.

SCD/SVD Management functions:

- SCD/SVD generation;
- SCD/SVD destruction;
- SCD loading, storage and utilization.

Signature Functions:

- Electronic signature creation

"qualified signature" / "non-qualified signature ":

The Morpho-Citiz 32 card performs the electronic signature service according to two functioning modes:

- The "qualified signature" mode for which compliance with protection profiles **[R3 – SSCD T2]** and **[R4 – SSCD T3]** is required;
- The "non-qualified signature" mode for which the requirements concerning the utilization qualified certificates such as those defined in § 3.4.2 of the organizational policies are not applicable. Compliance with protection profiles **[R3 – SSCD T2]** and **[R4 – SSCD T3]** is thus not required;

The mode is defined by the utilization framework of the Morpho-Citiz 32 card and especially at the time of its personalization, i.e. upon loading of the qualified- or non-qualified certificates.

2.1.3.4 Confidentiality – Integrity

"Secure Messaging" channel of trust functions:

Establishment of a channel of trust requires prior mutual authentification between the card and the IT product communicating with the card. This mutual authentification may be done via symmetrical (mutual) or asymmetrical authentification. The channel of trust functions perform the processes associated with the establishment and management of a channel of trust. This channel of trust supports the following services:

- **(SMI) Integrity**: Integrity on the commands and responses exchanged between the Morpho-Citiz 32 card and an IT product.
- **(SMC) Confidentiality**: Confidentiality on the commands and the responses exchanged between the Morpho-Citiz 32 card and an IT product.

On the basis of these two services, there are two protection modes on the CMD/RSP exchanged during a channel of trust session:

- Integrity protection: SMI;
- Integrity and confidentiality protection: SMI and SMC;

[1] the X 509 certificates are used solely within a framework of card authentification for SSL sessions and are thus not interpreted by the Morpho-Citiz 32. card.

Confidentiality Functions:

The Morpho-Citiz 32 card institutes encryption functions that protect the confidentiality of secrets and sensitive data. These functions are:

- **Asymmetrical secret decryption**: Allows decryption of an encrypted secret with the help of an RSA secret decryption key;
- **Symmetrical data encryption**: Allows data encrypting within the framework of an SM with the help of a TDES data encryption key;

Integrity function:

The Morpho-Citiz 32 card implements a calculation integrity function ensuring the integrity of secrets and sensitive data. This function uses MAC for calculating /verifying (MAC Retail) data integrity.

2.2 PRODUCT LIFE CYCLE

The life cycle corresponds to a "smart card" product life cycle. It is broken down into 7 phases:

Phase 1 ***Development of the smart card embedded software***

Sagem Défense Sécurité is in charge of the development of the smart card integrated software and of the specification requirements for the initialization of the integrated circuit.

Phase 2 ***Integrated Circuit (IC) Development***

Philips Semiconductors Plc designs the IC, develops the dedicated software IC and transmits the information, the software and the tools to the developer's embedded software (**Sagem Défense Sécurité**), by protected verification and delivery procedures. From the integrated circuit, the dedicated software and the embedded software, they build the integrated circuit smart card data base, indispensable for creating the integrated circuit mask.

Phase 3 ***Manufacture and test of the integrated circuit***

Philips Semiconductors Plc is in charge of the production of the integrated circuit which occurs in three principal steps: manufacture, test and initialisation of the integrated circuit.

Phase 4 ***Encapsulation and test of the integrated circuit***

The **integrated circuit packaging manufacturer** in charge of packaging (encapsulation) and testing of the integrated circuit.

Phase 5 ***Smart card product Finish***

The **smart card manufacturer** in charge of finishing and testing the smart card.

Phase 6 ***Smart card personalization***

The **personalizer** is in charge of personalizing the smart card and performing final tests.

Phase 7 ***Smart card use***

The **smart card issuer** is in charge of product delivery to the **end** user, as well as for the end of the life cycle.

The role of the embedded software designed in phase 1 is to check and protect the TOE during phases 4 to 7 (product use).

The overall security requirements of the TOE stipulate that the threats posed in subsequent phases must be anticipated during the development phase. That is why this security target addresses the functions implemented in phases 4 to 7 but that remain developed during phase 1.

Figure 2: The smart card product describes the smart card product life cycle.

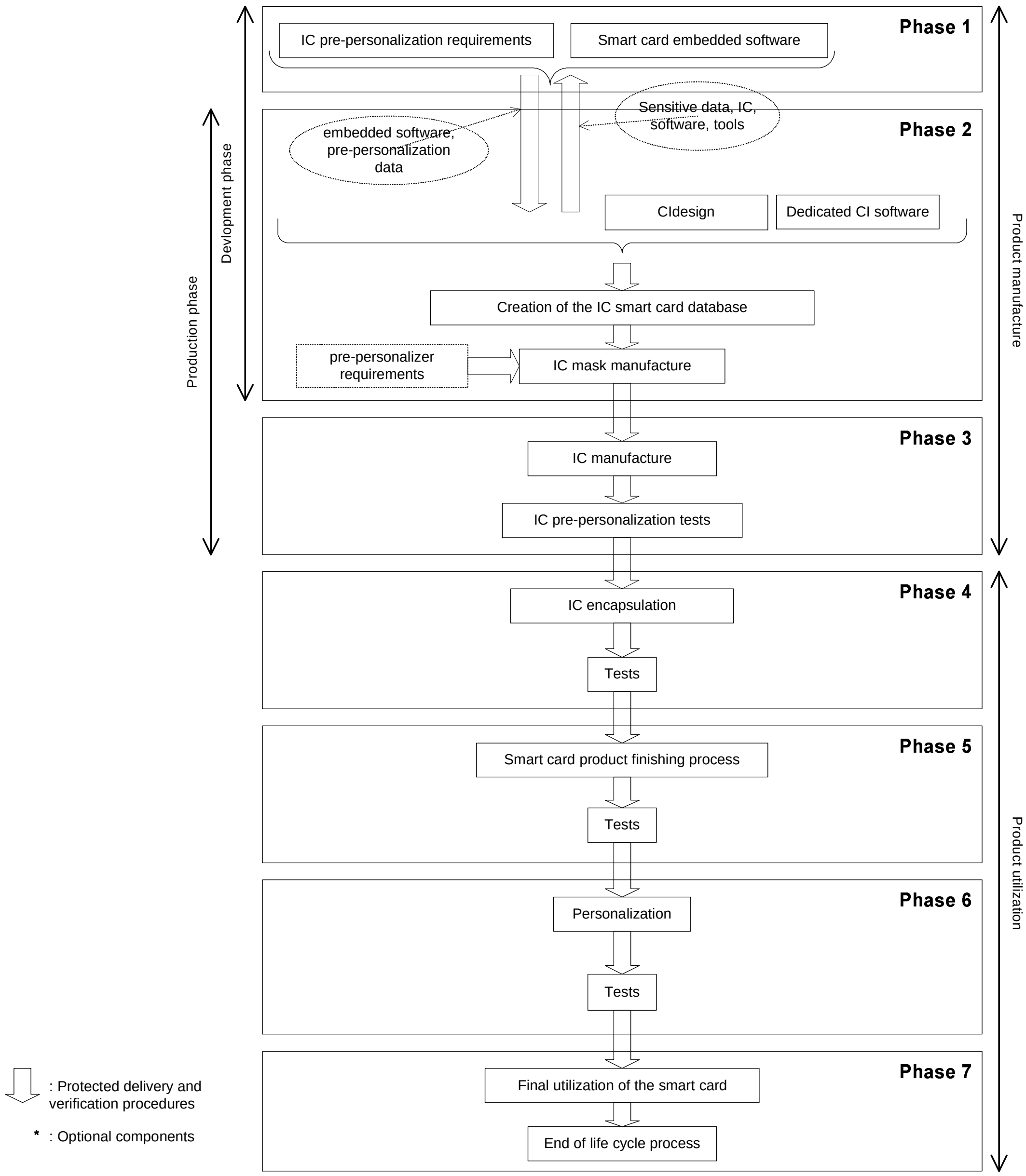
Phase 1
IC pre-personalization requirements
Smart card embedded software
Phase 2
embedded software, pre-personalization data
Sensitive data, IC, software, tools
CIdesign
Dedicated CI software
Creation of the IC smart card database
pre-personalizer requirements
IC mask manufacture
Phase 3
IC manufacture
IC pre-personalization tests
Phase 4
IC encapsulation
Tests
Phase 5
Smart card product finishing process
Tests
Phase 6
Personalization
Tests
Phase 7
Final utilization of the smart card
End of life cycle process
Devlopment phase
Production phase
Product manufacture
Product utilization
: Protected delivery and verification procedures
* : Optional components

Figure 2: The smart card product life cycle

The software and material module is designed during phases 1 to 3. However, the IAS-eGOV application is designed in phase 1.

The development of the application includes the phases of specification, design, coding, testing and qualification.

These different phases may be implemented in different places. Procedures must be set up for processing TOE delivery and must be applied within each phase as between each phase. This includes any form of delivery carried out from phase 1 through phase 6, including:

- Intermediate delivery of the TOE or of the TOE currently being manufactured within a given phase;
- Delivery of the TOE or of the TOE currently being manufactured from one phase to the following phase;
- Delivery of the code to the caster together with delivery of the initialisation and personalization parameters.

2.3 TOE PRESENTATION

The target of evaluation (TOE) described in this chapter is the IAS-eGOV application. This TOE is referred to hereinafter as the "IAS-eGOV application"

2.3.1 TOE Limits

The TOE is the IAS-eGOV application of the Morpho-Citiz 32 card. It is composed of the following elements:

- The operating system;
- The manager application;
- The embedded software functions of the Morpho-Citiz 32 card implemented in the IAS-eGOV application services;

The TOE is presented in the outline of the Figure 3.

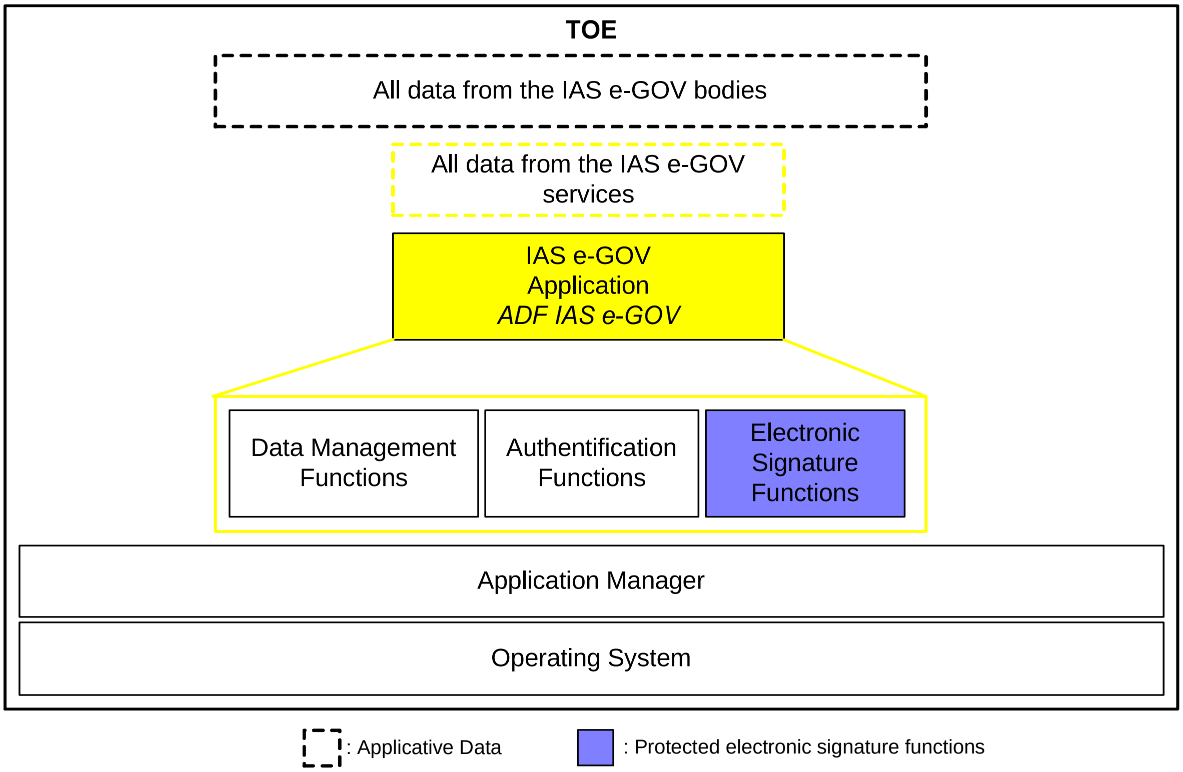
TOE
All data from the IAS e-GOV bodies
All data from the IAS e-GOV services
IAS e-GOV Application ADF IAS e-GOV
Data Management Functions
Authentification Functions
Electronic Signature Functions
Application Manager
Operating System
: Applicative Data
: Protected electronic signature functions

Figure 3: Services of the TOE

2.3.2 TOE Description

The IAS-eGOV application ensures the services described in chapter 2.1.2 on the data managed by the application.

The following data is linked to the IAS-eGOV application:

- The collective data, especially the data to be signed and the certificates to be stored on the card;
- All data pertaining to the cryptographic keys associated with the IAS-eGOV application services as well as the PIN code(s) used for authentifying the bearer and PUK code(s);
- All data pertaining to the bearer's identity;
- "Card" Certificates;
- The authentification card private key and the associated DH parameters;
- The data linked to the physical support of the card such as the serial number;

The IAS-eGOV application also performs the processing of protected electronic signatures, i.e.,:

(1) Generation of the corresponding SCD and SVD or loading of SCD;

(2) Creation of qualified signatures:

a. after having allowed the data to be signed (DTBS) to be correctly displayed by the adapted environment;

b. by using control functions that are, according to **[R7 – Algo]**, declared as being adapted to qualified electronic signatures;

c. after the signatory's adapted authentification by the TOE;

d. by using an adapted cryptographic signature function that uses adapted cryptographic parameters declared as such according to **[R7 – Algo]**.

The TOE preserves the secret of the SCDs. In order to avoid unauthorized SCD utilization, the TOE allows a user authentification and access control. The TOE employs IT measures for taking on a web of trust towards a protected human interface device.

The TOE keeps the RAD for verifying the VAD provided by the signatory.

The TOE is initialized for a utilization by the signatory when, as this latter may choose:

(1) importing an SCD;

(2) generating an SCD/SVD pair.

Solely the legitimate signatory may utilize the SCD during the signature creation process and during the validity of the SCD/SVD pairs.

The TOE stores the SCD and may export the SVD. The SVD corresponding to the signatory SCDs are included in the signatory's certificate by the certification service providers (CSP). The TOE destroys the SCDs that are no longer used for generating signatures.

In the user phase, the TOE authorizes the creation of new SCD/SVD pairs. The preceding SCD must be destroyed prior to the creation of new SCD/SVD pairs.

The user of the electronic signature creation service of the TOE presents the data to be signed (DTBS) to the signatory, and prepares the DTBS representation that the signatory wishes to sign for performing the cryptographic signature function. The TOE returns a qualified electronic signature.

SCD/SVD Management in the TOE life cycle:

Figure 4 [1] describes the TOE life cycle in its SSCD function.

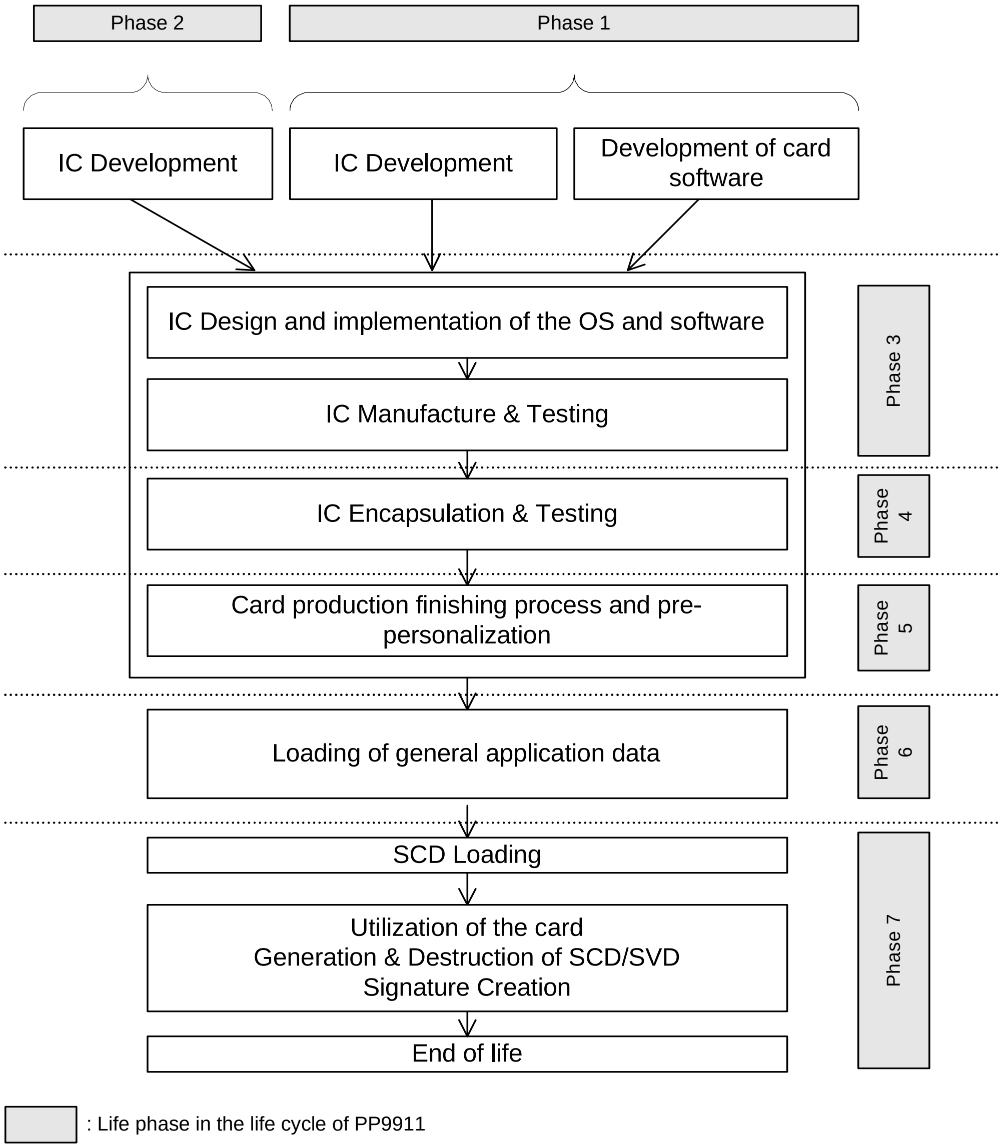
Phase 2
Phase 1
IC Development
IC Development
Development of card software
IC Design and implementation of the OS and software
IC Manufacture & Testing
IC Encapsulation & Testing
Card production finishing process and pre-personalization
Loading of general application data
SCD Loading
Utilization of the card
Generation & Destruction of SCD/SVD
Signature Creation
End of life
Phase 3
Phase 4
Phase 5
Phase 6
Phase 7
: Life phase in the life cycle of PP9911

Figure 4: SSCD life cycle

2.4 THE TOE ENVIRONMENT

2.4.1 Description of its environment:

With regards to TOE, four types of environments are defined:

- Development and manufacturing (phase 1 to 4);
- Pre-personalization (phase 5) and personalization (phase 6) of the Morpho-Citiz 32 card;
- User (phase 7) during which the TOE is operational;
- End of life of the TOE (phase 7) during which the TOE is rendered non-operational.

2.4.2 TOE logical phases

During its manufacture and operation, the TOE goes through several phases of logical life. These phases are classed according to a controlled logical sequence. The passage of a phase to the subsequent phase shall be carried out under the control of the TOE.

IC Configuration	Embedded Software Phases	Phases	Auditing Authority (Role)
Test	-	3	-
User	Initialisation	4 and 5	Pre-personalizer (administrator)
User	Personalization	6	Personalizer (administrator)
User	End user	7	Domain Authority and Issuer (administrator)
User	End of life	7	Issuer (administrator)

Table 1: Logical phases of the IAS-eGOV application

The configuration of the TOE environment is determined by the configuration of the integrated circuit (test or user of the integrated circuit), and by the life cycle of the TOE environment (pre-personalization, personalization, end user, end of life) provided by the embedded software.

Once the configuration is determined, the TOE may not return to a preceding configuration. The different stages are specified in Table 1, and only the authorized administrator may implement the passage of a phase to the following phase.

For the IAS-eGOV application, the passage from the "Non-Active” state to the "Active" state is performed subsequent to the initialisation and personalization of the Morpho-Citiz 32. card. The initialisation and personalization operations are performed under the control of the pre-personalizer and of the personalizer who act on the TOE as administrator via the IPA application commands.

In the user phase, the user may use the IAS-eGOV application. services. During the end of life phase, the TOE is invalidated, meaning that all commands are rejected.

Regardless of the life phase, the life phase change is irreversible.

2.5 USERS AND ROLES

TOE users are the entities, personal or material, having an interaction with the TOE via its external interfaces. The table below presents the different TOE users and specifies the roles that are associated with them.

2.5.1 "Generic" Users

Inserter : User who intervenes in the insertion phase and ensures TOE administration. He especially provides an insertion number and a serial number. (Phase 4 and 5)

Personalizer : User who intervenes in the personalizing phase and ensures TOE administration. He invalidates his own access to administration services at the end of the personalization phase by deactivation of the manufacturing key. (Phase 6)

Issuer : User who intervenes in the user phase. He may create/delete domains for an application. He also creates and updates secrets for the domains and the applications he accesses. He may also deactivate/activate an application. (Phase 7)

Domain Authorities : User who manages one or several domains. He may create/delete domains for a father domain. He also creates updates secrets for the domains he accesses. he may also deactivate/activate a domain if this latter is not an application. (Phase 7)

Bearer : The Morpho-Citiz 32 card bearer that benefits from IAS-eGOV application. services. (Phase 7)

2.5.2 Protected electronic signature: Users

In order to ensure compliance with protection profiles **[R3 – SSCD T2]** and **[R4 – SSCD T3]**, the following users are defined for the secure electronic signature services:

S.USER : TOE end user that may be identified as S.Admin or S.Signatory (Phase 7)

S.Admin : User that is in charge of initializing the TOE, its personalization or other TOE administrative functions. (Phase 7)

S.Signatory : User that keeps the TOE and uses it on his own behalf or for that of a physical or legal person that they represent. (Phase 7)

Threatening agent defined for the protected electronic signature services:

S.OFFCARD : Attacker. Human or process acting on its own behalf and located outside of the TOE. The S.OFFCARD attacker's primary goal is to access sensitive application information. The attacker has a **high potential attack level and knows no secret**.

3. THE TOE SECURITY ENVIRONMENT

3.1 THE PROPERTY TO BE PROTECTED

The list of property to be protected by the TOE is comprised of a group of functions and data that may be grouped as follows:

- The protective functions of the IAS-eGOV application;
- User data;
- TSF data;

To which we may add the embedded software including the specification documents, source code and associated design documents.

3.1.1 Functions of the IAS-eGOV application

The functions are supported by the executable code stored in ROM memory.

Identify	Functions
FCT.1	External asymmetrical authentification
FCT.2	External asymmetrical authentification
FCT.3	External symmetrical authentification
FCT.4	Internal symmetrical authentification
FCT.5	Mutual symmetrical authentification
FCT.6	Data Encryption/decryption
FCT.7	Mutual asymmetrical authentification
FCT.8	Seal calculator, on external data
FCT.9	Creation of an electronic signature
FCT.10	Generation of bi-key authentification
FCT.11	Generation of bi-key signature (SCD/SVD)
FCT.12	Addition of a cryptographic key
FCT.13	Establishment of a session key
FCT.14	Asymmetrical secret decryption
FCT.15	Activation of a cryptographic key
FCT.16	Unlocking of a cryptographic key
FCT.17	Activation of a bearer code
FCT.18	Unlocking of the bearer code
FCT.19	Verification of the bearer code
FCT.20	Updating of bearer code
FCT.21	Creation of files or directories
FCT.22	Deletion of file/directory
FCT.23	Writing/reading in a file or a TLV object with controlled access

Table 2: List of sensitive functions

3.1.2 User data

The data used is information stored within the TOE. The users may intervene on this data within the framework of the security policy (TSP). However, the TSF gives no particular meaning to this data for which the audit trail is either protected or protected with read/write access restricted to an authorized user. They are displayed in the following table:

Identify	Data	Protection
D.USE.1	Freely accessible read-only data, write protected	Audit trail protection writing restricted to the authorized user
D.USE.2	Read & write protected data	Audit trail protection and reading restricted to the authorized user
D.USE.3	Electronic signature data	Audit trail protection

Table 3: "User" sensitive data list

3.1.3 TSF data

TSF data is information used by the TSF for creating the security policy (TSP). TSF data may be modified by TSP-authorized users. This data must feature either audit trail protection or both audit trail protection and a confidentiality element signalling. It is displayed in the following table:

Identify	Data	Protection
D.TSF.1	TDES keys for decryption of secrets and encryption/decryption of external data	Audit trail and confidentiality
D.TSF.2	Private RSA Keys and DH parameters for internal and external asymmetrical authentifications	Audit trail and confidentiality
D.TSF.3	Private RSA Keys for decryption of secrets	Audit trail and confidentiality
D.TSF.4	Certificates and associated public keys	Audit trail and confidentiality
D.TSF.5	TDES session keys used for confidentiality (K_{ENC}) and Audit trail (K_{MAC}) in SM sessions	Audit trail and confidentiality
D.TSF.6	TDES Audit trail keys for data exportation and importation	Audit trail and confidentiality
D.TSF.7	Confidential bearer codes (PIN reference)	Audit trail and confidentiality
D.TSF.8	Deblocking codes for reference PIN codes (PUK code)	Audit trail and confidentiality
D.TSF.9	TOE security attributes	Audit trail and confidentiality

Table 4: TSF sensitive data list

3.1.4 Protected electronic signature: Definition of SSCD property

TOE property for secure electronic signature services are those defined in protection profiles **[R3 – SSCD T2]** and **[R4 – SSCD T3]**, i.e.:

SCD : Private key used for performing an electronic signature operation (SCD confidentiality shall be preserved).

SVD : Public key linked to the SCDs and used for performing electronic signature verification (SVD integrity during exportation shall be preserved).

DTBS[2] : Collective data or their representation to be signed (its audit trail must be preserved).

VAD : PIN Code entered by the bearer for performing a signature operation (VAD confidentiality and authenticity as required by the authentification method are necessary)

RAD : Reference PIN code used for identifying and authentifying the bearer (RAD audit trail and confidentiality must be preserved)

SSC : Secure signature creation function of the Morpho-Citiz 32 card using the SCD: (the quality of the function must be preserved in such a way as to allow it to participate in the electronic signatures validity).

SIG : Electronic signature: non-falsification electronic signatures must be preserved.

[2] As well as the DTBS representation.

3.2 ASSUMPTIONS

Table 5 presents the assumptions under consideration for the present TOE and their correspondence with protection profiles **[R2 – 9911]**, **[R3 – SSCD T2]** and **[R4 – SSCD T3]** as well as the target **[R15 – CLST]**.

TOE Assumptions	PP 9911	PP SSCD type 2	PP type3 SSCD	ST Crypto Library
A.CGA		A.CGA	A.CGA	
A.SCA		A.SCA	A.SCA	
A.SCD_Generate		A.SCD_Generate		
A.DEV_ORG	A.DEV_ORG			
A.DLV_PROTECT	A.DLV_PROTECT			A.Process-Card
A.DLV_AUDIT	A.DLV_AUDIT			A.Process-Card
A.DLV_RESP	A.DLV_RESP			A.Process-Card
A.USE_TEST	A.USE_TEST			
A.USE_PROD	A.USE_PROD			A.Process-Card
A.USE_DIAG	A.USE_DIAG			
A.Plat-Appl				A.Plat-Appl
A.Resp-Appl				A.Resp-Appl

Table 5: ST/PP Correspondences – assumptions for the TOE

3.2.1 Assumptions defined in [R15 – CLST]

A.Plat-Appl *Utilization of the material platform*
The smart card embedded software is designed such that the requirements stemming from the following documents are fulfilled: (i) the smart card integrated circuit guides (reference to the AGD Common Criteria insurance class) such as the material "data sheet," and the material application notes, and (ii) the conclusions of the assessment reports of the smart card integrated circuit pertaining to the smart card embedded software.

It must be emphasized that the smart card embedded software special requirements are often vague prior to consideration being given to a specific attack scenario during the smart card integrated circuit vulnerability analysis (AVA_VLA). Consequently, such results derived from the smart card integrated circuit assessment (such as those contained in the Technical Evaluation Report (TER) must be provided to smart card embedded software developers in an appropriate and authorized form and taken into consideration during software assessment. This also holds true for the additional tests required for combining the material and software. The smart card integrated circuit assessment must be completed prior to commencing assessment of the smart card embedded software.
The assessment of the smart card portion of the TOE may be conducted prior to and independently of the assessment of the smart card embedded software.

A.resp-Appl *User data processing*
All user data is kept by the smart card embedded software. Consequently, it shall be presumed that the user sensitive data, especially the cryptographic keys, are processed by the embedded software in the smart card as defined for the specific application context. Details must be specified within the application context.

3.2.2 Assumptions defined in [R2 – 9911]

3.2.2.1 Assumptions in phase 1

A.DEV_ORG
Procedures that handle technical, physical, and organizational measures related to personnel with regards to confidentiality and the audit trail of the smart card embedded software (ex.: source code and all associated documents) and designer proprietary microcircuit information (tools, software, documentation…) must exist and be applied during software development.

3.2.2.2 Delivery process assumptions (phases 4 to 7)

Procedures must guarantee the control of the delivery process and storage of the target of evaluation as well as compliance with these objectives as described in the following assumptions:

A.DLV_PROTECT
Upon delivery and storage, procedures must ensure material protection of the TOE as well as protection of information relative to the TOE.

A.DLV_AUDIT
Procedures must ensure that corrective action is executed in case of dysfunction of the delivery and storage process.

A.DLV_RESP
Procedures must ensure that the people handling the delivery procedure are qualified to do so.

3.2.2.3 Assumptions in phases 4 to 6

A.USE_TEST
It is presumed that the appropriate functionality tests of the target of evaluation are implemented in phases 4, 5 and 6.

A.USE_PROD
It is presumed that security procedures are implemented during all manufacture and test operations in phases 4, 5 and 6 in order to preserve the confidentiality and the audit trail of the target of evaluation and of its manufacture and test data (in order to avoid any possibility of copying, modification, retention, theft or unauthorized use).

3.2.2.4 Assumptions in phase 7

A.USE_DIAG
It is presumed that secure communication protocol and secure procedure are used between the smart card and the terminal.

3.2.3 Assumptions defined in [R3 – SSCD T2] and [R4 – SSCD T3]

Protection profile hypothesis **[R3 – SSCD T2]:**

A.SCD_Generate *Reliable generation of SCD/SVD*
If a party other than the signatory generates the SCD/SVD pair for a signatory, then:
(a) this party shall use a SSCD for SCD/SVD generation;
(b) the confidentiality of the SCD shall be preserved until the SCD falls under the signatory's exclusive control;
(c) the SCD shall not be used for signature creation until the SCD falls under the signatory's exclusive control;
(d) SCD/SVD generation shall be exclusively called upon by authorized users;
(e) the Type 1 SSCD shall assure the authenticity of the SVD that he created and exported.

Assumptions common to protection profiles **[R3 – SSCD T2] and [R4 – SSCD T3]**:

A.CGA *A reliable certification generation application*
The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by a CSP advanced signature.

A.SCA *A reliable signature creation application*

The signatory shall only use a reliable SCA. The SCA generates and sends the DTBS representation data that the signatory wishes to sign in an appropriate form for signature by the TOE.

3.3 THREATS

Table 6 presents the threats considered in the present TOE and their correspondence with protection profiles **[R2 – 9911]**, **[R3 – SSCD T2]** and **[R4 – SSCD T3]** as well as the target **[R15 – CLST]**.

Threats for the TOE	PP 9911	PP type 2 SSCD	PP SSCD 3	ST Crypto Lib
T.Hack_Phys		T.Hack_Phys	T.Hack_Phys	
T.SCD_Divulg		T.SCD_Divulg	T.SCD_Divulg	
T.SCD_Derive		T.SCD_Derive	T.SCD_Derive	
T.Sig_Forgery		T.Sig_Forgery	T.Sig_Forgery	
T.Sig_Repud		T.Sig_Repud	T.Sig_Repud	
T.SVD_Forgery		T.SVD_Forgery	T.SVD_Forgery	
T.DTBS_Forgery		T.DTBS_Forgery	T.DTBS_Forgery	
T.SigF_Misuse		T.SigF_Misuse	T.SigF_Misuse	
T.CLON	T.CLON			T.Phys-Probing
T.DIS_INFO	T.DIS_INFO			
T.DIS_DEL	T.DIS_DEL			
T.DIS_ES1	T.DIS_ES1			
T.DIS_TEST_ES	T.DIS_TEST_ES			
T.T_DEL	T.T_DEL			
T.T_TOOLS	T.T_TOOLS			
T.T_SAMPLE2	T.T_SAMPLE2			
T.MOD_DEL	T.MOD_DEL			
T.MOD	T.MOD			
T.DIS_DEL1	T.DIS_DEL1			
T.DIS_DEL2	T.DIS_DEL2			
T.MOD_DEL1	T.MOD_DEL1			
T.MOD_DEL2	T.MOD_DEL2			
T.DIS_ES2	T.DIS_ES2			T.Leak-Inherent T.Phys-Probing T.Leak-Forced
T.T_ES	T.T_ES			
T.T_CMD	T.T_CMD			T.Abuse-Func
T.MOD_LOAD	T.MOD_LOAD			T.Phys-Manipulation
T.MOD_EXE	T.MOD_EXE			T.Phys-Manipulation
T.MOD_SHARE	T.MOD_SHARE			T.Phys-Manipulation
T.MOD_SOFT	T.MOD_SOFT			T.Phys-Manipulation
T.Malfunction				T.Malfunction
T.RND				T.RND

Table 6: ST/PP Correspondences – threats for the TOE

3.3.1 Threats defined in [R15 – CLST]

T.Malfunction *Faulty functioning due to environmental stress*
An attacker may cause faulty functioning of the TSF or of the smart card embedded software by applying an environmental stress for the purpose of deactivating or modifying the security characteristics or the functions of the TOE. This may be done by using the smart card outside of its normal operating conditions.
In order to take advantage of this, an attacker needs information concerning the operational functioning.

T.RND *Random numbers deficiency*
An attacker may predict or obtain information concerning the random numbers generated by the TOE, for example, with the help of a lack of entropy of random numbers provided.
An attacker may obtain information on the random numbers generated. This could cause a problem if they are used for generating cryptographic keys, for example.
Here, the attacker is presumed to take advantage of the statistical properties of random numbers generated by the TOE without specific knowledge concerning the TOE generator. Dysfunction or premature ageing are also

considered as capable of facilitating acquisition of information regarding random data.
Both the PHILIPS component random numbers generator and that of the cryptographic library are considered here.

3.3.2 Threats defined in [R2 – 9911]

Threats are classified as:

- threats against which specific protection must be integrated into the target of evaluation (class I);
- threats against which specific protection must be integrated into the environment (class II).

3.3.2.1 Partial or total cloning of the unauthorized TOE

T.CLON
The functional cloning of the target of evaluation (total or partial) appears to apply to all phases of the life cycle of the target of evaluation, from phase 1 to phase 7, but only phases 1 and 4 to 7 are discussed here, insofar as the functional cloning of phases 2 and 3 is found solely in the field of application of the protection profile of the smart card microcircuits. Generally, this threat is derived from specific threats combining unauthorized disclosure, modification or theft of property in different phases.

3.3.2.2 Threats in phase 1

During phase 1, three types of threats must be considered:

a) : Threats on the smart card embedded software and its development environment, such as the unauthorized disclosure, modification or theft of the smart card embedded software and/or initialisation data in phase 1.
b) : Threats on the property transmitted by the microcircuit designer to the smart card software developers during the smart card embedded software development phase.
c) : Threats on the smart card embedded software and on the initialisation data transmitted during the delivery process by the smart card software developers to the microcircuit designer.

Unauthorized property disclosure

This type of threat covers the unauthorized disclosure of property by attackers who may have various technical skills, resources and motivations. Such attackers must also possess technical knowledge of the product.

T.DIS_INFO *(type b)*
Unauthorized property disclosure provided by the microcircuit designer to smart card embedded software developers, such as disclosure of sensitive information regarding the microcircuit specification, the conception and technology, the software and tools, as the case arises.

T.DIS_DEL *(type c)*
Unauthorized disclosure of the smart card embedded software and of any supplementary application data, (such as the microcircuits initialisation requirements) during the delivery phase to the microcircuit designer.

T.DIS_ES1 *(type a)*
Unauthorized disclosure of the embedded software (technical or detailed specifications, implementation code) and/or application data (e.g., secret codes, control parameters of the protection system, specifications and implementation of security mechanisms).

T.DIS_TEST_ES *(type a and c)*
Unauthorized disclosure of smart card embedded software test programmes or any other related information.

Theft or unauthorized utilization of property

Potential attackers may have access to the target of evaluation and perform operations without being authorized. For example, such an attacker may personalize, modify or influence the product in such a way as to access the smart card application system.

T.T_DEL *(type c)*
Theft of the smart card embedded software and of any supplementary application data (e.g., the pre-personalization requirements) during the delivery phase to the microcircuit designer.

T.T_TOOLS *(type a and b)*
Theft or unauthorized use of smart card embedded software development tools (e.g., PC, development software, databases)

T.T_SAMPLE2 *(type a)*
Theft or unauthorized use of target of evaluation samples (e.g., microcircuit unsoldered with embedded software).

Unauthorized modification of property

The target of evaluation may be subject to different types of logical or physical attacks that may diminish security. Because of the designated usage for the target of evaluation (its environment may be hostile), the security of the target of evaluation may be circumvented or compromised, thus reducing the security mechanisms of the target of evaluation and deactivating their capacity for managing the security of the target of evaluation. This type of threat includes employing hostile Trojan horses.

T.MOD_DEL *(type c)*
Unauthorized smart card embedded software modification and of any supplementary applicative data (e.g., microcircuit initialisation requirements) during the delivery phase to the microcircuit designer.

T.MOD *(type a)*
Unauthorized modification of the embedded software and/or applicative data or any information related thereto (technical specifications).

3.3.2.3 Threats on deliveries for phase 1 and phases 4 to 6

Threats on the data transmitted during the delivery process from the smart card developers to the microcircuit housing manufacturer, to the finishing process manufacturer or to the personalizer.

These threats are described below:

T.DIS_DEL1
Unauthorized disclosure of applicative data during delivery to the microcircuit housing manufacturer to the manufacturer of the finishing process or to the personalizer.

T.DIS_DEL2
Unauthorized disclosure of applicative data delivered to the microcircuit housing manufacturer, to the manufacturer of the finishing process or to the personalizer.

T.MOD_DEL1
Unauthorized modification of applicative data during delivery to the microcircuit housing manufacturer, to the manufacturer of the finishing process or to the personalizer.

T.MOD_DEL2
Unauthorized modification of applicative data delivered to the microcircuit housing manufacturer, to the manufacturer of the finishing process or to the personalizer.

3.3.2.4 Threats in phases 4 to 7

The threats considered during these phases may be grouped into three types:

- Unauthorized disclosure of property;
- Unauthorized theft or use of property;
- Unauthorized property modification.

Unauthorized property disclosure

This type of threat covers the unauthorized disclosure of property by attackers that may have various technical skills, resources and motivations. Such attackers may also have technical knowledge of the product.

T.DIS_ES2
Unauthorized disclosure of the embedded software and applicative data (such as data protection systems, memory compartmentalization, programmes and cryptography keys).

Theft or unauthorized use property

Potential attackers may have access to the target of evaluation and perform operations without being authorized. For example, these attackers may personalize the product in an unauthorized manner or attempt a fraudulent access to the smart card system.

T.T_ES
Theft or unauthorized use of the target of evaluation (e.g., microcircuit unsoldered with embedded software).

T.T_CMD
Unauthorized use of instructions, commands or command sequences sent to the target of evaluation.

Unauthorized modification of property

The target of evaluation may be subject to different types of logical or physical attacks liable to diminish security. Because of the designated usage for the target of evaluation (its environment may be hostile), the target of evaluation security elements may be circumvented or compromised, thus reducing the target of evaluation security mechanisms and deactivating their capacity for managing the security of the target of evaluation. This type of threat includes employing hostile Trojan horses, back doors, virus downloading or unauthorized programmes.

T.MOD_LOAD
Unauthorized loading of programmes.

T.MOD_EXE
Unauthorized execution of programmes.

T.MOD_SHARE
Unauthorized modification of the behaviour of the programme through interaction with different programmes.

T.MOD_SOFT
Unauthorized modification of the smart card embedded software and applicative data.

3.3.2.5 Classification des threats

Table 7 below indicates the relations between the life cycle phases of the smart card, the threats and the types of threats:

Threats	Phase 1	Phase 4	Phase 5	Phase 6	Phase 7
T.CLON	Class II	Class I	Class I	Class I	Class I
T.DIS_INFO	Class II				
T.DIS_DEL	Class II				
T.DIS_DEL1	Class II				
T.DIS_DEL2		Class II	Class II	Class II	
T.DIS_ES1	Class II				
T.DIS_TEST_ES	Class II				
T.DIS_ES2		Class I	Class I	Class I	Class I
T.T_DEL	Class II				
T.T_TOOLS	Class II				
T.T_SAMPLE2	Class II				
T.T_ES		Class I	Class I	Class I	Class I
T.T_CMD		Class I	Class I	Class I	Class I
T.MOD_DEL	Class II				
T.MOD_DEL1	Class II				
T. MOD_DEL2		Class II	Class II	Class II	
T.MOD	Class II				
T.MOD_SOFT		Class I	Class I	Class I	Class I
T.MOD_LOAD		Class I	Class I	Class I	Class I
T.MOD_EXE		Class I	Class I	Class I	Class I
T.MOD_SHARE		Class I	Class I	Class I	Class I
T.Malfunction				Class I	Class I
T.RND				Class I	Class I

Table 7: Threat Classification

Class I	:	Threats triggering protections implemented by the TOE.
Class II	:	Threats triggering protections implemented by the TOE environment.

3.3.3 Threats defined in [R3 – SSCD T2] and [R4 – SSCD T3]

The following threats are those defined in protection profiles **[R3 – SSCD T2]** and **[R4 – SSCD T3]**. The threatening agent is a human or a process acting on its own behalf and located outside of the TOE. The primary goal of the attacker is to access sensitive information linked to secure electronic signature services. The attacker has a high attack potential and knows no secret.

T.Hack_Phys *Physical attacks by the TOE interfaces*
An attacker interacts with the TOE interfaces for exploiting vulnerabilities, which resultingly compromises security arbitrarily. This threat concerns all property.

T.SCD_Divulg *Storage, copying and circulation of signature creation data*
An attacker may store or copy the SCD outside of the TOE. An attacker may distribute the SCD during their generation, storage and utilization for signature creation in the TOE.

T.SCD_Derive *Find the signature creation data*
An attacker finds the SCD in known public data, such as the SVD corresponding to the SCDs or the signatures created by SCDs or other data transmitted outside of the TOE which pose a threat to SCD confidentiality.

T.Sig_Forgery *Electronic signature forgery*
An attacker forges the signed data object and perhaps also his electronic signature created by the TOE and the violation of the audit trail of the object of the signed data is not detectable by the signatory or by third parties. The TOE-generated signature is subject to deliberate attacks by experts with a high attack potential with the help of advanced knowledge with regards to security principles and concepts employed by the TOE.

T.Sig_Repud *Signature renunciation*
Should an attacker successfully threaten a property, the non-renunciation of the electronic signature is then compromised. The signatory is thus able to deny having signed data by using SCDs in the TOE under his control even if the signature is successfully verified relative to the SVDs contained in his unrevoked certificate.

T.SVD_Forgery *Forgery of signature verification data*
An attacker forges the SVD presented by the TOE to the CGA, resulting in a loss of SVD integrity in the signatory's certificate.

T.DTBS_Forgery *Forgery of the DTBS representation*
An attacker modifies the representation of the DTBS sent by the SCA. The representation of the DTBS thus used by the TOE for signature does not correspond to the DTBS that the signatory intends to sign.

T.SigF_Misuse *Poor use of the TOE signature creation function*
An attacker poorly uses the TOE signature creation function for creating an SDO for data that the signatory has decided not to sign. The TOE is subject to deliberate attacks by experts with a high attack potential with the help of advanced knowledge with regards to security principles and concepts employed by the TOE.

3.4 ORGANIZATIONAL SECURITY POLICIES

Table 8 presents the organizational security policies considered for the present TOE and their correspondence with protection profiles **[R2 – 9911]**, **[R3 – SSCD T2]** and **[R4 – SSCD T3]** as well as the target **[R15 – CLST]**.

TOE Policies	PP 9911	PP type 2 SSCD	PP type3 SSCD	ST Crypto library .
P.Add-Components				P.Add-Components
P.Add-Func				P.Add-Func
P.CSP_Qcert		P.CSP_Qcert	P.CSP_Qcert	
P.Qsign		P.Qsign	P.Qsign	
P.Sigy_SSCD		P.Sigy_SSCD	P.Sigy_SSCD	

Table 8: ST/PP Correspondence – organizational security policies for the TOE

3.4.1 Policies defined in [R15 – CLST]

P.Add-Components *Addition of specific security components*
The integrated circuit part in the smart card of the TOE provides the following additional security functionalities to the smart card embedded software:
- TDES Encryption and decryption
- Zone-based access control memory
- Access control to Special Functions Registers
- Separation memory for different parts of the software

The cryptographic library part of the TOE uses the Triple DES processor of the material for providing DES security functions, as listed below in P.Add-Func.
The cryptographic library does not use the zone-based access control memory or the access control to Special Functions Registers. These characteristics are for the smart card embedded software, which includes the cryptographic library.

P.Add-Func *Addition of specific security functionalities*

The cryptographic library part of the TOE shall provide the following additional security functionalities to the smart card embedded software:
- TDES Encryption and decryption
- RSA RSA-CRT Algorithms
- RSA key generation
- SHA-1Hash Algorithm
- RNG access (implementation of RNG software and tests for RNG material)
- Secure copying routine.

Moreover, the TOE shall provide:
- protection of residual information; and
- resistance against attacks by covert channels as described in Table 9: Resistance of cryptographic algorithms .

The qualities of the cryptographic algorithms according to their resistance to attacks by covert channels are summarized in the following table:

Algorithm	Resistance against attacks:			
DES and DES3	Timing	SPA	DPA	DFA
RSA-CRT algorithm 1	Timing	SPA	DPA	DFA
RSA-CRT algorithm 2	Timing	SPA	DPA	n.a.
RSA	Timing	SPA	DPA	n.a.
RSA key generation	Timing	SPA	n.a.	n.a.
SHA-1	Timing*	SPA*	n.a.	n.a.

Table 9: Resistance of cryptographic algorithms

* The resistance is only guaranteed if the TOE functions according to certain pre-requisites.

The abbreviation n.a. means that the TOE does not provide countermeasures. This does not necessarily mean that the algorithm is not secure, but rather that at the time of drafting of this security target, no undesirable attack was known.

3.4.2 Policies defined in [R3 – SSCD T2] and [R4 – SSCD T3]

The organizational security policies of the TOE defined in protection profiles **[R3 – SSCD T2]** and **[R4 – SSCD T3]** are applicable when the TOE is used within the framework of a qualified electronic signature creation service. Otherwise, they are not applicable.

P.CSP_Qcert *Qualified Certificate*
The CSP uses a trustworthy CGA for generating the SVD qualified certificate generated by the SSCD. The qualified certificates contain at least the elements defined in Annexe I of the Directive, i.e., among other things, the signatory's name and the SVD corresponding to the SCDs implemented in the TOE under the signatory's exclusive control. The CSP guarantees that the utilization of the TOE for signature is proven by the certificate or other publicly available information.

P.Qsign *Qualified electronic signatures*
The signatory uses a signature creation system for signing the data with the help of qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate (in compliance with Annexe 1 of the Directive) and is created by an SSCD.

P.Sigy_SSCD *TOE as a secure signature creation device*
The TOE implements the SCD used for signature creation under the sole control of the signatory. In practise, the SCDs used for generating the signature may only appear once.

4. SECURITY OBJECTIVES

This section identifies and defines the TOE Security Objectives and the TOE environment Security Objectives. The Security Objectives reflect the stated intention and counter the threats identified while complying with the identified organizational security policies and assumptions.

The TOE Security Objectives and the TOE environment Security Objectives are those defined in protection profile **[R2 – 9911]**, **[R3 – SSCD T2]** and **[R4 – SSCD T3]** as well as the target **[R15 – CLST]**.

4.1 TOE SECURITY OBJECTIVES

Table 10 presents the Security Objectives established for the present TOE and their correspondence with protection profiles **[R2 – 9911]**, **[R3 – SSCD T2]** and **[R4 – SSCD T3]** as well as with the target **[R15 – CLST]**.

TOE Security Objectives	**PP 9911**	**PP type 2 SSCD**	**PP type3 SSCD**	**ST Crypto library .**
OT.EMSEC_Design		OT.EMSEC_Design	OT.EMSEC_Design	
OT.Lifecycle_Security		OT.Lifecycle_Security	OT.Lifecycle_Security	
OT.SCD_Secrecy		OT.SCD_Secrecy	OT.SCD_Secrecy	
OT.SCD_SVD_Corresp		OT.SCD_SVD_Corresp	OT.SCD_SVD_Corresp	
OT.SVD_Auth_TOE		OT.SVD_Auth_TOE	OT.SVD_Auth_TOE	
OT.Tamper_ID		OT.Tamper_ID	OT.Tamper_ID	
OT.Tamper_Resistance		OT.Tamper_Resistance	OT.Tamper_Resistance	
OT.SCD_Transfer		OT.SCD_Transfer		
OT.Init			OT.Init	
OT.SCD_Unique			OT.SCD_Unique	
OT.DTBS_Integrity_TOE		OT.DTBS_Integrity_TOE	OT.DTBS_Integrity_TOE	
OT.Sigy_SigF		OT.Sigy_SigF	OT.Sigy_SigF	
OT.Sig_Secure		OT.Sig_Secure	OT.Sig_Secure	
O.TAMPER_ES	O.TAMPER_ES			O.Leak-Inherent O.Phys-Probing O.Phys-Manipulation O.Leak-Forced O.Abuse-Func
O.CLON	O.CLON			
O.OPERATE	O.OPERATE			O.Malfunction O.Leak-Forced O.Abuse-Func O.SFR_ACCESS
O.DIS_MECHANISM2	O.DIS_MECHANISM2			O.Leak-Inherent O.Phys-Probing O.Leak-Forced
O.DIS_MEMORY	O.DIS_MEMORY			O.Leak-Inherent O.Phys-Probing O.Leak-Forced O.MEM_ACCESS O.SFR_ACCESS
O.MOD_MEMORY	O.MOD_MEMORY			O.Phys-Manipulation O.MEM_ACCESS O.SFR_ACCESS
O.RND				O.RND
O.HW_DES3				O.HW_DES3
O.DES3				O.DES3
O.RSA				O.RSA
O.RSA_KEYGEN				O.RSA_KeyGen
O.SHA-1				O.SHA-1
O.REUSE				O.REUSE

O.COPY				O.COPY

Table 10: ST/PP Correspondence – TOE Security Objectives

4.1.1 Security Objectives defined in [R15 – CLST]

O.RND *Random numbers*
The TOE shall ensure the cryptographic quality of random number generation. For example, random numbers must not be predictable and must have sufficient entropy.
The TOE shall ensure that no information concerning random numbers produced becomes available for an attacker since they can be used, for example, for generating cryptographic keys.
Both the PHILIPS component random number generator and that of the cryptographic library are considered here.

O.HW_DES3 *TDES material functionality*
The TOE shall provide the cryptographic functionality material for calculating a triple DES (TDES) encryption and decryption on the smart card embedded software. The component directly supports TDES calculation using up to three different keys.

Note: The TOE shall ensure user data confidentiality (especially that of cryptographic keys) during a cryptographic operation.

O.DES3
The TOE features the encryption and decryption functionality for the triple DES algorithm that resists the attacks described in Table 9: Resistance of cryptographic algorithms . It uses the DES material resource defined in objective O.HW_DES3 defined hereabove in this target.

O.RSA
The TOE features the public keys processing functionality using the RSA and RSA-CRT algorithms, resistant against the attacks described in Table 9: Resistance of cryptographic algorithms .

O.RSA_KeyGen
The TOE features the functionality for generating pairs of RSA and RSA-CRT keys, resistant to the attacks described in Table 9: Resistance of cryptographic algorithms .

O.SHA-1
The TOE features the functionality of providing hashing means using the SHA-1 algorithm, resistant to the attacks described in Table 9: Resistance of cryptographic algorithms .

O.COPY
The TOE features the memory content copy functionality using a routine that implements countermeasures towards attacks by covert channels.

O.REUSE
The TOE features measures for ensuring that the memory resources used by the TOE cannot be disclosed between consecutive users of the same resource memory.

4.1.2 Security Objectives defined in [R2 – 9911]

The TOE shall employ the most advanced technologies in order to ensure the following IT Security Objectives. In order to do so, when physical microcircuit security functionalities are used, their specifications must be respected. When the physical microcircuit security functionalities are not used, the Security Objectives must be reached through other means.

O.TAMPER_ES

The target of evaluation must hinder attacks on its critical security elements. Security mechanisms must especially hinder the unauthorized modification of functional parameters, security attributes and secret codes such as the life cycle sequence markers and the cryptography keys. The embedded software must be designed such that the interpretation of electrical signals emitted from material parts of the target of evaluation are avoided.

O.CLON
The target of evaluation functionality must be protected from cloning.

O.OPERATE
The target of evaluation shall ensure continuity of the correct functioning of the security functions.

O.DIS_MECHANISM2
The target of evaluation shall ensure that the embedded software security mechanisms are protected against unauthorized disclosure.

O.DIS_MEMORY
The target of evaluation shall ensure that the sensitive information stored in memory is protected against the unauthorized disclosure.

O.MOD_MEMORY
The target of evaluation shall ensure that the sensitive information stored in memory is protected against any corruption or unauthorized modification.

4.1.3 Security Objectives defined in [R3 – SSCD T2] and [R4 – SSCD T3]

[R3 – SSCD T2] protection profile objective:

OT.SCD_Transfer *Protected transfer of SCD between SSCDs*
The TOE shall ensure the confidentiality of SCD transferred between SSCDs.

Protection profile objectives **[R4 – SSCD T3]:**

OT.Init *SCD/SVD Generation*
The TOE provides security functions for guaranteeing that the generation of SCDs and SVDs is called for solely by authorized users.

OT.SCD_Unique *Unique character of signature creation data*
The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for the generation of the signature can appear, in practise, only once and can not be reconstructed from SVDs. In this context, "in practise only once” means that the probability of an identical SCD is negligible.

Protection profile objectives common to **[R3 – SSCD T2]** and **[R4 – SSCD T3]**:

OT.EMSEC_Design *Provide physical security for emanations*
Design and build the TOE for being able to control the production of intelligible emanations within specified limits.

OT.Lifecycle_Security *Life cycle security*
The TOE shall detect the defects during operational initialisation, personalization and utilization. The TOE shall provide safe destruction techniques for the SCD in the case of new generation.

OT.SCD_Secrecy *Confidentiality of signature creation data*
SCD confidentiality used for signature generation is sufficiently protected against high potential attacks.

OT.SCD_SVD_Corresp *Correspondence between the SVD and the SCD*

The TOE shall guarantee 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 they were sent to the TOE.

OT.SVD_Auth_TOE *The TOE guarantees the authenticity des SVD*
The TOE provides the means for allowing the CGA to verify the authenticity of the SVDs that were exported by this TOE.

OT.Tamper_ID *Intrusion detection*
The TOE provides system functions that detect physical intrusion of a system component and uses these functions for limiting the security breaches.

OT.Tamper_Resistance *Intrusion resistance*
The TOE avoids or resists physical intrusion with specified "system" devices and components.

OT.DTBS_Integrity_TOE *Verification of the integrity of the DTBS representation*
The TOE shall verify that the DTBS representation received of the SCA has not been modified during transfer between the SCA and the TOE. The TOE itself shall ensure that the DTBS representation is not modified by the TOE either. It must be emphasized that that does not enter into conflict with the signature creation process where the DTBS themselves may be "hashed" by the TOE.

OT.Sigy_SigF *Signature generation function solely for the legitimate signatory*
The TOE provides a signature generation function solely for the legitimate signatory and protects the SCD against utilization by someone else. The TOE shall resist high potential attacks.

OT.Sig_Secure *Cryptographic electronic signature protection*
With the help of robust encryption techniques, the TOE generates electronic signatures that can not be forged without knowing the SCD. The SCD can not be rebuilt with the help of electronic signatures. The electronic signatures must be able to resist these attacks even if they are performed with a high attack potential.

4.2 SECURITY OBJECTIVES FOR THE TOE ENVIRONMENT

Table 11 presents the Security Objectives established for the environment of the present TOE and their correspondence with protection profiles **[R2 – 9911]**, **[R3 – SSCD T2]** and **[R4 – SSCD T3]** as well as with target **[R15 – CLST]**.

Security Objectives for the TOE environment	PP 9911	PP type 2 SSCD	PP SSCD type3	ST crypto library.
OE.SCD_SVD_Corresp		OE.SCD_SVD_Corresp		
OE.SCD_Transfer		OE.SCD_Transfer		
OE.SCD_Unique		OE.SCD_Unique		
OE.CGA_Qcert		OE.CGA_Qcert	OE.CGA_Qcert	
OE.SVD_Auth_CGA		OE.SVD_Auth_CGA	OE.SVD_Auth_CGA	
OE.HI_VAD		OE.HI_VAD	OE.HI_VAD	
OE.SCA_Data_Intend		OE.SCA_Data_Intend	OE.SCA_Data_Intend	
O.DEV_TOOLS	O.DEV_TOOLS			OE.Process-TOE
O.DEV_DIS_ES	O.DEV_DIS_ES			OE.Process-TOE
O.SOFT_DLV	O.SOFT_DLV			OE.Process-TOE
O.INIT_ACS	O.INIT_ACS			OE.Process-Card
O.SAMPLE_ACS	O.SAMPLE_ACS			OE.Process-TOE OE.Process-Card
O.DLV_PROTECT	O.DLV_PROTECT			OE.Process-TOE OE.Process-Card
O.DLV_AUDIT	O.DLV_AUDIT			OE.Process-TOE
O.DLV_RESP	O.DLV_RESP			
O.DLV_DATA	O.DLV_DATA			OE.Process-Card
O.FLAW	O.FLAW			
O.TEST_OPERATE	O.TEST_OPERATE			OE.Process-Card
O.USE_DIAG	O.USE_DIAG			
OE.Plat-Appl				OE.Plat-Appl

OE.Resp-Appl				OE.Resp-Appl

Table 11: ST/PP Correspondence – Security Objectives for the TOE environment

4.2.1 Objectives for the TOE environment defined in [R15 – CLST]

OE.Plat-Appl *Utilization of the material platform*
In order to ensure that the TOE is used in a safe manner, the smart card embedded software must be designed such that the requirements of the following documents are satisfied: (i) the data sheet of the integrated circuit material of the smart card, (ii) the application notes of the smart card integrated circuit and (iii) the conclusions of the assessment reports of the integrated circuit of the smart card pertaining to the smart card embedded software.

OE.Resp-Appl *Processing user data*
The user sensitive data, especially the cryptographic keys, are processed by the smart card embedded software as required by the security needs of the specific context application.

4.2.2 Security Objectives for the TOE environment as defined in [R2 – 9911].

4.2.2.1 Phase 1 Objectives

O.DEV_TOOLS
The smart card embedded software must be designed in a safe manner, using solely software development tools (compiler assemblers, link editors, simulators…) and software-material (emulators) integration test tools ensuring programmes and data integrity.

O.DEV_DIS_ES
The embedded software developers shall use established procedures in order to control the storage and usage of classified development tools as well as the classified documentation in order to guarantee integrity and the confidentiality of the target of evaluation.
It must be guaranteed that the tools are provided and accessible exclusively for the authorized personnel of each party.
It must be guaranteed that the confidential information relatives to the property defined are provided to the authorized personnel of each party on the sole basis of the need to know them.

O.SOFT_DLV
The smart card embedded software must be delivered by the smart card embedded software developers (Phase 1) to the microcircuit designer via a procedure of delivery and secure verification capable of ensuring software integrity and confidentiality as the need arises.

O.INIT_ACS
Initialisation data (physical, organizational, technical and personnel-related procedures) shall be accessible to authorized personnel only.

O.SAMPLE_ACS
The samples used for performing tests must be accessible exclusively to authorized personnel.

4.2.2.2 Delivery process objectives for phases 4 to 7

O.DLV_PROTECT

Procedures must ensure protection of material/information of the target of evaluation upon delivery. They shall include the following objectives:

- Non-disclosure of security-related information;
- Identification of elements to be delivered;
- Respect of confidentiality rules (level of confidentiality, dispatch note, acknowledgement of receipt);
- Physical protection against the external damage;
- Secure storage and handling procedures, including refused assessment targets);
- Traceability of assessment targets being delivered, including the following parameters:
    - details regarding the origin and shipping;
    - reception, acknowledgement of receipt;

The equipment location and information.

O.DLV_AUDIT

The procedures must ensure that corrective action is taken in case of dysfunction in the delivery process (including, as the case may be, any non-compliance with confidentiality agreements) and highlight any non-respect of this process.

O.DLV_RESP

The procedures must ensure that the personnel (of the shipping and receiving department, the carrier,) who intervene during the delivery procedure have the skill, the training and the knowledge required for fulfilling the requirements of this procedure and are capable of acting in perfect correspondence with the expectations cited hereabove.

4.2.2.3 Delivery process objectives for phases 1 to 4, 5 and 6

O.DLV_DATA

The "applicative" data must be delivered by the embedded software developers (phase 1) either to the microcircuit housing manufacturer, to the process definition manufacturer or to the personalizer via a delivery and secure verification procedure capable of ensuring the audit trail and the confidentiality of the applicative data.

O.FLAW

The target of evaluation shall contain no flaws in design, implementation or functioning.

4.2.2.4 Objectives for phases 4 to 6

O.TEST_OPERATE

Appropriate functionality tests for the target of evaluation must be implemented in phases 4 to 6.
During all manufacturing and test operations, security procedures must be implemented in phases 4, 5 and 6 in order to ensure the confidentiality and audit trail of the target of evaluation and its manufacturing and test data.

4.2.2.5 Phase 7 objectives

O.USE_DIAG

Secure communications protocols and procedures must be used between the smart card and the terminal.

4.2.3 Security Objectives for the IT environment of the TOE

These objectives are defined in protection profiles **[R3 – SSCD T2]** and **[R4 – SSCD T3]**.

Security Objectives for the IT environment of the TOE in **[R3 – SSCD T2]**:

OE.SCD_SVD_Corresp *Correspondence between SVD and SCD*

Le SSCD Type 1 shall ensure the correspondence between the SVD and the SCD. The Type 1 SSCD shall verify the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or to the TOE.

OE.SCD_Transfer *Secure SCD transfer between SSCD*
The Type 1 SSCD shall ensure the confidentiality of the SCD transferred to the TOE. The Type 1 SSCD shall provide against the exportation of an SCD that has already been used for signature generation by a type 2 SSCD. The SCD shall be destroyed in the Type 1 SSCD every time it is exported into the TOE.

OE.SCD_Unique *Signature creation data unicity*
The Type 1 SSCD shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation cannot in practise appear only once and it cannot be reconstructed from SVDs. In this context, " in practise appear only once" means that the probability of an identical SCD is a negligible quantity.

Security Objectives for the IT environment of the TOE common to **[R3 – SSCD T2]** and **[R4 – SSCD T3]**:

OE.CGA_Qcert *Generation of qualified certificates*
The CGA generates qualified certificates that include among other things:

(a) the name of the signatory auditing the TOE;
(b) the SVD corresponding with the SCD implemented in the TOE under the sole control of the signatory;
(c) the advanced CSP signature.

OE.SVD_Auth_CGA *The CGA verifies the SVD authenticity*
The CGA verifies that the SSCD is the issuer of the SVD received and that the audit trail of the SVD received is intact. The CGA verifies the correspondence between the SCD in SSCD of the signatory and the SVD du qualified certificate.

OE.HI_VAD *VAD Protection*
If an external device provides a human interface for authentifying the user, this device shall guarantee the VAD confidentiality and audit trail necessary for the authentification method used.

OE.SCA_Data_Intend *Data that must be signed*
The SCA:

(a) generates the representation of the DTBS that was presented as DTBS and which the signatory intends to sign in a form adapted to signature by the TOE;
(b) sends the representation of the DTBS to the TOE and allows for the verification of the audit trail of the representation of the DTBS by the TOE;
(c) attaches the signature produced by the TOE to the data or provides it separately.

5. IT SECURITY REQUIREMENTS

This chapter presents the TOE security requirements.

The functional requirements for the TOE defined in these chapters are those defined in protection profiles **[R2 – 9911]**, **[R3 – SSCD T2]** and **[R4 – SSCD T3]** as well as in target **[R15 – CLST]**. Table 12 presents the distribution of the requirements for these three protection profiles and target **[R15 – CLST]**.

SFR for the TOE	PP 9911	PP type 2 SSCD	PP type3 SSCD	ST Crypto. Library
Security Audit				
FAU_SAA.1	FAU_SAA.1			
Cryptographic Support				
FCS_CKM.1			FCS_CKM.1	FCS_CKM.1
FCS_CKM.3	FCS_CKM.3			
FCS_CKM.4	FCS_CKM.4	FCS_CKM.4	FCS_CKM.4	
FCS_COP.1	FCS_COP.1	FCS_COP.1	FCS_COP.1	FCS_COP.1
FCS_RND.1				FCS_RND.1
FCS_RND.2				FCS_RND.2
User data protection				
FDP_ACC.1		FDP_ACC.1	FDP_ACC.1	
FDP_ACC.2	FDP_ACC.2			
FDP_ACF.1	FDP_ACF.1	FDP_ACF.1	FDP_ACF.1	
FDP_DAU.1	FDP_DAU.1			
FDP_ETC.1	FDP_ETC.1	FDP_ETC.1	FDP_ETC.1	
FDP_IFC.1				FDP_IFC.1
FDP_ITC.1	FDP_ITC.1	FDP_ITC.1	FDP_ITC.1	
FDP_ITT.1				FDP_ITT.1
FDP_RIP.1	FDP_RIP.1	FDP_RIP.1	FDP_RIP.1	FDP_RIP.1
FDP_SDI.2	FDP_SDI.2	FDP_SDI.2	FDP_SDI.2	
FDP_UCT.1		FDP_UCT.1		
FDP_UIT.1		FDP_UIT.1	FDP_UIT.1	
Identification and authentification				
FIA_AFL.1	FIA_AFL.1	FIA_AFL.1	FIA_AFL.1	
FIA_ATD.1	FIA_ATD.1	FIA_ATD.1	FIA_ATD.1	
FIA_UAU.1	FIA_UAU.1	FIA_UAU.1	FIA_UAU.1	
FIA_UAU.3	FIA_UAU.3			
FIA_UAU.4	FIA_UAU.4			
FIA_UID.1	FIA_UID.1	FIA_UID.1	FIA_UID.1	
FIA_USB.1	FIA_USB.1			
Security Administration				
FMT_MOF.1	FMT_MOF.1	FMT_MOF.1	FMT_MOF.1	
FMT_MSA.1	FMT_MSA.1	FMT_MSA.1	FMT_MSA.1	
FMT_MSA.2	FMT_MSA.2	FMT_MSA.2	FMT_MSA.2	
FMT_MSA.3	FMT_MSA.3	FMT_MSA.3	FMT_MSA.3	
FMT_MTD.1	FMT_MTD.1	FMT_MTD.1	FMT_MTD.1	
FMT_SMF.1				
FMT_SMR.1	FMT_SMR.1	FMT_SMR.1	FMT_SMR.1	
Privacy Protection				
FPR_UNO.1	FPR_UNO.1			
TSF Protection				
FPT_AMT.1		FPT_AMT.1	FPT_AMT.1	
FPT_EMSEC.1		FPT_EMSEC.1	FPT_EMSEC.1	
FPT_FLS.1	FPT_FLS.1	FPT_FLS.1	FPT_FLS.1	FPT_FLS.1
FPT_ITT.1				FPT_ITT.1
FPT_PHP.1		FPT_PHP.1	FPT_PHP.1	
FPT_PHP.3	FPT_PHP.3	FPT_PHP.3	FPT_PHP.3	FPT_PHP.3
FPT_SEP.1	FPT_SEP.1			FPT_SEP.1

FPT_TDC.1	FPT_TDC.1			
FPT_TST.1	FPT_TST.1	FPT_TST.1	FPT_TST.1	
FPT_TST.2				FPT_TST.2
Webs and channels of trust				
FTP_ITC.1		FTP_ITC.1	FTP_ITC.1	
FTP_TRP.1		FTP_TRP.1	FTP_TRP.1	
Resource Utilization				
FRU_FLT.2				FRU_FLT.2

Table 12: ST/PP Correspondence–TOE security requirements

5.1 SUBJECTS, OBJECTS AND TOE SECURITY ATTRIBUTES

5.1.1 List of TOE subjects

LIST subjects	Description
SUB_GEST	Process that receives all commands coming from the terminal and dispatches them towards another process (SUB_APPLI, SUB_IPA).
SUB_IPA	Process activated by default by SUB_GEST during the initialisation and personalization phases. SUB_IPA is an object for SUB_GEST.
SUB_APPLI	Process creating the services associated with the **IAS-eGOV application** and that is activated by SUB_GEST during the "user" phase when the command is a SELECT command. SUB_APPLI is an object for SUB_GEST.
SUB_CRYPTO	Process activated by SUB_APPLI for performing cryptographic operations or the operations using the bearer code. SUB_CRYPTO is an object for SUB_APPLI and for SUB_IPA.
SUB_GF	Process activated by SUB_APPLI for managing the OB_FILE objects. SUB_GF is an object for SUB_APPLI and for SUB_IPA.
SUB_GS	Process activated by SUB_APPLI for managing the OB_SECRET objects. SUB_GS is an object for SUB_APPLI and for SUB_IPA.
SUB_GT	Process activated by SUB_APPLI for managing the OB_TLV objects. SUB_GT is an object for SUB_APPLI and for SUB_IPA.

5.1.2 List of TOE objects

Objects LIST	Description
OB_FILE	Object designating in a generic manner the following objects: OB_DFILE, OB_EFILE, OB_TLV, OB_SECRET. Generally speaking, an oB_FILE is an object on which are applied access controls in read/write and creation/deletion and change of status outside of the OB_TLV object.
OB_DFILE	ADF or DF directory type, stored in E²PROM, that contains OB_FILEs.
OB_EFILE	Elementary EF File stored en E²PROM and containing proprietary user data.
OB_TLV	TLV type data = Threshold Limit Value. They merge the card parameter type data. When they are accessible, they are accessible in updating and for reading.
OB_SECRET	Object containing a cryptographic key or a PIN Code as well as the security information associated with them. It is stored in the OB_FILE (SECRET_INFO & SECRET_DATA) files.
OB_TEMP	Object designating the temporary data that is stored in RAM and that is used in secure operations.
OB_I/O	Buffers used for external communication.

5.1.3 List of TOE security attributes

LIST Attributes	Description
Checksum buffer I/O	Checksum for management of the audit trail of I/O buffers prior and following the processing performed by SUB_CRYPTO: - Corrupted/Non-corrupted.
Checksum directory/file	Checksum for management of the audit trail of the data of the directory or of the file: - Corrupted/Non-corrupted.
Checksum secret	Checksum for management of the audit trail of a key or of a PIN Code: - Corrupted/Non-corrupted.
Checksum TLV	Checksum for management of the audit trail of the parameter stored in the TLV object: - Corrupted/Non-corrupted.
DAC: Access control to files and directories	This attribute defines the access conditions to objects to which it is attached. Its structure is presented as follows: *DAC = [(Operation1, (list of conditions for operation1)), ((Operation2, (list of conditions for operation2)), …]* The operations are the writing or the reading of data in the file concerned. The conditions for an operation are: - ALWAYS: Operation always authorized; - NEVER: Operation never authorized;

	- USERx: Operation authorized if USERx authentified; - SMI: Operation authorized if the command protection is SMI; - SMC: Operation authorized if the securization command is SMI + SMC. Every object (directory, file, secret or TLV) is associated with an attribute indicating the access conditions. The DAC is compared with the current security attributes in the security card status.
Command header	The "CLA, INS, P1, P2" fields of the command are used for analysing the command.
Security card status	This attribute contains the current security statuses for the Morpho-Citiz 32 card. It is composed of the following attributes: - The user(s) authentified on the different domains: When a user is successfully authentified, their authentification on a domain is indicated on the security card status; - The breadth of authentifications: The validity of users' authentification statuses is a function of the domain on which the authentification secrets are associated; - The current Channel of trust (SM): Indicates if a SMI/SMC has been established; The domain authentification statuses are initialized at "no authentified user" when the operations exit the domain. The current channels of trust are initialized at "no SM" and "no current nature" at each new operation (i.e. upon each new command).
Secret status	Attribute that defines the current status of an OB_SECRET: - Created/Activated/Deactivated/Terminated/blocked;
File status	Attribute that defines the current status of an OB_FILE (except for OB_TLVs): - Created/Activated/Deactivated/Terminated;
Utilization Counter	Attribute associated with a secret and limiting the maximum number of secret utilizations.
Ratification Group	Attribute associated with a secret that counts the successive authentification failures on this secret: PTC: Ratification counter PTL: Maximum number of presentations
Card life phase	This attribute defines the life phase in which the card is found: INIT/PERSO/USER/BLOCKED/END OF LIFE
Application status	This attribute defines the current status of the application: It describes the different conditions of the application: - Active/Non-Active; - Selected/pause; - Blocked/Non-blocked;
Services Table	This attribute defines the access rights of subjects to the services that create the subjects that they solicit. For example, SUB_APPLI calls SUB_CRYPTO for creating the cryptographic processing services.
Algorithm Type	This attribute is used for controlling the "key/algorithm" association, i.e.: AUTH_INT, AUTH_EXT, ENC/DEC, MAC, GEN_SIGN, VERIF_SIGN, SEC_DEC.
Key Type	This attribute defines the use of the key: - AUTH_INT: Internal authentification; - AUTH_EXT: External authentification; - ENC/DEC: Data Encryption / decryption; - MAC: MAC Calculation; - GEN_SIGN: Electronic signature generation; - VERIF_SIGN: Electronic signature verification; - SEC_DEC: Secret decryption;
Object Type	This attribute is used for defining an object type: MF/ADF/DF/EF/SECRET/TLV.

5.1.4 Security attributes defined in [R3 – SSCD T2] and [R4 – SSCD T3]

The user security attributes, TOE components and the associated statuses are:

User, subject or object to which the attribute is associated	Attribute	Status
Group of general attributes		
User	Role	Administrator/Signatory
Group of initialisation attributes		
User	SCD/SVD Management	Authorized/Non-authorized
SCD	Secure authorized SCD Importation	No/Yes
Group of signature creation attributes		
SCD	Operational SCD	No/Yes
DTBS	Sent by an authorized CSA	No/Yes

5.2 DEFINITION OF TOE FUNCTIONAL SECURITY REQUIREMENTS

5.2.1 FAU Security Audit

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a group of rules while surveilling the audited events and indicate, according to these rules, a potential TSP violation.

FAU_SAA.1.2 The TSF shall apply the following rules for the surveillance of audited events:

1. Accumulation or combination of the known **[posting: following auditables events]** for indicating a potential security violation;

   <u>Assignment: Auditable events</u>

   - Modification of the operating mode by the environment (captor);
   - Attempted access control violation;
   - Memory autotest failure (ROM, E²PROM);
   - Audit trail failure on a directory/file, on a file header, on a TLV object, an I/O buffer, on a key or on a PIN Code;
   - Audit trail failure of the unknown generator and crypto processor.
2. Other rules: **[do not apply]**.

5.2.2 FCS Cryptographic Support

FCS_CKM.1 Generating cryptographic keys

SSCD Iteration

FCS_CKM.1.1 The TSF shall generate cryptographic keys in compliance with the cryptographic key generation algorithm **[RSA key generation]** and with the specified sizes of **[1024 à 2048 bits]** cryptographic keys in respect of **[standards [R10 – AREAK1]**, **[R11 – AREAK2]]**.

Crypto library iteration

FCS_CKM.1.1 The TSF shall generate cryptographic keys according to a specified cryptographic key generation algorithm **[RSA (simple) and RSA-CRT]** with sizes of cryptographic keys of **[1024-2048 bits]** that respect **[the standard: "Regulierungsbehörde für Telekommunication und Post : Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetez und der Signaturverordnung, German "Bundesanzeiger Nr 30 » p2537-2538, February 13th, 2004]**.

FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall create **[posting: access to cryptographic keys]** in compliance with a specified **[posting: an access method for cryptographic keys]** that satisfies the following standards: **[not applicable]**

<u>Assignment</u> **<u>Access Type</u>**

Access to SCD/SVDs in read/write mode for performing SCD/SVD generation/destruction operations and for loading SCD/SVD in the cryptographic processing blocks for electronic signature generation.

<u>Cryptographic key access method</u>

Access in read/write mode of the code executed in ROM towards a key stored in the E²PROM by featuring RAM audit trail protection and confidentiality element signalling.

FCS_CKM.4 Destruction of cryptographic keys

FCS_CKM.4.1 The TSF shall destroy the cryptographic keys in compliance with a specified **[posting: method for destroying cryptographic keys]** that satisfies the following standards: **[not applicable]**

Assignment **Destruction Method:**

Deletion of the EEPROM memory containing the key.

SSCD Refinement The SCDs are destroyed upon request by the Signatory or by the Administrator. The destruction of the existing SCD is mandatory prior to re-generation by the TOE of the SCD/SVD pair or re-loading of the SCD in the TOE.

FCS_COP.1 Cryptographic operation

Iteration

FCS_COP.1.1 The TSF shall execute **[posting: list of cryptographic operations]** in compliance with a specified cryptographic algorithm **[posting: cryptographic algorithm]** and with the sizes of cryptographic keys **[posting: sizes of cryptographic keys]** that satisfy the following: **[posting: list of standards]**.

Assignment **See Table 13: Cryptographic operations**

LIST of cryptographic operations	**Algorithms**	**Key sizes**	**List of standards**
Calculation of authentification cryptogrammes	MAC RETAIL	112 bits	ISO 9797-1 – Algo n°3
MAC Calculation	MAC RETAIL	112 bits	ISO 9797-1 – Algo n°3
Encryption/decryption	TDES	112 bits	ISO 10116 / X9.52-1998
Calculation of cryptogramme authentification card	RSA	1024 to 2048 bits	ISO9796-2 coupled with CVC
Calculation of SSL cryptogramme authentification	RSA	1024 to 2048 bits	Signature PKCS#1 V2.1 – padding v 1.5
Asymmetrical decryption	RSA	1024 to 2048 bits	Encryption PKCS#1 V2.1 – padding v 1.5
Verification of the SCD/SVD correspondence	Calculation of RSA key	1024 to 2048 bits	Signature PKCS#1 V2.1 – padding v 1.5
Electronic signature creation	RSA	1024 to 2048 bits	Signature PKCS#1 V2.1 – padding v 1.5
HASH Calculation	DTBS-Hash	N/A	SHA-1 and SHA-2 **[R10 – AREAK1]**, **[R11 – AREAK2]**, **[R13 – ERRATUM]**
DH key exchange	DH	1024 to 2048 bits	**[R10 – AREAK1]**, **[R11 – AREAK2]**

Table 13: Cryptographic operations

Crypto library iteration

FCS_COP.1.1 The TSF shall execute **[posting: list of cryptographic operation]** in compliance with a cryptographic algorithm **[posting: cryptographic algorithm]** and with sizes of specified cryptographic keys **[posting: sizes of cryptographic keys]** that satisfy: **[posting: list of standards]**.

Assignment **See Table 14: Cryptographic Operations**

LIST of cryptographic operations	Algorithms	Key sizes	List of standards
Encryption/decryption	TDEA	112 or 168 bits	FIPS PUB 46-3 federal information processing standards publication data encryption standard (DES) reaffirmed 1999 October 25, keying option 1 and 2.
Encryption/decryption	Triple-DES, modes ECB, CBC, or CBC-MAC	112 or 168 bits	ANSI X9.52-1998 (mode ECB and CBC), FIPS PUB 81 (mode ECB and CBC) ISI 9797-1, algorithm 1 (mode CBC-MAC).
Generation of cryptographic checksum	SHA-1	None	FIPS 180-1
Encryption/decryption	RSA/RSA-CRT	1024 to 2048 bits	Schneier page 468 or Meenezes, Van Oorshot and Vanstone section 8.2 and also standard ISO/IEC 9796 Annex A, section A.4

Table 14: Cryptographic Operations

FCS_RND.1 Quality measurement of random numbers

FCS_RND.1.1 The TSF shall provide a mechanism for generating random numbers that satisfy **[posting: a defined measure of quality]**.

Assignment **Define a quality measure:**

Requirement for providing an entropy of at least 7.976 bits in every octet.

FCS_RND.2 Generation of random numbers

FCS_RND.2.1 The TSF shall provide a mechanism for generating random numbers that respects standard: **[ANSI X9.17 comme décrit dans A. Menezes, P. van Oorshot and S. Vanstone : Handbook of Applied Cryptography, CRC Press, 1996]**.

Scope note: due to the specific characteristics of the smart card (e.g.. absence of a real time clock), the random number generator does not strictly follow this standard. Rather, it is based on this standard for the purpose of improving the quality of the random number generator. The implementation of the random number generator differs from the standard hereabove in the following manner:

- The random numbers originating from the material random number generator are used for initialising the pseudo generator (software), and not as a "time stamp" as suggested in the standard.
- After each reset of the TOE, the internal status is completely reinitialized.
- After generation of several random octets, the random number generator is reinitialized with its own output.

5.2.3 FDP User data protection

FDP_ACC.1 Partial access control

SSCD Iteration

FDP_ACC.1.1 /SFP Initialisation The TSF must apply the **[SFP initialisation]** during **[generation of the SCD/SVD pair]** by the user.

SSCD Iteration

FDP_ACC.1.1 The TSF must apply **[SFP personalization]** during **[RAD creation]** by the administrator.

/SFP Personalization

SSCD Iteration

FDP_ACC.1.1 /SFP SVD Transfer The TSF shall apply the **[SFP Transfer of SVD]** during **[SVD importation or exportation]** by the user.

SSCD Iteration

FDP_ACC.1.1 /SFP signature creation The TSF shall apply the **[SFP signature creation]** during:

1. **[transmission of DTBS representations by the SCA]**,
2. **[signature of the DTBS representations by the Signatory]**.

SSCD Iteration

FDP_ACC.1.1 /SFP SCD Importation The TSF shall apply the **[SFP Importation of SCD]** during **[user SCD importation]**.

FDP_ACC.2 Total access control

Iteration

FDP_ACC.2.1 /APPLI The TSF shall apply the **[posting: SFP access control to "IAS-eGOV" services]** to the **[posting: list of subjects and objects]** and to all operations on the subjects and objects covered by the SFP.

Assignment **List of subjects:**

- SUB_GEST, SUB_APPLI, SUB_IPA;

List of objects:

- SUB_APPLI, SUB_IPA;

Access control to "IAS-eGOV" services:

- SUB_IPA is not selectable;
- Only SUB_GEST activates SUB_APPLI if the command "SELECT" bears on the IAS-eGOV application;
- SUB_GEST forbids the call to a service of a subject by another subject if the said call is not valid;
- SUB_APPLI processes a command if the command format is valid;

FDP_ACC.2.2 /APPLI The TSF shall ensure that all operations between every TSC subject and every TSC object are covered by an SFP access control.

Iteration

FDP_ACC.2.1 /FILE The TSF shall apply the **[posting: SFP access control to files]** to the **[posting: list of subjects and objects]** and to all operations on the subjects and objects covered by the SFP.

Assignment **List of subjects:**

- SUB_APPLI, SUB_GF;

List of objects:

- SUB_GF, OB_DFILE, OB_EFILE;

File access control:

- SUB_APPLI accesses objects OB_DFILE and OB_EFILE only if an application is selected and if these objects are accessible by the selected application;
- SUB_APPLI accesses objects OB_DFILE and OB_EFILE only by

SUB_GF;
- SUB_GF creates on behalf of SUB_APPLI an oB_DFILE or an oB_EFILE in the current OB_DFILE only if the status of the current OB_DFILE is coherent with the operation and if the access conditions of this OB_DFILE for creation are verified;
- SUB_GF never creates in user phase and on behalf of SUB_APPLI an OB_DFILE or an OB_EFILE in an OB_DFILE if this OB_DFILE is not under the current ADF and is not under the current DF;
- SUB_GF never creates in user phase and on behalf of SUB_APPLI an OB_DFILE of the ADF type;
- SUB_GF deletes on behalf of SUB_APPLI a OB_DFILE or a current OB_EFILE only if the status of the file is coherent with the operation and if the access conditions for the deletion of this object are verified;
- SUB_GF never deletes in user phase and on behalf of SUB_APPLI an OB_DFILE if this OB_DFILE contains an OB_DFILE or an OB_EFILE or if the OB_DFILE to be deleted is the MF or an ADF;
- SUB_GF accesses for read/write operations on behalf of SUB_APPLI to data stored in an OB_EFILE only if the object OB_EFILE is audit trail protected, if its status is coherent with the operation and if the access conditions in read/write on this OB_EFILE are verified;
- SUB_GF accesses for operations of activation, deactivation or termination of an object OB_DFILE or OB_EFILE if the status of the object accessed is coherent with the operation and if the access conditions in activation, deactivation or termination on this object are verified;

FDP_ACC.2.2 /FILE The TSF shall ensure that all operations between every TSC subject and every TSC object, are covered by an SFP access control.

Iteration

FDP_ACC.2.1 /TLV The TSF shall apply the **[posting: SFP access control to TLV parameters]** to the **[posting: list of subjects and objects]** and to all operations on the subjects and objects covered by the SFP.

Assignment **List of subjects:**

- SUB_APPLI, SUB_GT;

List of objects:

- SUB_GT, OB_DFILE, OB_TLV;

TLV parameters access control:

- SUB_APPLI access OB_TLV objects only through SUB_GT;
- SUB_GT creates on behalf of SUB_APPLI an OB_TLV in the current OB_DFILE only if the status of the current OB_DFILE is coherent with the operation and if the access conditions for the creation of this OB_DFILE are verified;
- SUB_GT accesses in read / write mode to parameters stored in a OB_TLV, on behalf of SUB_APPLI, only if the access conditions for the operation de read/write on this OB_TLV are verified;

FDP_ACC.2.2 /TLV The TSF shall ensure that all operations between every TSC subject and every TSC object, are covered by an SFP access control.

Iteration

FDP_ACC.2.1 /SEC The TSF shall apply the **[posting: SFP access control to secrets]** to **[posting: list of subjects and objects]** and to all the operations on the subjects and objects covered by the SFP.

<u>Assignment</u> **<u>List of subjects:</u>**

- SUB_APPLI, SUB_CRYPTO, SUB_GS;

<u>List of objects:</u>

- SUB_GS, OB_FILE, OB_SECRET, SUB_CRYPTO;

<u>Access control to secrets:</u>

- Only SUB_CRYPTO and SUB_APPLI access OB_SECRET objects and only through SUB_GS;
- SUB_GS never accesses in read mode values of symmetrical keys or private keys of asymmetrical bi-keys or of a PIN Code, contained in OB_SECRET on behalf of SUB_APPLI;
- SUB_GS creates on behalf of SUB_APPLI a OB_SECRET in the directory OB_DFILE current if the access conditions and the status de this OB_DFILE for the creation are verified;
- SUB_GS accesses OB_SECRET in write mode on behalf of SUB_APPLI or SUB_CRYPTO if the OB_SECRET displays the Created or Activated status and if the access conditions and the status of the object OB_SECRET for a write operation are verified;
- SUB_GS accesses on behalf of SUB_APPLI, for activation operations, deactivation or termination of an OB_SECRET object if the status of the secret is coherent with the operation and if the access conditions for the operation on this object are verified;
- SUB_GS accesses on behalf of SUB_APPLI, for the releasing operation of an OB_SECRET object if the status of the secret is coherent with the operation and if the access conditions for the operation on the secret counter(s), are verified;
- SUB_GS transfers the OB_SECRET into the cryptographic processing blocks on behalf of SUB_CRYPTO if the access conditions for the secret utilization are verified and if the audit trail OB_SECRET is protected and unobstructed;
- SUB_CRYPTO performs a cryptographic operation on behalf of SUB_APPLI with the OB_SECRET transferred into the cryptographic processing blocks;
- SUB_APPLI accesses SUB_CRYPTO for cryptographic operations with OB_SECRETs if the key and algorithm used are coherent for cryptographic operation;

FDP_ACC.2.2 /SEC The TSF shall ensure that all operations between every TSC subject and every TSC object, are covered by an SFP access control.

SSCD Iteration

FDP_ACC.2.1 The TSF shall apply the **[posting: SFP access control to "secure electronic signature" secrets]** to the **[posting: list of subjects and objects]** and to all operations on the subjects and objects covered by SFP.

<u>Assignment</u> **<u>List of subjects:</u>**

- Signatory;
- Administrator;

<u>List of objects:</u>

- SCD;
- SVD;
- DTBS;

<u>Access control to secrets of “secure electronic signature”:</u>

- SCD/SVD objects are accessible in write mode for generation of an SCD/SVD pair only if the user is the signatory or the administrator and if the user has the management rights for SCD/SVD objects;
- SCD/SVD objects are accessible in write mode for destruction of an SCD/SVD pair only if the user is the signatory or the administrator;
- SCD objects are never accessible in read mode for an exportation;
- SVD objects are accessible in read mode for exportation of an SVD only if the user is the administrator or the signatory;
- SCD objects are accessible in utilization mode for creation of a signature on DTBS objects only if the user is the signatory using an “operational” SCD for signing DTBS;
- DTBS objects are accessible in write mode for loading a “DTBS representation” only if the CSA is authorized;
- DTBS objects are not accessible in read mode for signature creation with an operational SCD if the DTBS object has not been sent by an authorized CSA;

FDP_ACC.2.2 The TSF shall ensure that all operations between every TSC subject and every TSC object are covered by an SFP access control.

FDP_ACF.1 Access control based on security attributes

Iteration

FDP_ACF.1.1 /APPLI The TSF shall apply the **[posting: SFP access control to “IAS-eGOV” services]** to objects according to **[posting: the list of security attributes]**.

FDP_ACF.1.2 /APPLI The TSF shall apply the following rules for determining whether an operation between controlled subjects and objects is authorized or not.

Assignment **Rules:**

1. SUB_GEST activates SUB_APPLI upon reception of a "SELECT" command if:
   - The **command header is** coherent with the status of the **life phase card**;
   - The **command header** is valid and corresponds to a “SELECT” command of the IAS-eGOV application;
   - The **directory/file checksum** of SUB_APPLI is correct;
2. SUB_GEST prohibits calling a service if:
   - The subject called and the subject calling are not coherent with the **services table**;
3. SUB_APPLI processes the command received if:
   - The **command header is** coherent with the status of the **life phase card** and the status **file** of the selected ADF;
   - The **command header** is coherent with the SUB_APPLI **application status**;

List of security attributes:

- Command header;
- Table of services;
- Life phase card;
- Application status;
- Checksum file/directory;
- Status file;

FDP_ACF.1.3 /APPLI The TSF shall explicitly authorize the access of subjects to objects according to the following complementary rules: **[posting: not applicable]**.

FDP_ACF.1.4 /APPLI The TSF shall explicitly refuse the access of subjects to objects according to **[posting: Specific rules]**.

<u>**Assignment**</u> <u>**Specific rules:**</u>

1. SUB_GEST <u>does not activate</u> SUB_IPA if:
   - **Life phase card** is: USER, BLOCKED or END OF LIFE;

Iteration

FDP_ACF.1.1 /FILE The TSF shall apply the **[posting: SFP access control to files]** to objects according to **[posting: the list of security attributes]**.

FDP_ACF.1.2 /FILE The TSF shall apply the following rules for determining whether an operation between controlled subjects and objects is authorized or not.

<u>**Assignment**</u> <u>**Rules:**</u>

1. SUB_APPLI activates SUB_GF for performing operations of creation / deletion / reading / writing / activation / deactivation / termination on an OB_DFILE / OB_EFILE if the **command header** and the **type of object** are coherent;
2. SUB_GF performs the creation operation of an OB_DFILE / OB_EFILE file in a current OB_DFILE if:
   - The **type of object** of the file created is DF or EF;
   - The status **file** of the current file is coherent with the operation;
   - The **DAC is** coherent with the **security card status**;
3. SUB_GF performs the deletion operations of a current OB_DFILE / OB_EFILE file if:
   - The **type of object** of the deleted file is different from MF;
   - The status **file** of the current file to be deleted is coherent with the operation;
   - The **DAC is** coherent with the **security card status**;
   - For an OB_DFILE, it does not contain any object or objects of a SECRET or TLV type (these latter are then destroyed);
4. SUB_GF performs the read / write operations in a current OB_DFILE / OB_EFILE file if:
   - The **checksum directory/file** of the accessed file is correct;
   - The status **file** of the accessed file is coherent with the operation;
   - The **DAC** is coherent with the **security card status**;
5. SUB_GF performs the activation / deactivation and termination operations of a current OB_DFILE / OB_EFILE if:
   - The **type of object** of the deleted file differs from the MF;
   - The status **file** of the accessed file is coherent with the operation;
   - The **DAC is** coherent with the **security card status**;

<u>**List of security attributes:**</u>

- Command header;
- Type of object;
- Checksum directory/file;
- DAC;
- Security card status;
- Status file;

FDP_ACF.1.3 /FILE The TSF shall explicitly authorize the access of subjects to objects according to the following complementary rules : **[posting: not applicable]**.

FDP_ACF.1.4 /FILE The TSF shall explicitly refuse the access of subjects to objects according to **[posting: Specific rules]**.

<u>**Assignment**</u> <u>**Specific rules:**</u>

1. SUB_GF never accesses in creation / write / read / activation / deactivation /

termination mode if the **type of object** of the OB_FILE accessed is SECRET or TLV;

2. SUB_GF never accesses in user phase in creation of an OB_DFILE / OB_EFILE in a current OB_DFILE if:
   - The **life phase card** is: BLOCKED and END OF LIFE;
   - The **security card status** does not indicate that an SMI is valid;
   - The file created is of the MF or ADF **type**;
   - The **status file** of the current OB_DFILE is Deactivated or Terminated;
3. SUB_GF never accesses in deletion of an OB_DFILE / OB_EFILE in a current OB_DFILE if:
   - The **life phase card** is: BLOCKED and END OF LIFE;
   - The object deleted is of **type** MF, ADF;
4. SUB_GF never accesses in activation of a current OB_DFILE / OB_EFILE if:
   - The **status file** of the current file is Terminated;
5. SUB_GF never accesses in deactivation of an OB_DFILE/OB_EFILE current if:
   - The **status file** of the current file is Terminated;
   - The current file is of **type** MF;
6. SUB_GF never accesses in termination of an OB_DFILE / OB_EFILE if:
   - The file is **type** MF;
   - The file is not the current file;

Iteration

FDP_ACF.1.1 /TLV The TSF shall apply the **[posting: SFP access control to TLV parameters]** to objects according to **[posting: the list of security attributes]**.

FDP_ACF.1.2 /TLV The TSF shall apply the following rules for determining whether an operation between controlled subjects and objects is authorized or not.

Assignment **Rules:**

1. SUB_APPLI activates SUB_GT for performing the creation / read / write operations in an OB_TLV if **the command header** and the **type of object** are coherent;
2. SUB_GT creates an OB_TLV in a current OB_DFILE if:
   - The current OB_DFILE status **file** is coherent with the operation;
   - The **DAC is** coherent with the **security card status**;
3. SUB_GT performs the read / write operations in an OB_TLV if:
   - The **checksum TLV** of OB_TLV is correct;
   - The **DAC** is coherent with the **security card status**;

List of security attributes:

- Command header;
- Type of object;
- Checksum TLV;
- DAC;
- Security card status;
- File status;

FDP_ACF.1.3 /TLV The TSF shall explicitly authorize the access of subjects to objects according to the following complementary rules: **[posting: not applicable]**.

FDP_ACF.1.4 /TLV The TSF shall explicitly refuse the access of subjects to objects according to **[posting: Specific rules]**.

Assignment **Specific rules:**

1. SUB_GT never accesses an OB_TLV in deletion;

Iteration

FDP_ACF.1.1 The TSF shall apply the **[posting: SFP access control to secrets]** to objects according to

/SEC **[posting: the list of security attributes]**.

FDP_ACF.1.2 /SEC The TSF shall apply the following rules for determining whether an operation between controlled subjects and objects is authorized or not.

Assignment **Rules:**

1. SUB_APPLI activates SUB_GS for accessing OB_SECRET if **the command header** and the **type of object** are coherent;
2. SUB_GS performs the creation operation of an OB_SECRET in a current OB_DFILE if:
   - The status **file** of the OB_DFILE current is coherent for the operation;
   - Le **DAC** is coherent with the **security card status**;
3. SUB_GS accesses an OB_SECRET in write / read / unlocking / activation / deactivation / termination if:
   - The **secret** status of the OB_SECRET is coherent with the operation;
   - The **ratification group** or the **utilization counter** or the **error counter** of the OB_SECRET do not indicate that the secret is locked for read / write / activation / deactivation / termination operations;
   - The **DAC** of the secret agrees with the **security card status** for the operation**;**
4. SUB_GS performs the activation / desactivation and termination operations of an OB_SECRET if:
   - The **status of the secret** is coherent with operation;
   - The **DAC** of the secret is coherent with the **security card status**;
5. SUB_GS accesses the transfer of an OB_SECRET in the cryptographic processing blocks on behalf of SUB_CRYPTO if the:
   - **key type and algorithm type** are coherent;
   - **ratification group,** the **usage counter** or the **error counter** do not indicate that the secret is locked;
   - **checksum directory/file** containing OB_SECRET **is** correct;
   - **secret status** of secret OB_SECRET is "activated";
   - **DAC** of the secret OB_SECRET agrees with the **security card status;**

List of security attributes:

- Type of key;
- Type of algorithm;
- Ratification group;
- Checksum directory/file;
- DAC;
- Security card status;
- Secret status;
- File status;

FDP_ACF.1.3 /SEC The TSF shall explicitly authorize the access of subjects to objects according to the following complementary rules: **[posting: not applicable]**.

FDP_ACF.1.4 /SEC The TSF shall explicitly refuse the access of subjects to objects according to **[posting: Specific rules]**.

Assignment **Specific rules:**

1. SUB_GS never accesses, in read mode on behalf of SUB_APPLI, the values for symmetrical keys of private keys of asymmetrical bi-keys or of a PIN Code contained in OB_SECRET;
2. SUB_GS never accesses, in write mode, an OB_SECRET on behalf of SUB_APPLI, if the **security card status** does not indicate that an SMI and a SMC are valid;
3. SUB_GS never deletes an OB_SECRET;

SSCD Iteration

***FDP_ACF.1.1* /SFP Initialisation** The TSF shall apply the **[posting: SFP initialisation]** to objects according to **[posting: The group of general attributes]** and **[posting: The group of initialisation attributes]**.

***FDP_ACF.1.2* /SFP Initialisation** The TSF shall apply the following rules for determining whether an operation between controlled subjects and objects is authorized or not.

Assignment **Rules:**

1. The user for whom the security attribute role is defined at Administrator or at Signatory and for whom the security attribute **SCD/SVD management** is defined at Authorized may generate an SCD/SVD pair.

***FDP_ACF.1.3* /SFP Initialisation** The TSF shall explicitly authorize the access of subjects to objects according to the following complementary rules: **[posting: not applicable]**.

***FDP_ACF.1.4* /SFP Initialisation** The TSF shall explicitly refuse the access of subjects to objects according to **[posting: Specific rules]**.

Assignment **Specific rules:**

1. The user for whom the security attribute role is defined at Administrator or at Signatory and for whom the security attribute **management des SCD/SVD** is defined at Non-authorized may not generate an SCD/SVD pair.

SSCD Iteration

FDP_ACF.1.1 /SFP Personalization The TSF shall apply the **[posting: personalization SFP]** to objects according to **[posting: The group of general attributes]**.

FDP_ACF.1.2 /SFP Personalization The TSF shall apply the following rules for determining whether an operation between controlled subjects and controlled objects is authorized.

Assignment **Rules:**

1. The user for whom the security attribute role is defined at Administrator is authorized to create an RAD.

FDP_ACF.1.3 /SFP Personalization The TSF shall explicitly authorize the access of subjects to objects according to the following complementary rules: **[posting: not applicable]**.

FDP_ACF.1.4 /SFP Personalization The TSF shall explicitly refuse the access of subjects to objects according to **[posting: not applicable]**.

SSCD Iteration

FDP_ACF.1.1 /SFP SVD Transfer The TSF shall apply the **[posting: SFP Transfert of SVD]** to objects according to **[posting: The group of general attributes]**.

FDP_ACF.1.2 /SFP SVD Transfer The TSF shall apply the following rules for determining whether an operation between controlled subjects and controlled objects is authorized.

Assignment **Rules:**

1. The user for whom the security attribute role is defined at Administrator or at Signatory is authorized to export SVDs.

FDP_ACF.1.3 The TSF shall explicitly authorize the access of subjects to objects according to the

/SFP SVD Transfer following complementary rules: **[posting: not applicable]**.

FDP_ACF.1.4 /SFP SVD Transfer The TSF shall explicitly refuse the access of subjects to objects according to **[posting: not applicable]**.

SSCD Iteration

FDP_ACF.1.1 /SFP signature creation The TSF shall apply the **[posting: SFP signature creation]** to objects according to **[posting: The group of general attributes]** and **[posting: The group of signature creation attributes]**.

FDP_ACF.1.2 /SFP signature creation The TSF shall apply the following rules for determining whether an operation between controlled subjects and controlled objects is authorized.

<u>Assignment</u> **<u>Rules:</u>**

1. The user for whom the security attribute role is defined at <u>Signatory</u> is authorized to create electronic signatures for the DTBS sent by an authorized SCA, with SCDs by the Signatory for whom the **SCD operational** security attribute is defined at <u>Yes</u>.

FDP_ACF.1.3 /SFP signature creation The TSF shall explicitly authorize the access of subjects to objects according to the following complementary rules: **[posting: not applicable]**.

FDP_ACF.1.4 /SFP signature creation The TSF shall explicitly refuse the access of subjects to objects according to **[posting: Specific rules]**.

<u>Assignment</u> **<u>Specific rules:</u>**

(a) The user for whom the security attribute role is defined at <u>Signatory</u> is not authorized to create electronic signatures for the DTBS that are not sent by an authorized SCA, with Signatory SCDs for whom the **SCD operational** security attribute is defined at <u>Yes</u>.

(b) The user for whom the security attribute role is defined at <u>Signatory</u> is not authorized to create electronic signatures for the DTBS sent by an authorized SCA, with Signatory SCDs for whom the SCD operational security attribute is defined at <u>No</u>.

SSCD Iteration

FDP_ACF.1.1 /SFP SCD Importation The TSF shall apply the **[posting: SFP Importation of SCD]** to objects according to **[posting: The group of general attributes]** and **[posting: The group of initialisation attributes]**.

FDP_ACF.1.2 /SFP SCD Importation The TSF shall apply the following rules for determining whether an operation between controlled subjects and controlled objects is authorized.

<u>Assignment</u> **<u>Rules:</u>**

1. The user for whom the security attribute role is defined at <u>Administrator</u> or <u>Signatory</u> and with the **SCD/SVD Management** security attribute positioned at <u>Authorized</u> is authorized to import SCDs if the security attribute **Protected Importation of authorized SCD** is positioned at <u>Yes</u>.

FDP_ACF.1.3 /SFP SCD Importation The TSF shall explicitly authorize the access of subjects to objects according to the following complementary rules : **[posting: not applicable]**.

FDP_ACF.1.4 The TSF shall explicitly refuse the access of subjects to objects according to **[posting:**

/SFP SCD Importation **Specific rules]**.

Assignment **Specific rules:**

(a) The user for whom the security attribute role is defined at Administrator or Signatory and with the **SCD/SVD Management** security attribute positioned at Unauthorized is not authorized to import SCDs if the security attribute **Protected importation of authorized SCD** is positioned at Yes.
(b) The user for whom the security attribute role is defined at Administrator or Signatory and with the **SCD/SVD Management** security attribute positioned at Authorized is not authorized to import SCDs if the **Protected importation of authorized SCD** security attribute is positioned at No.

FDP_DAU.1 Authentification of elementary data

Iteration

FDP_DAU.1.1 The TSF shall offer a capacity to generate proof that may be used as a guarantee of the validity of **[posting: List of objects or types of following information]**

Assignment **List of objects and information:**

- OB_SECRET (keys and PIN codes);
- OB_FILE (contained file);
- OB_TLV (des data proprietary application);

FDP_DAU.1.2 The TSF shall offer to **[posting: list of subjects]** the ability to prove the validity of information indicated.

Assignment **List of subjects:**

- SUB_APPLI;
- SUB_GS;
- SUB_GT;
- SUB_GF;

SSCD Iteration

FDP_DAU.1.1 The TSF shall offer a capacity to generate proof that may be used as a guarantee of the validity of the **[posting: List of objects or types of following information]**

Assignment **List of objects and information:**

- SCD
- SVD;
- RAD;
- DTBS;

FDP_DAU.1.2 The TSF shall offer to **[posting: list of subjects]** the ability to verify the proof of the validity of the information indicated.

Assignment **List of subjects:**

- Signatory;
- Administrator;

FDP_ETC.1 Exportation of user data without security attributes

Iteration

FDP_ETC.1.1 The TSF shall apply the **[posting: list of SFP access control]** during exportation of user data, audited by the SFP(s), outwards from the TSC.

Assignment **List SFP access controls:**

- SFP access control to "IAS-eGOV" services;

- SFP access control to files;
- SFP access control to TLV parameters;
- SFP access control to secrets;

FDP_ETC.1.2 The TSF shall export user data without the security attributes associated with user data.

SSCD Iteration

FDP_ETC.1.1 /SVD Transfer The TSF shall apply the **[posting: SFP Transfert of SVD]** during exportation of user data, audited by the SFP(s), outwards from the TSC.

FDP_ETC.1.2 /SVD Transfer The TSF shall export user data without the security attributes associated with user data.

FDP_IFC.1 Partial Control of information flow

FDP_IFC.1.1 The TSF shall ensure the **[posting: SFP for control of information flow]** on all **[posting: list of subjects, information and operations that channel the flow of controlled information towards and away from controlled subjects covered by the SFP]**.

The SFP Data Processing Policy is defined for requirement FDP_IFC.1 (Partial Control of Information Flow): user data and TSF data shall not be accessible from the TOE except for when the smart card embedded software decides to communicate the user data via an external interface. The protection shall apply to confidential data only but without distinction between the attributes controlled by the smart card embedded software.

Assignment **SFP for controlling information flow:**

Data Processing Policy.

Assignment **List of subjects, information and operations that entail a controlled information flow towards and away from controlled subjects covered by the SFP:**

All confidential data when processed or transmitted by the TOE or the smart card embedded software.

Refinement: FDP.IFC.1 is refined for this composite assessment for including the resistance against secret information leaks as well (attacks by SPA, DPA, Timing) during the execution of DES, 3DES, SHA-1, RSA and RSA-CRT algorithms as well as during RSA key generation.

FDP_ITC.1 Importation of user data without security attributes

Iteration

FDP_ITC.1.1 The TSF shall apply the **[posting: list of access control SFP]** when importing user data checked by the SFP originating outside the TSC.

Posting **List of SFP access controls:**

- SFP access control to “IAS-eGOV” services;
- SFP access control to files;
- SFP access control to TLV parameters;
- SFP access control to secrets;

FDP_ITC.1.2 The TSF shall ignore all security attributes associated with user data when they are imported from outside of the TSC.

FDP_ITC.1.3 The TSF shall apply the following rules during importation of user data controlled by the SFP originating outside of the TSC **[complementary rules for importation control: not applicable].**

SSCD Iteration

FDP_ITC.1.1 /SCD The TSF shall apply the **[posting: SFP Importation of SCD]** during importation of use data controlled by the SFP originating outside of the TSC.

FDP_ITC.1.2 /SCD The TSF shall ignorer all security attributes associated with user data when they are imported from outside of the TSC.

FDP_ITC.1.3 /SCD The TSF shall apply the following rules during importation of user data controlled by the SFP originating outside of the TSC: **[The SCD must be sent by an authorized SSCD].**

SSCD Iteration

FDP_ITC.1.1 /DTBS The TSF shall apply the **[posting: SFP signature creation]** during importation of user data controlled by the SFP originating outside of the TSC.

FDP_ITC.1.2 /DTBS The TSF shall ignorer all security attributes associated with user data when they are imported from outside of the TSC.

FDP_ITC.1.3 /DTBS The TSF shall apply the following rules during importation of user data controlled by the SFP originating outside of the TSC: **[The DTBS representation must be sent by an authorized CSA].**

FDP_ITT.1 Basic internal transfer protection

Crypto library iteration

FDP_ITT.1.1 The TSF shall ensure **[posting: the SFP access control(s) and/or the SFP flow control(s)]** for preventing the **[selection: disclosure, modification, loss of utilization]** of user data when it is transmitted between physically separated parts of the TOE.

Assignment **SFP access control and/or SFP flow control:**

Data Processing Policy.

Selection Disclosure.

Refinement The different memories, the CPU and the other functional units of the TOE (e.g. a cryptographic co-processor) are considered as physically separated parts of the TOE.

FDP_ITT.1 is refined for this composite assessment to include resistance against secret information leaks as well (attacks by SPA, DPA, Timing) during execution of DES, 3DES, SHA-1, RSA and RSA-CRT algorithms as well as during RSA key generation.

Crypto library iteration.

Basic internal transfer protection requires that the user data be protected when it is transmitted between different parts of the TOE. The TOE provides a safe copy routine that copies the data blocks in such a way that they are protected against certain attacks by covert channels. The following functional requirement is derived from component FDP_ITT.1 of the **[R1 – CC]**:

FDP_ITT.1.1 /COPY The TSF shall ensure the **[posting: SFP access control and/or SFP control of information flow]** for preventing the disclosure of user data when it is transmitted between physically separated parts of the TOE.

Assignment **SFP access control and/or SFP information flow control:**

Data Processing Policy

Refinement The different TOE memories are considered as physically separated parts of the TOE. The TSF shall provide a safe copy routine that copies the data blocks in such a way that the confidentiality of the data is protected against certain attacks by covert channels.

FDP_RIP.1 Partial protection of residual information

Iteration

FDP_RIP.1.1 The TSF shall ensure that all information previously contained in a resource is rendered inaccessible upon **[selection: resource deallocation]** for the following objects **[posting: List of objects]**

Assignment **List of objects:**

- OB_SECRET;
- OB_FILE;
- OB_TLV;
- OB_I/O;
- OB_TEMP;

SSCD Iteration

FDP_RIP.1.1 The TSF shall ensure that all information previously contained in a resource is rendered inaccessible upon **[selection: resource deallocation]** of the following objects **[posting: List of objects]**

Assignment **List of objects:**

- SCD;
- VAD;
- RAD;

Crypto library iteration.

FDP_RIP.1.1 The TSF shall ensure that all previous information contained in a resource is rendered unavailable upon **[selection: resource deallocation]** for the following objects: **[Posting: all objects used by the cryptographic library as specified in the users guides]**.

FDP_SDI.2 Control of the audit trail data stored and action to be taken

Iteration

FDP_SDI.2.1 The TSF shall control the user data stored within the TSC for searching for **[posting: audit trail errors on checksum]** on all objects, based on the following attributes **[posting: List of attributes]**

Assignment **List of attributes**

- Directory and file checksum;
- Secret checksum;
- TLV checksum;
- I/O buffer checksum before and after a SUB_CRYPTO operation;

FDP_SDI.2.2 Should an audit trail error be detected, the TSF shall **[posting: refuse usage of corrupted data]**.

SSCD Iteration

FDP_SDI.2.1 /Persistent Data The TSF shall control user data stored within the TSC that seeks **[posting: audit trail errors]** on all objects, based on the following attributes **[posting: permanently stored**

data with audit trail review]

Refinement **Persistent Data[3]:**

- SCD;
- RAD;
- SVD (if permanently stored in the TOE);

FDP_SDI.2.2 / Persistent Data Should an audit trail error be detected, the TSF shall:

1. **[refuse usage of corrupted data**
2. **inform the Signatory of the audit trail error]**

Iteration

FDP_SDI.2.1 /DTBS The TSF shall audit user data stored within the TSC that seeks **[posting: audit trail errors]** on all objects, basing itself on the following attributes **[posting: data stored avec audit trail review]**

Refinement **Temporary Data[4]:**

- The representation of the DTBS;

FDP_SDI.2.2 /DTBS Should an audit trail error be detected, the TSF shall:

1. **[refuse usage of corrupted data**
2. **inform the Signatory of the audit trail error]**

FDP_UCT.1 Fundamental confidentiality of data exchanged

FDP_UCT.1.1 /Reception The TSF shall apply the **[SFP Importation of SCD]** in order to **[receive]** the objects in such way as to protect from any unauthorized disclosure.

FDP_UIT.1 Audit trail data exchange

SSCD Iteration

FDP_UIT.1.1 /SVD Transfer The TSF shall apply the **[SFP Transfert of SVD]** in order to be able to **[transmit]** user data in such a way as to avoid **[modification]** and **[insertion]** errors.

FDP_UIT.1.2 /SVD Transfer The TSF shall be able to determine upon reception of user data whether a **[modification]** or **[insertion]** have occurred.

SSCD Iteration

FDP_UIT.1.1 /TOE DTBS The TSF shall apply the **[signature creation SFP]** in order to be able to **[receive]** user data in such a way as to avoid **[modification]**, **[deletion]** and **[insertion]** errors.

FDP_UIT.1.2 /TOE DTBS The TSF shall be able to determine upon reception of user data whether **[modification]**, **[deletion]** or **[insertion]** have occurred.

5.2.4 Identification and authentification (FIA)

FIA_AFL.1 Management of an authentification failure

Iteration

FIA_AFL.1.1 The TSF shall detect the fact that **[posting: the numbers following]** unsuccessful authentification attempts have occurred in relation with **[posting: the authentification of users of the services of the** Morpho-Citiz 32 **card in user phase]**.

Assignment **Numbers of attempts:**

[3] Data permanently stored by the TOE display the user data attribute “data permanently stored with audit trail storage”

[4] The representation of the DTBS, temporarily stored by the TOE display the user data attribute “data stored with audit trail storage”

- 3 successive attempts to authentify the bearer;
- 5 successive attempts to authentify the issuer;

FIA_AFL.1.2 When the specified number of unsuccessful authentification attempts is reached or surpassed, the TSF shall **[posting: List of actions]**.

Assignment **List of actions:**

- PIN Code Blocking;
- PUK code Blocking;

SSCD Iteration

FIA_AFL.1.1 The TSF shall detect the fact that **[posting: the following number of]** unsuccessful authentification attempts have taken place following **[failures of consecutive authentification attempts]**.

Assignment **Number of attempts:**

- 5 successive authentification attempts by the signatory;

FIA_AFL.1.2 When the specified number of unsuccessful authentification attempts has been reached or surpassed, the TSF shall **[posting: block the RAD]**.

Refinement When the RAD is blocked, any new authentification attempt shall fail.

FIA_ATD.1 Definition of user attributes

Iteration

FIA_ATD.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[posting: List of security attributes]**

Assignment **List of security attributes:**

- File status;
- Secret status;
- Security card status;

SSCD Iteration

FIA_ATD.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[posting: RAD]**

FIA_UAU.1 Authentification programming

Iteration

FIA_UAU.1.1 The TSF shall authorize that **[posting: all actions passing through the TSF, except those identified below,]** are performed on behalf of the user before he is authentified.

Assignment **List of unauthorized actions prior to user authentification:**

- Creation or deletion of a directory or file;
- Life cycle management of a file;
- Generation or addition of a secret;
- Life cycle management of a secret;
- Writing or reading of confidential user data;

FIA_UAU.1.2 The TSF shall require every user to be successfully authentified prior to authorization of any other action passing through the TSF on behalf of this user.

SSCD Iteration

FIA_UAU.1.1 The TSF shall authorize that **[posting: List of actions]** are performed on behalf of the user before he is authentified.

Assignment **List of actions:**

1. User identification by means of the TSF required by FIA_UID.1;
2. Creation of a channel of trust between the TOE and a Type 1 SSCD by means of the TSF required by FTP_ITC/SCD importation;
3. The creation of a web of trust between the local user and the TOE by means of the TSF required by FTP_TRP.1/TOE;
4. The creation of a channel of trust between the SCA and the TOE by means of the TSF required by FTP_ITC.1/Importation des DTBS;

FIA_UAU.1.2 The TSF shall require that each user be successfully authentified prior to authorizing any other action passing through the TSF on behalf of this user.

Note The "local user" mentioned in the FIA_UAU.1.1 component is the user using the channel of trust provided between the SCA in the TOE environment and the TOE as mentioned by FTP_TRP.1/SCA and FTP_TRP.1/TOE.

FIA_UAU.3 Unforgeable authentification

FIA_UAU.3.1 The TSF shall **[selection: prevent]** the utilization of authentification data that have been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall **[selection: prevent]** the utilization of authentification data that have been copied by any other TSF user.

FIA_UAU.4 Single-use authentification mechanisms

Iteration

FIA_UAU.4.1 The TSF shall hinder the re-use of authentification data linked to **[posting: the list of authentifications]**.

Assignment **List of authentifications:**

- Issuer authentification;
- Domain authorities authentification.

SSCD Iteration

FIA_UAU.4.1 The TSF shall prevent the reutilization of authentification data linked to **[posting: the list of authentifications]**.

Assignment **List of authentifications:**

- Signatory Authentification;
- Administrator Authentification.

FIA_UID.1 Identification Programming

Iteration

FIA_UID.1.1 The TSF shall authorize that **[posting: All actions passing through the TSF]** are performed on behalf of the user before he is identified.

FIA_UID.1.2 The TSF shall require that every user be successfully identified prior to authorizing any other action passing through the TSF on behalf of this user.

SSCD Iteration

FIA_UID.1.1 The TSF shall authorize the **[posting: List of actions]** to be performed on behalf of the user before he is identified.

Assignment **List of actions:**

1. Creation of a channel of trust between the TOE and a Type 1 SSCD by means of

the TSF required by FTP_ITC.1/SCD Importation;

2. Creation of a web of trust between the local user and the TOE by means of the TSF required by FTP_TRP.1/TOE;
3. Creation of a channel of trust between the SCA and the TOE by means of the TSF required by FTP_ITC.1/Importation of the DTBS;

FIA_UID.1.2 The TSF shall require that every user be successfully identified prior to authorizing any other action passing through the TSF on behalf of this user.

FIA_USB.1 User-subject link

FIA_USB.1.1 The TSF shall link the appropriate user security attributes with the subjects acting on behalf of this user.

5.2.5 FMT Security Management

The following actions are undertaken on behalf of the FMT functions management.

SFR	Management Action	SFR	Management Action	SFR	Management Action
FAU_SAA.1	NA	FIA_AFL.1	a)	FMT_MTD.1	a)
FSC_CKM.3	a)	FIA_ATD.1	a)	*FMT_SMF.1*	*NM*
FCS_CKM.4	a)	FIA_UAU.1	a)	FMT_SMR.1	NA
FCS_COP.1	NM	FIA_UAU.3	NM	FPR_UNO.1	NA
FDP_ACC.2	NM	FIA_UAU.4	NM	FPT_FLS.1	NM
FDP_ACF.1	a)	FIA_UID.1	NA	FPT_PHP.3	NA
FDP_DAU.1	a)	FIA_USB.1	a)	FPT_SEP.1	NM
FDP_ETC.1	NM	FMT_MOF.1	a)	FPT_TDC.1	NM
FDP_ITC.1	a)	FMT_MSA.1	a)	FPT_TST.1	NA
FDP_RIP.1	NA	FMT_MSA.2	NM		
FDP_SDI.2	NA	FMT_MSA.3	a)		

NA : Not Applicable
NM : No Management (no management action identified in the criteria)
a) : CC Management Actions a) adopted

FMT_MOF.1 Administration of the behaviour of security functions

Iteration

FMT_MOF.1.1 The TSF shall restrict the ability to **[selection: determine the behaviour of, deactivate, activate, modify the behaviour of]** the **[posting: list of functions]** to **[posting: authorized identified role]** functions.

<u>**Assignment**</u> See Table 15: Behaviour/functions/roles

SSCD Iteration

FMT_MOF.1.1 The TSF shall restrict the ability to **[selection: activate]** the **[posting: signature creation function]** functions to the **[posting: Signatory]**.

Behaviour	Functions	Roles
Activate / deactivate	Initialisation operations	Pre-personalizer
Activate / deactivate	Personalization operations	Personalizer
Activate	Secret creation	Domain authorities or Issuer
Activate	Creation or deletion of directories or files	Domain authorities or Issuer
Activate	Life cycle management of files or directories	Domain authorities or Issuer
Activate	Life cycle management of a secret	Domain authorities or Issuer

Deactivated	Block a cryptographic key	Domain authorities or Issuer
Deactivated	Block PIN Code	Issuer
Activate	Change PIN Code	Issuer or bearer
Activated / Deactivated	Block a cryptographic key except for keys SCD/SVD	Domain authorities or Issuer
Activated / Deactivated	Block an SCD/SVD type cryptographic key	Issuer and signatory
Activate	Loading of a cryptographic key except for SCD/SVD keys	Domain authorities or Issuer
Activate	Generation or Loading of an SCD/SVD type cryptographic key	Issuer and signatory
Activate / Deactivate	Block application	Issuer

Table 15: Behaviour/functions/roles

FMT_MSA.1 Administration of security attributes

Iteration

FMT_MSA.1.1 The TSF shall implement the **[posting: list of access control SFP]** in order to restrict the **[posting: following administrators]** with regards to **[posting: execution of the following operations]** on the following security attributes:

Assignment **List of SFP access control:**

- SFP access control to "IAS-eGOV" services;
- SFP access control to files;
- SFP access control to TLV parameters;
- SFP access control to secrets;

The TSF shall restrict the:

- Issuer or the domain authority from re-initializing the PTC counter of the attribute **ratification group** and the attribute **utilization counter;**
- Issuer or the domain authority from modifying the **secret status** attribute to "Activated";
- Issuer from modifying the **application status** attribute**;**
- Issuer or the domain authority from charging the **file type**, **file status**, and **DAC** attributes during creation of a directory or of a file in a directory belonging to his domain;
- Domain authority or issuer from charging the **key type**, **DAC** and **secret status** attributes during addition of a secret.

SSCD Iteration

FMT_MSA.1.1 Administrator The TSF shall implement the **[posting: initialisation SFP and SFP Importation of SCD]** in order to restrict the **[administrator]** from **[modifying]** the **[SCD/SVD management and protected importation of authorized SCD]** security attributes.

FMT_MSA.1.1 Signatory The TSF shall implement the **[posting: SFP signature creation]** in order to restrict the **[Signatory]** from **[modifying]** the **[SCD operational]** security attributes.

FMT_MSA.2 Safe security attributes

FMT_MSA.2.1 The TSF shall ensure that solely safe values are accepted for security attributes.

FMT_MSA.3 Static initialisation attribute

Iteration

FMT_MSA.3.1 The TSF shall implement **[posting: the list of access control SFP]** in order to provide **[restrictive]** default values for security attributes that are used for applying the SFP.

Courtesy translation

Assignment **List of SFP access control:**

- SFP access control to “IAS-eGOV” services;
- SFP access control to files;
- SFP access control to TLV parameters;
- SFP access control to secrets;

Refinement **Creation of directories or files (SFP access control to files)**

- The “**file type**, **DAC**” attributes must be provided by the domain administrator or by the issuer during creation of directories or files;
- The “**key type**, **DAC**, **secret status**” attributes must be provided by the domain administrator or by the issuer when adding a key;
- The “**security card status**“ attribute is constructed dynamically according to successful authentifications and established channels of trust. When switching on the Morpho-Citiz 32 card, the **security card** status is at “none authentified“ and “no SM open.“

FMT_MSA.3.2 The TSF shall allow **[posting: no role]** to specify initial alternative values for replacing default values when an object or information are created.

SSCD Iteration

FMT_MSA.3.1 / SFP Initialization The TSF shall implement **[SFP initialisation]** and **[SFP signature creation]** in order to provide **[restrictive]** default values for the security attributes that are used for applying the SFP.

Refinement The SCD “**SCD operational”** security attribute is defined at No after generation of the SCD.

FMT_MSA.3.2 / SFP Initialization The TSF shall allow **[the Administrator]** to specify alternative initial values for replacing default values when an object or information are created.

SSCD Iteration

FMT_MSA.3.1 /SFP SCD Importation The TSF shall implement **[SFP Importation of SCD]** and **[SFP signature creation]** in order to provide **[restrictive]** default values for the security attributes that are used for applying the SFP.

Refinement The SCD “**SCD operational**“ security attribute is defined at No after SCD importation.

FMT_MSA.3.2 /SFP SCD Importation The TSF shall allow **[the Administrator]** to specify initial alternative values for replacing the default values when an object or information are created.

FMT_MTD.1 Management of TSF data

Iteration

FMT_MTD.1.1 The TSF shall restrict the ability to **[selection: change a default value, question, modify, delete, erase [posting: other operations]]** the **[posting: list of TSF data]** to **[posting: the authorized identified roles]**.

Assignment **Management of TSF data:**

- Modification of the PIN Code value by the issuer or by the bearer;
- Modification of the cryptographic key value by the issuer or the domain authority;
- Creation of a secret by the issuer or the domain authority;
- Blocking or deblocking of the cryptographic key by the issuer or the domain authority;

- Deblocking a PIN Code by the issuer;
- Blocking or deblocking of an application by the issuer;

SSCD Iteration

FMT_MTD.1.1 The TSF shall restrict the ability to **[modify [posting: not applicable]]** the **[RAD]** to the **[Signatory]**.

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 *The TSF shall be capable of implementing the following security management functions* ***[posting: FS_GESTION, FS_SEC]***

FMT_SMR.1 Security roles

Iteration

FMT_SMR.1.1 The TSF shall keep the **[posting: the authorized identified roles]** up to date.

Assignment **Authorized roles:**

- See Table 16

FMT_SMR.1.2 The TSF shall be capable of associating the users to roles.

SSCD Iteration

FMT_SMR.1.1 The TSF shall keep the **[Administrator]** and **[Signatory]** roles up to date.

FMT_SMR.1.2 The TSF shall be capable of associating users to roles.

Life cycle	Roles	Description
Initialisation (Phase 4 and 5)	Pre-personalizer (Administrator)	After successful user authentification, this role authorizes, in a secure environment, initialisation of the Morpho-Citiz 32 card.
Personalization (Phase 6)	Personalizer (Administrator)	After successful user authentification, this role authorizes TOE personalization, in a secure environment. This administrator may: – Create object files; – Charger and update user data and TSF;
End user (Phase 7)	Issuer (Administrator)	After successful issuer authentification, the user may: – Block /unblock an application (ADF); – Create a secret; – Modify the status of a secret during its life cycle; – Block /unblock a secret; – Load the value of a secret; – Create and delete files / directories;
End user (Phase 7)	Domain authority (Administrator)	After successful administrator authentification, the issuer may: – Modify the status of a secret during its life cycle; – Block /unblock a secret; – Create a secret; – Modify the status of a secret during its life cycle; – Block /unblock a secret; – Load the value of a secret; – Create and delete files / directories (domains) within an application;
End user (Phase 7)	Bearer (User)	This role has possibilities defined by the functionalities of the Morpho-Citiz 32 card. The possibilities available to the bearer depend upon the initialisation and personalization options.

Table 16: Authorized roles

5.2.6 (FPR) Protection of privacy

FPR_UNO.1 Non observability

Iteration

FPR_UNO.1.1 The TSF shall ensure that **[posting: all users]** may not observe the execution of **[posting: list of operations]** on **[posting: list of objects]** by **[posting: list of users or protected subjects]**

Assignment **Authorized roles:**

- See Table 17

SSCD Iteration

FPR_UNO.1.1 The TSF shall ensure that **[posting: all users]** may not observe the execution of **[posting: list of operations]** on **[posting: list of objects]** by **[posting: list of users or protected subjects]**

Assignment **Authorized roles:**

- See Table 18

Operations	List of objects	List of users or subjects
Updating	OB_SECRET	SUB_GS
Utilization	OB_SECRET	SUB_CRYPTO

Table 17: Privacy protection

Operations	List of objects	List of users or subjects
Generation	SCD/SVD	Signatory, Administrator
Utilization	SCD	Signatory
Updating	RAD	Administrator

Table 18: SSCD Privacy Protection

5.2.7 Protection of TOE (FPT) security functions

FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 The TSF shall perform a series of tests **[during start-up]** for proving the correct functioning of the security hypotheses provided by the abstract machine that forms the basis of the TSF.

FPT_EMSEC.1 TOE Emanation

This requirement is an extension of part 2 of the CC **[R1 – CC]** and originating from the PP **[R3 – SSCD T2]** and **[R4 – SSCD T3]**.

FPT_EMSEC.1.1 The TOE shall not emit **[covert channels]** exceeding **[limits of the state of the art]** allowing access to **[RAD et to SCD]**.

Refinement The limits of the state of the art are the limits currently expected for security assessments of "smart card" products at insurance level EAL 4+.

FPT_EMSEC.1.2 The TSF shall ensure that **[all users]** are incapable of using the following interface **[posting: external interface]** for gaining **[RAD]** and **[SCD]** access.

FPT_FLS.1 Failure with preservation of a safe status

FPT_FLS.1.1 The TSF shall preserve a safe status when the following types of failures result:**[List of defects]**

Assignment **Failure List:**

- Unexpected interruption of the TSF execution due to extraneous events (power supply, extraction);
- Faulty audit trail on memories;
- Faulty audit trail on proprietary applications;
- Faulty audit trail on E²PROM programmation;

Crypto library iteration.

FPT_FLS.1.1 The TSF shall preserve a safe status when the following error types occur : **[posting: list of TSF error types].**

Assignment **List of TSF error types:**

- Exposition to operating conditions that may be intolerable according to the TOLERANCE LIMITED TO ERRORS (FRU_FLT.2) requirement and where dysfunction may thus occur.
- Attacks by DFA on the DES, the TDES and the RSA-CRT.

Refinement The term "error" hereabove covers the "circumstances." The TOE prevents errors for the "circumstances," defined hereabove.

FPT_ITT.1 Basic internal transfer protection of TSF data

Crypto library iteration.

FPT_ITT.1.1 The TSF shall protect TSF data from **[selection: disclosure, modification]** when it is transmitted between separate parts of the TOE.

Selection Disclosure

Refinement The different memories, the CPU and the other TOE functional units (e.g. a cryptographic co-processor) are considered as separate parts of the TOE.

FPT.ITT.1 is refined for this composite assessment in order to include resistance against secret information leaks (attacks by SPA, DPA, Timing) as well during the execution of DES, 3DES, SHA-1, RSA and RSA-CRT algorithms as during the generation of RSA keys.

This requirement is equivalent to FDP_ITT.1 but concerns the TSF data instead of user data. It shall thus be understood that it refers to the same Data Processing Policy defined in FDP_IFC.1.

Crypto library iteration .

The basic internal transfer protection of TSF data requires that the TSF data be protected when it is transmitted between different parts of the TOE. The TOE provides a safe copy routine that copies data blocks in such a way that this data is protected against certain attacks by covert channels. The following functional requirement is derived from the FPT_ITT.1 component of **[R1 – CC]**:

FPT_ITT.1.1 /COPY The TSF shall ensure protection of TSF data in order to prevent its **[selection: disclosure, modification]** when it is transmitted between separate parts of the TOE.

<u>Selection</u> Disclosure

<u>Refinement</u> The different TOE memories are considered separate parts of the TOE. The TSF shall provide a safe copy routine that copies the data blocks in such a way that the confidentiality of this data is protected against certain attacks by covert channels.

FPT_PHP.1 Passive detection of a physical attack

FPT_PHP.1.1 The TSF shall detect without ambiguity a physical intrusion that may jeopardize the TSF.

FPT_PHP.1.2 The TSF shall be able to determine whether a physical intrusion in the TSF devices or in the TSF elements has occurred.

FPT_PHP.3 Resistance to a physical attack

FPT_PHP.3.1 The TSF shall resist **[posting: physical intrusion scenarios]** in the **[posting: List of TSF mechanisms or elements]** by automatically responding such that there be no violation of the TSP.

<u>Assignment</u> **<u>Physical intrusion scenarios on the following elements:</u>**

- Reduction of the clock frequency in order to stop the TOE during a specific operation;
- Raising of the clock frequency for corrupting the TOE;
- Temperature modification for the purpose of corrupting TOE operations;
- Modification of the current for the purpose of corrupting TOE operations;

Crypto library iteration.

FPT_PHP.3.1 The TSF shall resist **[posting: physical probing scenarios]** on the **[posting: list of TSF elements]** by automatically responding such that there is no infringement of the TSP.

<u>Assignment</u> **<u>Physical probing scenarios:</u>**

Physical manipulation and physical probing.

<u>Assignment</u> **<u>List of TSF elements:</u>**

The TSF

<u>Refinement</u> The TOE shall implement the appropriate measures for continually countering physical manipulations and the physical probing. Due to the nature of these attacks (especially manipulation), the TOE may in no way detect the attacks on all of its elements. Thus, permanent protection against these attacks is required, guaranteeing that the TSP may not be infringed at any time. Thus, an "automatic response" here means (i) it may suffer an attack at any time and (ii) countermeasures are provided at all times.

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interferences and intrusions by unsafe subjects.

FPT_SEP.1.2 The TSF shall apply a separation between the security domains of TSC subjects.

Crypto library iteration.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interferences and intrusions by potential attackers.

FPT_SEP.1.2 The TSF shall apply a separation between the security domains of TSC subjects.

Refinement The parts of the TOE that support the functional security requirements "Tolerance limited to errors" (FRU_FLT.2) and "Error with preservation of a safe status" (FPT_FLS.1) must be protected from interferences originating in the smart card embedded software.

FPT_TDC.1 Elementary coherence of TSF data inter TSF

Iteration

FPT_TDC.1.1 The TSF shall provide the capacity to interpret **[posting: the user keys and the bearer code]** in a coherent fashion when they are shared between the TSF and another trustworthy IT product.

FPT_TDC.1.2 The TSF shall use **[posting: the [R9 – E-ADMIN] specification]** in order to interpret the TSF data of another trustworthy IT product.

SSCD Iteration

FPT_TDC.1.1 The TSF shall provide the capacity to interpret **[posting: the users' SCD/SVD and the Signatory's code]** in a coherent fashion when they are shared between the TSF and another trustworthy IT product.

FPT_TDC.1.2 The TSF shall use **[posting: the [R9 – E-ADMIN] specification]** in order to interpret the TSF data of another trustworthy IT product.

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall execute a series of self tests **[during start-up]** in order to demonstrate the proper functioning of the TSF.

FPT_TST.1.2 The TSF shall provide authorized users the capacity to audit the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorized users the capacity to audit the integrity of executable code of the TSF in memory.

FPT_TST.2 Partial TOE security test

FPT_TST.2.1 The TSF shall perform a series of tests **[selection: during start-up, periodically during normal functioning, upon request by the authorized user and/or to conditions…]** in order to demonstrate the proper functioning of **[posting: functions and/or mechanisms].**

Selection Upon request by the authorized user.

Assignment **Functions and/or mechanisms:**

RNG material.

5.2.8 Web and Channels of Trust (FTP)

FTP_ITC.1 Inter-TSF Channel of trust

SSCD Iteration

FTP_ITC.1.1 /SVD Transfer The TSF shall provide a secure communication channel between itself and a distant **CGA** IT product that is logically distinct from other communication channels and that provides a sure identification of its terminations as well as protection against data modification or disclosure on the channel.

FTP_ITC.1.2 /SVD Transfer The TSF shall allow **[the remote protected IT product]** to initiate communication by the channel of trust.

FTP_ITC.1.3 /SVD Transfer The TSF **or the CGA** shall initiate communication by the channel of trust for **[SVD transfer]**.

SSCD Iteration

FTP_ITC.1.1 /Importation of DTBS The TSF shall provide a secure communication channel between itself and a distant IT product that is logically distinct from other communication channels and that provides sure identification of its terminations as well as protection against a data modification or disclosure on the channel.

FTP_ITC.1.2 /Importation of DTBS The TSF shall authorize the **CGA** to initiate communication through the channel of trust.

FTP_ITC.1.3 /Importation of DTBS The TSF or the **SGA** shall initiate communication through the channel of trust for signature of the DTBS representation.

SSCD Iteration

FTP_ITC.1.1 /SCD Importation The TSF shall provide a secure communication channel between itself and a distant IT product that is logically distinct from other communication channels and that provides sure identification of its terminations as well as protection against a modification or disclosure of data on the channel.

FTP_ITC.1.2 /SCD Importation The TSF shall allow **[the remote protected IT product]** to initiate communication by the channel of trust.

FTP_ITC.1.3 /SCD Importation The TSF shall initiate communication by the channel of trust for **[SCD importation]**.

SSCD Refinement The " secure distant IT product" mentioned is a Type 1 SSCD.

FTP_TRP.1 Web of trust

FTP_TRP.1.1 /TOE The TSF shall provide a web of communication between itself and a local user that is logically distinct from other webs of communication and that protects the identification from its extremities as well as protecting transferred data against modification or disclosure.

FTP_TRP.1.2 /TOE The TSF shall allow **[local users]** to initiate communication by the web of trust.

FTP_TRP.1.3 /TOE The TSF requires utilization of a web of trust for **[initial user authentification][posting: no other services]**.

5.2.9 Resource Utilization FRU

FRU_FLT.2 Tolerance limited to errors

FRU_FLT.2.1 The TSF shall ensure the functioning of all TOE capacities when the following errors occur: **[posting: list of error types]**.

<u>Assignment</u> <u>List of error types:</u>

Exposition under operating conditions that are not detected according to the “Error with preservation of a safe status (FPT_FLS.1)” requirement.

Refinement The term "error," hereabove means "circumstances." The TOE prevents errors for the "circumstances," defined hereabove.

5.3 TOE SECURITY INSURANCE REQUIREMENTS

The selected insurance security requirements correspond to assessment level EAL4 augmented by components ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

ADV_IMP.2 TSF implementation

Developer’s tasks

ADV_IMP.2.1D The developers shall provide a representation of the implementation of the entirety of the TSF.

Content and presentation of elements of proof

ADV_IMP.2.1C The representation of the implementation shall define the TSF in no uncertain terms with a sufficient level of detail so that it may be generated without supplementary design decision.

ADV_IMP.2.2C The representation of the implementation shall have internal coherence.

ADV_IMP.2.3C The representation of the implementation shall describe the relations between all **parts of the implementation.**

The evaluator’s tasks

ADV_IMP.2.1E The evaluator shall confirm that the information provided satisfies all requirements relatives to content and to presentation of elements of proof.

ADV_IMP.2.2E The evaluator shall determine that the **representation of the implementation** is a correct instantiation and fulfils the TOE functional security requirements.

<u>Dependencies</u> <u>List of dependencies</u>

- ADV_LLD.1, ADV_RCR.1, ALC_TAT.1;

ALC_DVS.2 Sufficient character of security measures

Developers’ tasks

ALC_DVS.2.1D The developers shall produce documentation relating to development security.

Content and presentation of elements of proof

ALC_DVS.2.1C The documentation relating to development security shall describe all measures of physical and organizational security affecting personnel and others necessary for protecting the confidentiality, design audit trail and TOE implementation in its development environment.

ALC_DVS.2.2C The documentation relating to development security shall provide elements of proof indicating that these security measures are applied during TOE development and maintenance.

ALC_DVS.2.3C The elements of proof shall justify the security measures providing the level of protection necessary for maintaining the TOE confidentiality and audit trail.

Evaluator Tasks

ALC_DVS.2.1E The evaluator shall confirm that the information provided satisfies all requirements relative to the content and to the presentation of elements of proof.

ALC_DVS.2.2E The evaluator shall confirm that the security measures are applied.

<u>Dependencies</u> **<u>No dependencies</u>**

AVA_MSU.3 Analysis and testing of unsafe statuses

Developer's tasks

AVA_MSU.3.1D The developers shall provide information documentation.

AVA_MSU.3.2D The developers shall document an analysis of the information documentation.

Content and presentation of elements of proof

AVA_MSU.3.1C The information documentation shall identify all possible TOE functioning modes (including the functioning following a failure or an operational error), their consequences and implications for maintaining secure functioning.

AVA_MSU.3.2C The information documentation shall be complete, clear, coherent and reasonable.

AVA_MSU.3.3C The information documentation shall list all assumptions regarding the anticipated environment.

AVA_MSU.3.4C The information documentation shall list all external security measures requirements, including the external audit procedure, physical and personal.

AVA_MSU.4.5C The analytical documentation shall prove the completeness of the information documentation.

The evaluator's tasks

AVA_MSU.3.1E The evaluator shall confirm that the information provided satisfies all requirements relating to the content and to the presentation of elements of proof.

AVA_MSU.3.2E The evaluator shall re-apply all configuration, installation and, selectively, other procedures, in order to confirm that the TOE may be configured and used safely by using only the guides provided.

AVA_MSU.3.3E The evaluator shall determine whether the utilization of the guides allows for detection of all unsure statuses.

AVA_MSU.3.4E The evaluator shall confirm that the analytical documentation demonstrates that the data for safe TOE operating advice in all operating modes is provided.

AVA_MSU.3.5E The evaluator shall perform independent tests in order to determine whether an administrator or a user, having acquired a solid understanding of the guides, would be reasonably capable of determining if the TOE is configured and operated in an unsafe manner.

<u>Dependencies:</u> **<u>List dependencies</u>**

- ADV_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD, USR.1;

AVA_VLA.4 High resistance

Developer's tasks

AVA_VLA.4.1D The developers shall perform a vulnerability analysis.

AVA_VLA.4.2D The developers shall produce the documentation relating to the vulnerability analysis.

Content and presentation of elements of proof

AVA_VLA.4.1C The documentation relating to the vulnerability analysis shall describe the analysis of the TOE deliverables in order to find the routes by which the user may violate the TSP.

AVA_VLA.4.2C The documentation relating to the vulnerability analysis shall describe the disposition of the vulnerabilities identified.

AVA_VLA.4.3C The documentation relating to the vulnerability analysis shall demonstrate for all vulnerabilities identified that the vulnerability may not be exploited in the desired TOE environment.

AVA_VLA.4.4C The documentation relating to the vulnerability analysis shall justify that, once the vulnerabilities identified, the TOE resistent to obvious penetration attacks.

AVA_VLA.4.5C The documentation relating to the vulnerability analysis shall demonstrate that the search for vulnerabilities is systematic.

AVA_VLA.4.6C The documentation relating to the vulnerability analysis shall provide justification that the analysis completely takes into consideration the TOE supplies.

The evaluator's tasks

AVA_VLA.4.1E The evaluator shall confirm that the information provided satisfies all requirements relating to content and to the presentation of elements of proof.

AVA_VLA.4.2E The evaluator shall conduct penetration tests, constructed on the developer's vulnerability analysis, in order to guarantee that the vulnerabilities identified have been addressed.

AVA_VLA.4.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.4.4E The evaluator shall perform independent penetration tests based on the independent vulnerability analysis, in order to determine whether the additional vulnerabilities identified may be exploited in the desired environment.

AVA_VLA.4.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker with a high attack potential.

Dependencies: **List of dependencies**

- ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1;

5.4 EXTENSION OF FUNCTIONAL SECURITY REQUIREMENTS

The additional FPT_EMSEC family (emanation of the TOE) of the FPT class (TSF protection) is defined herein in order to describe the IT functional security requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data when the attack is based on the external observation of physical phenomena of the TOE. For example, such attacks correspond to the assessment of TOE electromagnetic radiation, of the simple power analysis (SPA), of the differential power analysis (DPA), of the timing of the attack, etc. This family describes the functional requirements for limiting the emanations that may be exploited. The description of this family is that presented in the PP **[R3 – SSCD T2]** and **[R4 – SSCD T3]**.

The FCS_RND family, stemming from PP **[R5 – BSI0002]** and targets **[R15 – CLST]** and **[R14 – HWST]**, describes the functional requirements for generating random numbers for cryptographic purposes:

- FCS_RND.1 requires that the random numbers have a certain metric quality. The description of this requirement is presented in PP **[R5 – BSI0002]**.
- FCS_RND.2 requires that the generation of random numbers be based on a given standard. This requirement is described below:

FCS_RND.2 Random number generation

FCS_RND.2.1 The TSF shall provide a mechanism for random number generation that respects: **[Posting: list of standards]**.

Subordination: To no other component.

Dependencies: No dependencies.

FPT_TST.2 is an additional component of the FPT_TST family of part 2 of **[R1 – CC]**. It provides the ability for testing the proper working of the special security functions or mechanisms, as well as the ability to verify the audit trail of the TSF data and executable code. This requirement is described below.

FPT_TST.2 Partial TOE security test

FPT_TST.2.1 The TSF shall perform a series of auto-tests **[selection: during start-up, periodically during normal functioning, upon request by the authorized user and/or to [posting: conditions at which the auto-tests must be executed]** in order to demonstrate the correct functioning of the **[posting: functions and/or mechanisms].**

Superior to: No other component.

Dependencies : FPT_AMT.1.

5.5 IT ENVIRONMENT SECURITY REQUIREMENTS

5.5.1 IT environment security requirements stemming from [R15 – CLST]

Certain requirements defined in security target **[R15 – CLST]** pertain to the embedded software, i.e. to the TOE of the present security target. With regards to these requirements, they are covered by TOE requirements defined in § 5.2.

FCS_CKM.1 Cryptographic key generation

This requirement is covered by requirement FCS_CKM.1 au § 5.2

FCS_CKM.2 Cryptographic key distribution

Not applicable in the present case. No cryptographic keys are exported from the TOE.

FCS_CKM.4 Cryptographic key destruction

This requirement is covered by requirement FCS_CKM.4 au § 5.2

FDP_ITC.1 Importing user data without security attributes

This requirement is covered by requirement FDP_ITC.1 au § 5.2

FMT_MSA.2 Secured security attributes

This requirement is covered by requirement FMT_MSA.2 au § 5.2

FMT_SMR.1 Security roles

This requirement is covered by requirement FMT_SMR.1 au § 5.2

5.5.2 IT environment security requirements stemming from the SSCD profile

5.5.2.1 Generation of signature key (Type 1 SSCD)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in compliance with the cryptographic key generation algorithm **[affectation: List of key generating algorithms]** and to specified cryptographic key sizes **[affectation: Sizes of associated keys]** that respect the **[List of standards]**.

Assignment **See Table 19**

List of key generation algorithms	Key sizes	List of standards
RSA key generation	1024 to 2048 bits	AREA-K **[R10 – AREAK1]**, **[R11 – AREAK2]**

Table 19: Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 /Type 1 The TSF shall destroy the cryptographic keys in compliance with a specified **[posting: a cryptographic key destruction method]** that satisfies the following standards: **[deletion from the memory containing the key]**

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 /CORRESP The TSF shall execute **[posting: auditing of SCD/SVD correspondence]** in compliance with a cryptographic algorithm **[posting: RSA key calculation]** and with specified cryptographic key sizes **[posting: from 1024 to 2048 bits]** that satisfy the following: **[posting: Signature PKCS#1 V2.1 – padding v 1.5]**.

FDP_ACC.1 Partial access control

FDP_ACC.1.1 /SFP SCD The TSF shall apply the **[SFP exportation of SCD]** during **[SCD exportation by the administrator]**.

Exportation

FDP_UCT.1 Elementary confidentiality of data exchanged

FDP_UCT.1.1 /Exportation The TSF shall apply the **[SFP Exportation of SCD]** in order to be able to **[transmit]** the objects in such a way as to protect against any unauthorized disclosure.

FTP_ITC.1 Inter-TSF Channel of trust

FTP_ITC.1.1 /SCD Exportation The TSF shall provide a secure communication channel between itself and a distant IT product that is logically distinct from other communication channels and that provides sure identification of its terminations as well as protection against modification or disclosure of data on the channel.

FTP_ITC.1.2 /SCD Exportation Les TSF shall allow **[the remote protected IT product]** to initiate communication by the channel of trust.

FTP_ITC.1.3 /SCD Exportation The TSF shall initiate communication by the channel of trust for **[SCD exportation]**.

SSCD Refinement The "remote secure IT product" mentioned is a Type 2 SSCD.

5.5.2.2 Certificate Generation Application (CGA)

FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 /CGA The TSF shall distribute cryptographic keys according to a cryptographic key distribution method in compliance with qualified certificates and in respect of the following rules: **[posting: [R10 – AREAK1], [R11 – AREAK2]]**.

FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 /CGA The TSF shall perform **[SVD importation]** in compliance with a cryptographic key access method to **[cryptographic key importation through a channel of trust]** in respect of the following rules: **[affectation: [R10 – AREAK1], [R11 – AREAK2]]**.

FDP_UIT.1 Data exchange audit trail

FDP_UIT.1.1 /SVD Importation The TSF shall apply the **[SFP for SVD importation]** in order to be able to receive user data protected against **[modification]** and **[insertion]** errors.

FDP_UIT.1.2 /SVD Importation The TSF shall be able to determine upon reception of user data whether **[modification]** or **[insertion]** have occurred.

FTP_ITC.1 Inter-TSF Channel of trust (FTP_ITC.1)

FTP_ITC.1.1 /SVD Importation The TSF shall provide a secure communication channel between itself and a distant IT product, logically distinct from other channels of communication and that provides sure identification of its terminations as well as protection against modification or disclosure of data on the channel.

FTP_ITC.1.2 The TSF shall allow **[the TSF]** to initiate communication by the channel of trust.

/SVD Importation

FTP_ITC.1.3 /SVD Importation The TSF **or the TOE** shall initiate communication by the channel of trust for **[SVD importation]**.

5.5.2.3 Signature Creation Application (SCA)

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 /Hash of the SCA The TSF shall execute **[DTBS Hash calculation]** in compliance with a cryptographic algorithm specified at **[posting: in [R10 – AREAK1], [R11 – AREAK2] and [R13 – ERRATUM]]** and with the sizes of the cryptographic keys that respect the following rules: **[posting: [R10 – AREAK1], [R11 – AREAK2]]**.

FDP_UIT.1 Data exchange audit trail

FDP_UIT.1.1 /DTBS of the SCA The TSF shall apply the **[SFP signature creation]** in order to be able to transmit user data in such manner as to avoid **[modification]**, **[deletion]** and **[insertion]** errors.

FDP_UIT.1.2 /DTBS of the SCA The TSF shall be able to determine upon reception whether **[modification]**, **[deletion]** or **[insertion]** have occurred within user data.

FTP_ITC.1 Channel of trust inter-TSF

FTP_ITC.1.1 /DTBS of the SCA The TSF shall provide a secure communication channel between itself and a distant IT product, logically distinct from other communication channels and that provides sure identification of its terminations as well as protection against modification or disclosure of data on the channel.

FTP_ITC.1.2 /DTBS of the SCA The TSF shall authorize **[the TSF]** to initiate the communication by the channel of trust.

FTP_ITC.1.3 /DTBS of the SCA The TSF **or the TOE** must initiate communication by the channel of trust for **[signature of the representation of the DTBS by the SSCD]**.

FTP_TRP.1 Web of trust

FTP_TRP.1.1 /SCA The TSF shall provide a web of communication between itself and a local user logically distinct from other communication webs and that provides sure identification of its terminations as well as protection against data modification or disclosure.

FTP_TRP.1.2 /SCA The TSF shall allow **[the TSF]** to initiate the communication by the web of trust.

FTP_TRP.1.3 /SCA The TSF requires the utilization of a web of trust for **[initial user authentification][posting: no other services]**.

5.6 NON IT ENVIRONMENT SECURITY REQUIREMENTS

5.6.1 Non IT environment security Requirements stemming from [R3 – SSCD T2] and [R4 – SSCD T3]

R.Administrator_Guide *Application of administrator information*

The implementation of the requirements of the Directive, ANNEXE II, “Requirements concerning certification service providers delivering qualified certificates," stipulates at para. (e) that the employees of CSP or of other corresponding entities shall respect the information of the administrator provided by the TOE. An audit adapted by the CSP or from other corresponding entities shall ensure the current compliance.

R.Sigy_Guide *Application of user information*
The implementation of the CSPP according to the requirements of the Directive, ANNEXE II “Requirements concerning the certification service providers delivering qualified certificates," stipulates at para. (k) that the signatory shall respect the TOE user information.

R.Sigy_Name *Signatory name on the qualified certificate*
The CSP shall verify the identity of the person to whom a qualified certificate is delivered in compliance with Directive [1], ANNEXE II “Requirements concerning the certification service providers delivering qualified certificates," para. (d). The CSP shall verify that this person holds a SSCD that implements the SCD corresponding to SVD to be included in the certificate qualified.

5.6.2 Non IT environment security requirements stemming from [R15 – CLST]

RE.Phase-1 *Conception and implementation of the smart card embedded software*
The developers smart card embedded software shall create and implement the smart card embedded software in such manner that the following documents requirements are satisfied: (i) the TOE data sheet material; (ii) the TOE application notes and (iii) the conclusions of the assessment reports of the relevant cryptographic library for the smart card embedded software.
The developers must implement the smart card embedded software in such manner that the user data (especially the cryptographic keys) is protected, as required by the security needs of the specific context of the application.

RE.Cipher *Coding Diagramme*
The smart card embedded software developers must not implement any routine in a manner that will compromise the keys when the routines are executed as part of the smart card embedded software. Executing functions that access cryptographic keys could allow an attacker to divert these functions in order to gather information on the key used during the calculation of the function.
The keys must be kept secret as soon as they are generated. The keys must be unique with a very high probability as well as cryptographically strong. For example, it must be ensured that it is not possible to derive the private key of the public key if asymmetrical algorithms are used. If keys are imported into the TOE and/or derived from other keys, the quality and the confidentiality must be maintained. This implies performing appropriate environmental key management.

RE.RNG2 *Random numbers testing*
Smart card embedded software developers must call up the RNG material test routines in an apppropriate manner. These routines are implemented in the cryptographic library prior to using random numbers generated by the RNG material. The operating system shall be especially sure that, prior to utilizing random numbers generated by the RNG software, the RNG software initialisation is routine called up. This routine performs on line tests of the RNG material and uses the tested RNG material for initializing the RNG software.
The random number generator software uses an internal XRAM buffer. The smart card embedded software shall insure that this buffer is read or written by the cryptographic library only during utilization of the cryptographic library, i.e., from testing of the RNG material up through the last call of whatever cryptographic library routine.

6. TOE GENERAL SPECIFICATIONS

6.1 COMPONENT LEVEL SECURITY FUNCTIONS

F.RNG
The random number generator produces random numbers continuously.

F.HW_DES
The TOE provides the TDES algorithm (as described in the FIPS PUB 46) thanks to a material co-processor.
F.HW_DES has a high SOF.

F.OPC
The F.OPC function ensures proper TOE functioning during execution of support software dedicated to the integrated circuit and to the smart card embedded software. This includes all specific security characteristics of the TOE that are capable of providing an active response.

F.LOG
The F.LOG function implements measures geared to limiting or eliminating information that may be contained in the form and amplitude of signals or in the intervals of time between events found while measuring such signals.

6.2 LOW LEVEL SECURITY FUNCTIONS

FS_CHECKSUM
Generation of a checksum in order to ensure the audit trail integrity.
FS_CHECKSUM has a high SOF.

FS_PHYS
Physical protection against the external intrusion type attacks.

FS_RANDOM
Random number generation function of an octet length n.

FS_CAPTOR
This function manages the exceptions and the indicators gathered and reported by F.OPC.

6.3 OS LEVEL SECURITY FUNCTIONS

FS_CHECK
This function tests the integrity of TOE sensitive elements.

FS_TEST
This function tests part of the TOE start.

FS_MEMOIRE
This function manages deletion of the E²PROM memory.

FS_INIT

This function is called up after each reset and performs:

- The TOE test by calling up the FS_TEST function;
- ATR issue;
- Initialisation of all software modules and applications.

FS_BACKUP

This function ensures that all write operations are properly executed.

FS_OTP

This function manages the OTP zone in E^{2}PROM memory.

FS_ACCES

This function manages access to files, directories, proprietary data (TLV) and to keys stored en E^{2}PROM.

FS_AUDIT

The function FS_AUDIT provides for reaction to an anomaly or a detected flaw.

6.4 CRYPTO LIBRARY LEVEL SECURITY FUNCTIONS

F.LOG_CL

F.LOG_CL is a complement to the F.LOG at the software level.
F.LOG_CL contains software countermeasures for attacks by covert channels.

F.RNG_Access

The TOE contains both RNG material and RNG software. F.RNG_Access consists of an RNG software implementation and appropriate RNG material on line tests.

F.DES

F.DES is a cryptographic function that provides the DES algorithm as defined by the FIPS PUB 46-3 standard and supports the 2 and 3 key Triple DES algorithms according to the ANSI X9.52 standard.
F.DES has a high SOF.

F.RSA

The TOE provides functions that implement the RSA and RSA-CRT algorithms as described in Schneier, page 468 or Menezes, van Oorshot and Vanstone, section 8.2, as well as the ISO/IEC 9796 [24] Annexe A, section A.4 standard.
F.RSA has a high SOF.

F.SHA-1

The TOE implements functions for calculating the SHA-1 algorithm according to the FIPS 180-1 standard.
F.SHA-1 has a high SOF.

F.RSA_KeyGen

The TSF F.RSA_KeyGen provides the functionality for generating pairs of RSA public keys as described in Regulierungsbehörde für Telekommunikation und Post: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German “Bundesanzeiger Nr. 30”, p.2537-2538, February 13th, 2004.
F.RSA_KeyGen has a high SOF.

F.Object_Reuse

The TOE provides internal security measures that delete memory zones used by the cryptographic library after usage.

F.COPY
F.COPY implements the memory content copy functionality by using a routine that includes countermeasures against attacks by covert channels.

6.5 APPLICATION MANAGER LEVEL SECURITY FUNCTIONS

FS_MANAGEMENT
Upon starting the card, this function calls up FS_INIT and then waits for a terminal command. This command is either processed or redirected towards another element.
In particular, the function manages:

- selection of an application;
- the status of the security card;
- security function applications.

6.6 APPLICATIVE LEVEL SECURITY FUNCTIONS

FS_AUTH
This function manages the authentifications of different TOE users on the basis of secrets authentification associated with different users (call to FS_CRYPTO).
FS_AUTH has a high SOF.

FS_RATIF
This function manages the ratification counters associated with a secret.

FS_CRYPTO
This function ensures high level cryptographic operations:

- Data Encryption/Decryption;
- Production/verification of authentification cryptogrammes;
- Audit trail inspection of cryptographic keys and data;
- Generation of secure electronic signature on external data;
- Calculation of hash value;
- PIN Code Verification.

FS_CRYPTO calls up F.DES, F.RSA and F.SHA-1 for performing these cryptographic operations.
FS_CRYPTO has a High SOF.

FS_SEC
This function allows for ensuring secrets management. Secrets management includes the following functions:

- Electronic signature bi-key generation;
- Session key generation;
- Key destruction;
- Secret modification;
- Secret transfer;
- Secret unlocking.

FS_SEC calls up F.COPY for manipulating secrets and F.RSA_KeyGen for generating RSA bi-keys in RSA-CRT format.
FS_SEC has a High SOF.

FS_COMMAND
When the manager receives a command, he dispatches it to a processing application. The FS_COMMAND function implemented in the applications then performs the following:

- Command validity test;
- Tests concerning the command semantics;

7. PP COMPLIANCE NOTICE

7.1 PP REFERENCE

The present security target complies with protection profiles **[R3 – SSCD T2]** and **[R4 – SSCD T3]**.

The distribution between these two protection profiles for the assumptions, threats, TOE Security Objectives and its environment as well as for TOE functional security requirements are presented in the following tables:

- Table 5: ST/PP Correspondences – assumptions for the TOE;
- Table 6: ST/PP Correspondences – threats for the TOE;
- Table 10: ST/PP Correspondence – TOE Security Objectives ;
- Table 11: ST/PP Correspondence – Security Objectives for the TOE environment ;
- Table 12: ST/PP Correspondence–TOE security .

7.2 PP ADDITIONS

In the present security target, the additions to the following security requirements have been made to the security requirements of protection profiles **[R2 – 9911]**, **[R3 – SSCD T2]** and **[R4 – SSCD T3]** and of the target **[R15 – CLST]** already present in the present security target:

- FMT_SMF: Specification of management functions

The additions to the security requirements are presented in "*italics*" in the following chapters and tables:

- Chapter 5.2.5: FMT Security
- Table 12: ST/PP Correspondence–TOE security .

END OF DOCUMENT