MICROELECTRONICA
ESPAÑOLA

Tarjeta Electrónica del Ministerio de Defensa (M.MAR TEMDv1.0)

SECURITY TARGET

Version: 1.01, EAL 4+
(Public Version)

THIS PAGE WAS INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

REVISION HISTORY

Revision history			
Version	**Date**	**Author**	**Comments**
1.01	24/01/06	Área de Seguridad	Public ST_Lite.

1. INTRODUCTION

This section provides document management and overview information for this document required to identify uniquely this Security Target (ST).

Section 1.1 “Identification and purpose” gives labelling and descriptive information necessary for registering this ST. Section 1.2 “Overview” summarises this ST in narrative form. As such, this section gives an overview to the potential user to decide whether a particular device evaluated in compliance with this ST satisfies all of the expected requirements. Section 1.3 “CC compliance” describes the compliance of this ST with CC.

1.1. Identification and purpose

This document is the Security Target (ST) for the Common Criteria (CC) evaluation of the Tarjeta Electrónica del Ministerio de Defensa (M.MAR TEMDv1.0), which is the Target of Evaluation (TOE). The author of this ST and developer of the TOE Operating System is Microelectrónica Española.

This ST complies with the “Secure Signature-Creation Device Type 3 Protection Profile” (SSCD PP) [6]. Sections not appearing in this ST are those which do not contribute anything new to the content of that PP.

The PP has been written in accordance with CC v2.1 and the ST respecting CC v2.2 [2, 3, 4].

1.2. Overview

The framework for this Security Target (ST) is the project for the development of a secure smart card for the Ministry of Defence.

The intent of this ST is to specify the necessary functional and assurance requirements for the Tarjeta Electrónica del Ministerio de Defensa (M.MAR TEMDv1.0) which is the target of evaluation (TOE). A smart card evaluated according to this ST will be granted to comply with all specified requirements for M.MAR TEMD.

The Target of Evaluation (TOE) is the Tarjeta Electrónica del Ministerio de Defensa (M.MAR TEMDv1.0), which satisfies the top requirements in terms of performance and security. The Operating System for the TOE has been developed by Microelectrónica Española, and its use is oriented towards environments and applications with special security requirements. In particular, a device evaluated in accordance with this ST shall comply with the requirements established in the Directive 1999/93/CE of the European Parliament and the Council of 13 December 1999 on a community framework for electronic signature [1]. This Directive is the generally recognised standard for electronic signature products in the Official Journal of the European Communities.

This ST defines the security requirements of the TOE for the generation of signature-creation data (SCD), the creation of qualified electronic signatures and the encryption of data.

The assets, threats, security objectives and security functional requirements are defined in the Protection Profile “Secure Signature-Creation Device Type 3 Protection Profile” [6] and are referenced here. These constitute the minimal requirements for any electronic-signature product.

The security functions of the TOE are defined in this ST. Also, this particular TOE is proven to comply with the requirements defined in the PP.

1.3. CC Compliance

This ST has been written in compliance with parts 2 (extended with requirement FPT_EMSEC.1) and 3 of the CC [3, 4]. The assurance level for this ST is EAL4 augmented with components AVA_VLA.4 and AVA_MSU.3. The minimum strength level for the TOE security functions is 'SOF high' (Strength of Functions High), however, the algorithm strength of the cryptographic mechanisms is not part of the evaluation.

This ST complies with the “Secure Signature-Creation Device Type 3 Protection Profile” [6].

2. TOE DESCRIPTION

The description of the TOE helps to understand the specific security requirements. The following is a more detailed description of the TOE than the one given in the SSCD PP, as it refers to a particular TOE.

2.1. Product Type

The Target of Evaluation (TOE) is the Tarjeta Electrónica del Ministerio de Defensa (M.MAR TEMDv1.0), developed upon the SLE66CX322P Smart Card Integrated Circuit produced by INFINEON TECHNOLOGIES AG, with a smart card Operating System developed by Microelectrónica Española, the use of which is oriented towards environments and applications with special security requirements.

The term **Integrated Circuit (IC)** is used in this document to indicate the hardware and firmware of the device over which the software is developed. The Integrated Circuit has been evaluated and certified in accordance with CC, as is proven in documents Certification Report BSI-DSZ-CC-0223-2003 for Infineon Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a24, m1484a27 and m1484b14 from Infineon Technologies AG. [7] and Smart Card Security Target [8]. This integrated circuit corresponds to version m1484b14 Release GDS-file-ID: m1484b14 with production line indicator: “2” (Dresden) and uses libraries RMS V1.3 and RSA2048 V0.44.

The operating system of the TOE includes code that will be stored in the EEPROM memory of the IC. This code is supplied in file INI_TEMD_V1_0.TST.

The functional features of the TOE are constituted by operative management of the smart card issues as well as administrative management issues. The Especificación Funcional del Sistema Operativo M.MAR TEMDv1.0 [9] can be consulted.

The operating system of the TOE is formed by different layers that manage specific parts of the IC as is illustrated in Figure 1.

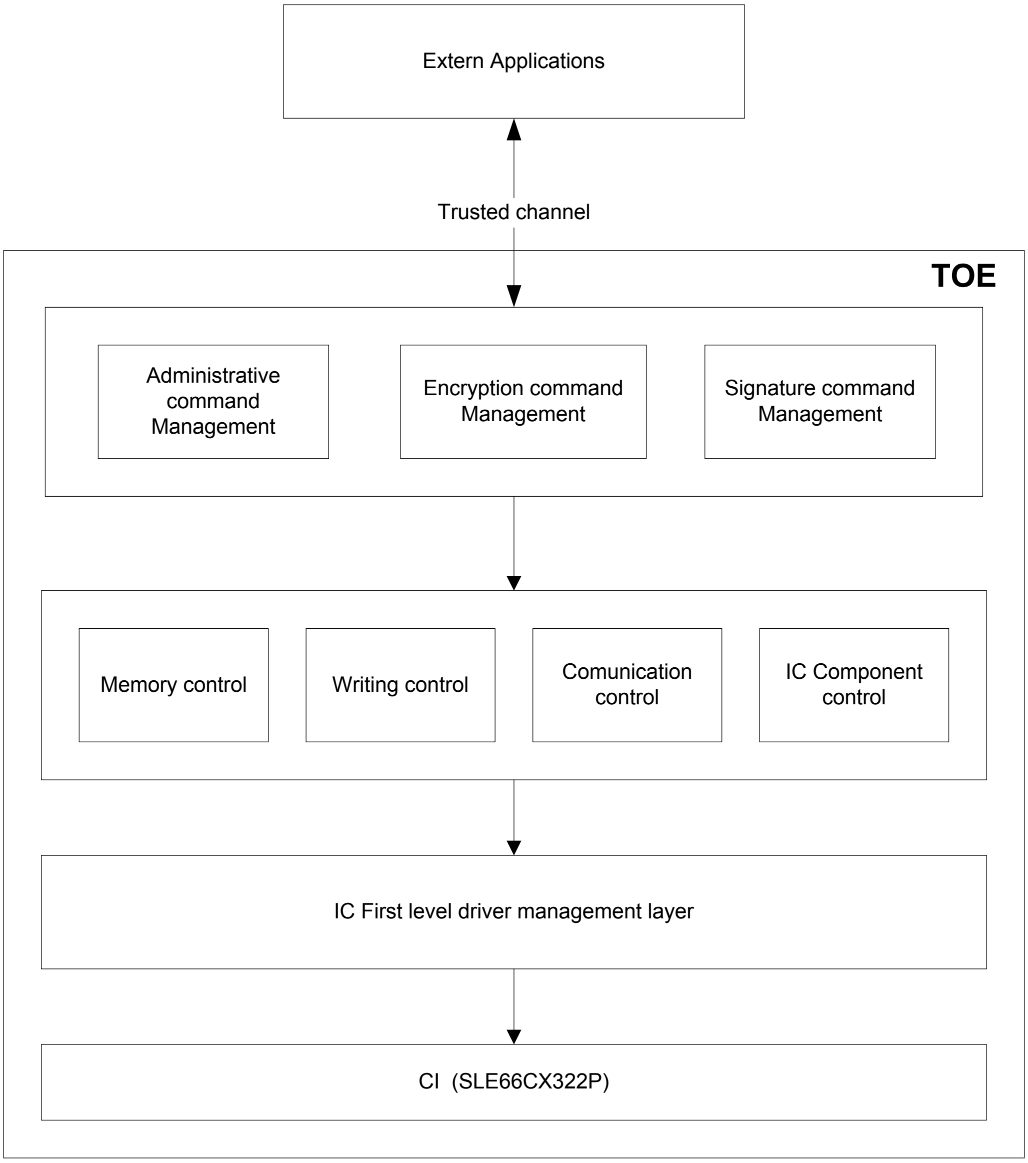
Extern Applications
Trusted channel
TOE
Administrative command Management
Encryption command Management
Signature command Management
Memory control
Writing control
Comunication control
IC Component control
IC First level driver management layer
CI (SLE66CX322P)

Figure 2-1: TOE layer description

The **IC first level driver management layer** is made up of functions that access the IC directly, creating an interface with the upper layers. These drivers control the following components of the IC: ROM, PROM, EEPROM, RAM, MMU, RMS, PLL, TIMER, STS, Random Number Generator, DES Coprocessor and Advanced Crypto Engine.

The **memory control** manages non-volatile memory including application structures such as file structures managed by the operating system.

The **writing control** manages all writing operations made on non-volatile memory, generating a different interface that can only be used by layers above or at the same level. The functions of this interface are based mainly on the driver that performs writing on EEPROM and RAM of the lower level.

The **communication control** manages communication protocol T=0, creating a communication interface for the upper layers. The functions of this interface are based mainly on the drivers that control the UART on the lower level layer.

The **IC component control** generates the interface to be used by layers above and at the same level when operating with IC specific components such as the random number generator, the DES coprocessor or the crypto-engine. Functions in this interface are based on the lower level drivers.

To be distinguished on the upper layer are:

- The **Administrative command Management** is the layer connected to the management of the operating system.
- The **Signature command Management**, the objective of which is to serve as a basis for signature cryptographic operations.
- The **Encryption command Management**, whose objective is to serve as a basis for data encryption and decryption operations.

2.2. Limits of the TOE

The TOE is a secure signature-creation device (SSCD type3) according to Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1]. The destruction of the signature creation data (SCD) is mandatory before the TOE can generate a new pair of signature creation data/signature verification data (SCD/SVD).

The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures:

1. to generate the signature creation data (SCD) and the correspondent signature-verification data (SVD)
2. to create qualified electronic signatures:
   a) after allowing for the data to be signed (DTBS) to be displayed correctly by the appropriate environment.
   b) using appropriate hash functions agreed as suitable for qualified electronic signatures.
   c) after appropriate authentication of the signatory by the TOE.
   d) using an appropriate cryptographic signature function that employs appropriate cryptographic parameters agreed as suitable.

The TOE implements all security functionalities which are necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control.

This ST assumes that the Signature Creation Application (SCA) is part of the environment of the TOE.

The SSCD protects the SCD during the whole life cycle of the card as to be solely used in the signature creation process by the legitimate signatory. The TOE will be initialised for the signatory's use by:

1. Generating a SCD/SVD pair
2. Personalisation for the signatory by means of the signatory's verification authentication data (SVAD).

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP). The TOE will destroy the SCD if it is no longer used for signature generation.

The TOE allows user authentication by means of a trusted human interface (HI) device connected via a trusted channel with the TOE. The HI device is used for the input of verification authentication data (VAD) for authentication by knowledge. The TOE holds reference authentication data (RAD) to check the provided VAD.

In addition to being a Secure Signature Creation Device (SSCD) according to Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a community framework for electronic signatures, the TOE is a Secure Cipher Creation Device which provides the following functions:

1. Encryption/Decryption with asymmetric keys using algorithms RSA 1024 bit and RSA 2048 bit.
2. Encryption/Decryption with symmetric keys using algorithms DES, AES and Triple-DES.
3. Performance of other signature processes with asymmetric keys using algorithms RSA 1024 bit and RSA 2048 bit.
4. The TOE is also capable of generating and storing keys, whether symmetric or asymmetric.
5. The TOE is also able to store different objects securely.

This ST assumes that the Cipher Creation Application (CCA) is part of the environment of the TOE.

For the encryption/decryption functionality, the TOE may use a symmetric or asymmetric key that can be imported to the TOE by a CCA or can be generated by the TOE itself. This key can only be managed or generated when the CCA is satisfactorily authenticated with the TOE. When using asymmetric keys, the public part (SVD) is used for encryption and the private part (SCD) for decryption.

There also exists functionality for protected storage of data, by which the TOE may store data encrypted with an internal key, termed master key, which is different for each TOE. The master key is always stored encrypted in each card and is never displayed to the outside world. In order to store protected data, a previous authentication through VAD is necessary.

The TOE life cycle is shown in Figure 2. Basically, it consists of a development phase and the operational phase. In the initialisation phase the basic structures of the system are built. The operational phase starts with personalisation, including loading of the structures generated during initialisation, generation of the master key and generation of the first key pair SCD/SVD. The main functionality in the usage phase is signature-creation including all supporting functionality (e.g., SCD storage and SCD use).

The life cycle ends with the blocking of the TOE and the annulment of the SSCD and SCCD.

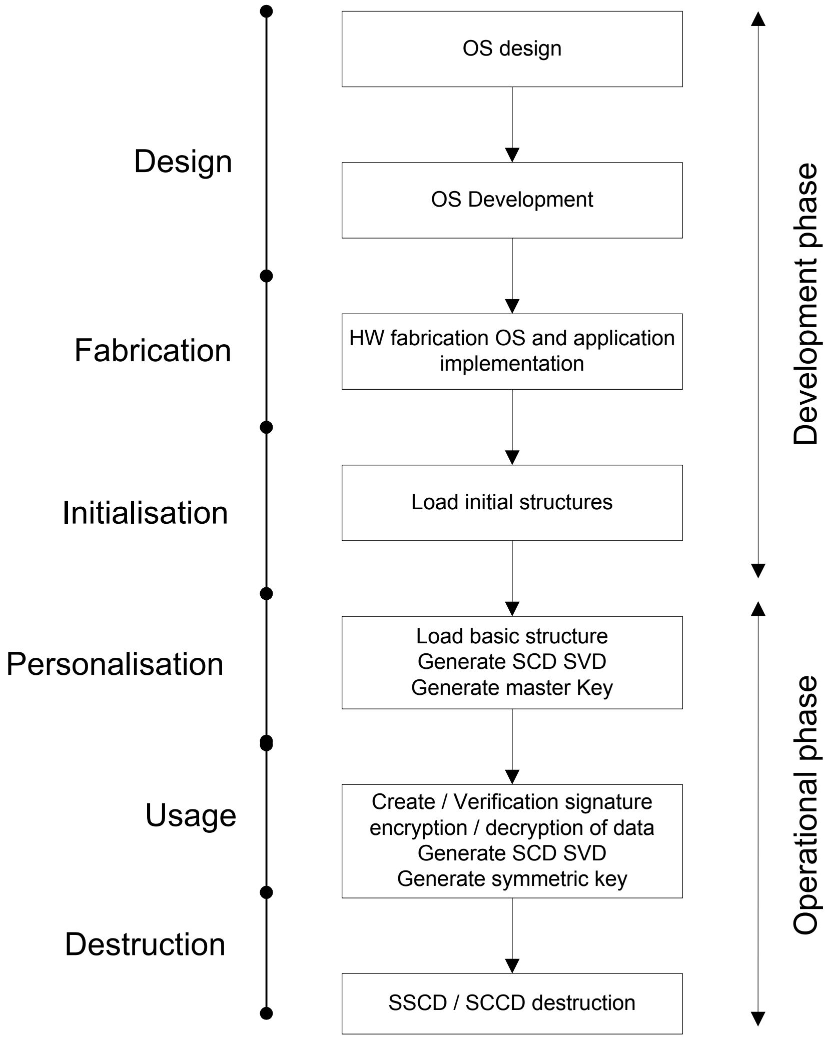

Figure 2-2: Life Cycle

3. TOE SECURITY ENVIRONMENT

This section describes security issues for the TOE and for the environment in which it shall be used, and the manner in which it will supposedly be used.

Please refer to this chapter in the Protection Profile “Secure Signature-Creation Device Type 3 Protection Profile” [6].

Different features particular to this TOE and not included in the PP are now detailed.

Assets:

New assets are added to the ones considered in the Protection Profile, aiming to extend which, the same format and numeration are used. The following variation is applied: SCD and SVD are used as defined by the PP for the Signature Application, however, when used in a different application, they are also employed as private (SCD) and public (SVD) keys for encryption/decryption.

8. **Master key**: key used for the protected storage of data (internal encryption).

9. **Symmetric key**: key used in the encryption or decryption of data with a symmetric algorithm (DES, 3DES and AES).

10. **Protected storage function**: the master key is used with Triple Data Encryption Standard (3DES) algorithm, implemented in ECB mode, for the internal encryption of data.

11. **SSCD encryption/decryption function**: a symmetric or asymmetric key is used for the encryption and decryption of data using symmetric or asymmetric algorithms respectively.

12. **Data to be Ciphered** (DTBC): set of external data to be ciphered.

Subjects:

No subject is added. The Signatory, as described in the PP, may use all of the TOE functionalities during the Usage phase.

Threat agents:

There is no need to add any threat to those specified in the Profile.

3.1. Assumptions

A.CCA *Trustworthy cipher creation application*

The Signatory uses a trustworthy CCA. The CCA generates and sends data to be enciphered/deciphered by the TOE under the appropriate conditions.

3.2. Threats to Security

T.Cipher_Divulg *Encryption key divulgation*

An attacker can obtain the encryption key outside the TOE during generation, storage and use of the encryption key.

T.CCA_Deduce *Encryption/decryption key deduction*

An attacker can obtain the encryption/decryption key (symmetric or asymmetric) from the performed ciphering.

T.CCA_Misuse *Misuse of the TOE encryption/decryption function*

An attacker misuses the TOE encryption/decryption function to create CDO which the signatory has not decided to cipher. The TOE is deliberately attacked by experts with a high attacking capacity, possessing a wide knowledge of the security principles and concepts employed by the TOE.

T.DTBC_Forgery *DTBC forgery*

An attacker modifies the DTBC sent by the CCA. Thus, the DTBC used by the TOE for encryption do not correspond to the DTBC that the Signatory pretends to encrypt.

T.Key_Cipher_Forgery *Encryption key forgery*

An attacker modifies the cipher keys exported to the CCA. As a result, the integrity of the encryption key is lost.

T.Cipher_Forgery *Cipher forgery*

An attacker modifies the ciphertext data and their integrity goes undetected by the signatory or by third persons. Ciphertexts generated by the TOE are deliberately attacked by experts with a high attacking capacity, possessing a wide knowledge of the security principles and concepts employed by the TOE.

3.3. Organisational Security Policies

P.CSD *The TOE as a secure cipher creation device*

The TOE implements the CCD used for cipher creation (with symmetric or asymmetric keys) under sole control of the Signatory.

P.Cipher *Secure encryption/decryption*

The signatory uses a cipher mechanism to encrypt/decrypt data implementing symmetric and asymmetric algorithms. The DTBC are presented to the Signatory by the CCA. Encryption/decryption is based on the use of robust cryptographic algorithms and is generated by a SCCD.

4. SECURITY OBJECTIVES

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

Please refer to this section in the Protection Profile “Secure Signature-Creation Device Type 3 Protection Profile” [6].

Different objectives, particular to this TOE and its environment, and not included in the PP are now detailed.

4.1. Security Objectives for the TOE

OT.Cipher_Secrecy *Encryption key secrecy*

The secrecy of the ciphering keys for the encryption/decryption function is reasonably guaranteed against high capacity attacks.

OT.Cipher_Auth_OE *The TOE guarantees the authenticity of encryption keys*

The TOE provides means to allow the CCA to verify the authenticity of the encryption keys exported by that TOE.

OT.Cipher_Secure *Security of the cryptographic encryption/decryption algorithms*

The TOE generates ciphertexts that cannot be decrypted without knowledge of the encryption key, due to the robustness of the employed algorithms. The cryptographic encryption/decryption algorithms resist high capacity attacks.

OT.DTBC_Integrity_OE *Verification of DTBC integrity*

The TOE must verify that the DTBC received from the CCA have not been altered in the transit between the CCA and the TOE. The TOE itself shall ensure that the DTBC is not altered by the TOE as well.

OT.Cipher_Function *Cipher generation function for the legitimate Signatory alone*

The TOE provides the cipher generation function only for the legitimate Signatory, and protects cipher keys against their use by others. The TOE shall resist attacks with high attack potential.

OT.Init_Cipher *Encryption/decryption key generation*

The TOE provides security features to ensure that the generation of cipher keys is invoked by authorised users only.

4.2. Security Objectives for the Environment

OE.CCA *Trustworthy encryption/decryption application*

Ensure that it was using trustworthy CCA the Signatory performs a correct encryption/decryption data.

The CCA

a) Generates DTBC, which the Signatory intends to encrypt/decrypt.
b) Sends the DTBC to the TOE and enables verification of the integrity of the DTBC by the TOE.

OE.Cipher_Transfer *Secure transfer of the encryption/decryption key*

Guaranteed that it was using trustworthy CCA the Signatory ensure the confidentiality encryption/decryption keys exchanged.

5. IT Security Requirements

This chapter only gives the security functional requirements for the TOE and its environment that contribute something new to what is indicated in section 5.1 ”TOE Security Functional Requirements” of the PP.

Security functional requirements components given in section 5.1 “TOE Security Functional Requirements” excepting FPT_EMSEC.1 which is explicitly stated, and those indicated in section 5.3 “Security Requirements for the Environment”, are drawn from Common Criteria part 2 [3]. Some security functional requirements present certain additional assignment, selection and refinement operations with respect to their definition in [3].

The TOE security assurance requirements statement given in section 5.2 “TOE Security Assurance Requirement” is drawn from the security assurance components from Common Criteria part 3 [4].

5.1. TOE Security Functional Requirements

5.1.1. Cryptographic support (FCS)

5.1.1.1. Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with the specified cryptographic key generation algorithm [**RSA**] and specified cryptographic key sizes [**1024 bit and 2048 bit**] that meet the following: [**ISO/IEC 9796-1, Annex A, section A.4 and A.5, and Annex C [14]**].

FCS_CKM.1.1/DES The TSF shall generate cryptographic keys in accordance with the specified cryptographic key generation algorithm [**Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES), implementing operation modes CBC, CFB8 and CFB64**] and specified cryptographic key sizes [**64 or 128 bit**] that meet the following: [**FIPS PUB 46-3 with Keying Option 2 [10]**].

FCS_CKM.1.1/AES The TSF shall generate cryptographic keys in accordance with the specified cryptographic key generation algorithm [**Advanced Encryption Standard (AES) implementing operation modes CBC, CFB8 and CFB64**] and specified cryptographic key size [**128 bit**] that meet the following: [**FIPS PUB 197 [13]**].

5.1.1.2. Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1

The TSF shall destroy cryptographic keys [**in case of regeneration of a new SCD**] in accordance with a specified cryptographic key destruction method [**overwriting keys with a random number**] that meets the following: [**CI SLECX322P random number generation method**].

FCS_CKM.4.1/ DES_AES

The TSF shall destroy cryptographic keys [**symmetric**] in accordance with a specified cryptographic key destruction method [**overwriting keys with a random number**] that meets the following: [**CI SLECX322P random number generation method**].

Application notes:

The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator.
The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.
Please refer to the Security Target of CI SLECX322P [8] for further information to the random number generation method.

5.1.1.3. Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP

The TSF shall perform [**SCD / SVD correspondence verification**] in accordance with a specified cryptographic algorithm [**Rivest Shamir Adleman (RSA)**] and cryptographic key sizes [**1024 bit and 2048 bit**] that meet the following: [**Algorithms and Parameters for Secure Electronic Signatures [12]**].

FCS_COP.1.1 / SIGNING

The TSF shall perform [**digital signature generation**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**1024 bit and 2048 bit**] that meet the following: [**Algorithms and Parameters for Secure Electronic Signatures [12]**].

FCS_COP.1.1 / DES

The TSF shall perform [**DES calculation**] in accordance with a specified cryptographic algorithm [**Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES)**] and cryptographic key sizes [**64 bit (DES), 128 bit (3-DES)**] that meet the following: [**FIPS PUB 46-3 with Keying Option 2 [10]**].

FCS_COP.1.1 / AES

The TSF shall perform [**AES calculation**] in accordance with a specified cryptographic algorithm [**Advanced Encryption Standard (AES)**] and cryptographic key sizes [**128 bit**] that meet the following: [**FIPS PUB 197 [13]**.

FCS_COP.1.1 / RSA

The TSF shall perform [**RSA encryption with SVD and RSA decryption with SCD**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**1024 bit and 2048 bit**] that meet the following: [**PKCS#1 v2.1: RSA Cryptography Standard [15]**].

5.1.2. User data protection (FDP)

5.1.2.1. Subset access control (FDP_ACC.1)

FDP_ACC.1.1 / SFP de Creación de Cifrado

The TSF shall enforce the [**SFP de Creación de Cifrado**] on:

[**1. DTBC sent from the CCA.**
2. Creation of the DTBC CDO by the Signatory].

FDP_ACC.1.1/ SFP de Transferencia de Claves de Cifrado

The TSF shall enforce the [**SFP de Transferencia de Claves de Cifrado**] on [**Cryptographic Key exportation by the Signatory**].

5.1.2.2. Security attribute based access control (FDP_ACF.1)

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

User, subject or object the attribute is associated with	Attribute	Status
General attribute		
User	Role	Signatory
Cipher creation attribute group		
CCD	Operative CCD	No, yes
DTBC	Sent by an authorised CCA	No, yes

Application note:

A CCA is considered as authorised if it is able to establish a trusted channel to the Cipher Application in the card.

Cipher Creation SFP

FDP_ACF.1.1/ SFP de Creación de Cifrado

The TSF shall enforce the [**SFP de Creación de Cifrado**] to objects based on [**general attribute and cipher creation attribute group**].

FDP_ACF.1.2/ SFP de Creación de Cifrado

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[**User with the security attribute "role" set to "Signatory", with Signatory CCD whose attribute "Operative CCD" is set to "yes", is allowed to create CDO for DTBC sent by an authorised CCA**].

FDP_ACF.1.3/ SFP de Creación de Cifrado

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4/ SFP de Creación de Cifrado

The TSF shall explicitly deny access of subjects to objects based on the rule:
[**User with the security attribute "role" set to "Signatory", with Signatory CCD whose attribute "Operative CCD" is set to "yes", is not allowed to create CDO for DTBC which is not sent by an authorised CCA.**
User with the security attribute "role" set to "Signatory", with Signatory CCD whose attribute "Operative CCD" is set to "no", is not allowed to create CDO for DTBC sent by an authorised CCA].

Cryptographic Key Transfer SFP

FDP_ACF.1.1/ SFP de Transferencia de Claves de Cifrado

The TSF shall enforce the [**SFP de Transferencia de Claves de Cifrado**] to objects based on [**general attribute**].

FDP_ACF.1.2/ SFP de Transferencia de Claves de Cifrado

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[**User with the security attribute "role" set to "Signatory", with Signatory CCD whose attribute "Operative CCD" is set to "yes", is allowed to export Cryptographic Keys to an authorised CCA**].

FDP_ACF.1.3/ SFP de Transferencia de Claves de Cifrado

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4/
SFP de Transferencia
de Claves de Cifrado

The TSF shall explicitly deny access of subjects to objects based on the rule:
[**User with the security attribute "role" set to "Signatory", with Signatory CCD whose attribute "Operative CCD" is set to "yes", is not allowed to export Cryptographic Keys to an unauthorised CCA.**
User with the security attribute "role" set to "Signatory", with Signatory CCD whose attribute "Operative CCD" is set to "no", is not allowed to export Cryptographic Keys to an authorised CCA].

5.1.2.3. Export of user data without security attributes (FDP_ETC.1)

FDP_ETC.1.1/
Transferencia de
Claves de Cifrado

The TSF shall enforce the [**Transferencia de Claves de Cifrado**] when exporting user data, controlled under one or more SFP, outside the TSC.

FDP_ETC.1.2/
Transferencia de
Claves de Cifrado

The TSF shall export the user data without the user data's associated security attributes.

5.1.2.4. Import of user data without security attributes (FDP_ITC.1)

FDP_ITC.1.1/DTBC

The TSF shall enforce the [**SFP de Creación de Cifrado**] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2/DTBC

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

FDP_ITC.1.3/DTBC

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [**DTBC shall be sent by an authorised CCA**].

5.1.2.5. Residual information protection (FDP_RIP.1)

FDP_RIP.1.1/Cipher

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**de-allocation of the resource**] from the following objects: [**Cipher Keys**].

5.1.2.6. Stored data integrity monitoring and action (FDP_SDI.2)

DTBC temporarily stored by TOE has the user data attribute "integrity checked stored data":

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

FDP_SDI.2.2/DTBC — Upon detection of a data integrity error, the TSF shall
[**Prohibit the use of the altered data,**
Inform the Signatory about integrity error].

Encryption/decryption keys (symmetric or asymmetric) persistently stored by TOE have the user data attribute "integrity checked persistent stored data":

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

FDP_SDI.2.2/ Cipher — Upon detection of a data integrity error, the TSF shall:
[**Prohibit the use of the altered data,**
Inform the Signatory about integrity error].

5.1.2.7. Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ Transferencia de Claves de Cifrado — The TSF shall enforce the [**SFP de Transferencia de Claves de Cifrado**] to be able to [**transmit**] user data in a manner protected from [**modification**] and [**insertion**] errors.

FDP_UIT.1.2/ Transferencia de Claves de Cifrado — The TSF shall be able to determine on receipt of user data, whether [**modification**] and [**insertion**] has occurred.

FDP_UIT.1.1/DTBC — The TSF shall enforce the [**SFP de Creación de Cifrado**] to be able to [**receive**] the DTBC in a manner protected from [**modification**] and [**insertion**] errors.

FDP_UIT.1.2/DTBC — The TSF shall be able to determine on receipt of user data, whether [**modification**] and [**insertion**] has occurred.

5.1.3. Identification and authentication (FIA)

5.1.3.1. *Authentication failure handling (FIA_AFL.1)*

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**block RAD**].

FIA_AFL.1.1/PUK The TSF shall detect when [**three**] unsuccessful authentication attempts occur related to [**consecutive failed authentication attempts when using PUK with blocked PIN**].

FIA_AFL.1.2/PUK When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**block PUK use**].

5.1.3.2. *Timing of authentication (FIA_UAU.1)*

FIA_UAU.1.1/Cipher The TSF shall allow the following actions on behalf of the user to be performed before the user is authenticated:

[

1. **Identification of the user by means of TSF required by FIA_UID.1/Cipher.**
2. **Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/OE.**
3. **Establishing a trusted channel between the CCA and the TOE by means of TSF required by FTP_ITC.1/Importación de DTBC**].

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

5.1.3.3. *Timing of identification (FIA_UID.1)*

FIA_UID.1.1/Cipher The TSF shall allow the following actions on behalf of the user to be performed before the user is identified:

[

1. **Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/OE.**
2. **Establishing a trusted channel between the CCA and the TOE by means of TSF required by FTP_ITC.1/Importación de DTBC**].

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

5.1.4. Security management (FMT)

5.1.4.1. Management of security functions behaviour (FMT_MOF.1)

FMT_MOF1.1/ Cipher

The TSF shall restrict the ability to [**enable**] the [**encryption/decryption function**] to [**Signatory**].

5.1.4.2. Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/ Administrador

The TSF shall enforce the [**SFP de Inicialización**] to restrict the ability to [**modify** [**none**]] the security attributes [**SCD/SVD management**] to [**Administrator**].

FMT_MSA.1.1/ Cipher

The TSF shall enforce the [**SFP de Creación de Cifrado**] to restrict the ability to [**modify** [**none**]] the security attributes [**Operativo CCD**] to [**Signatory**].

5.1.4.3. Attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1/Cipher

The TSF shall enforce the [**SFP de Inicialización**] and the **[SFP de Creación de Cifrado**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Cipher

The TSF shall allow the [**Signatory**] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.4. Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1

The TSF shall restrict the ability to [**modify** [**none**]] the [**RAD**] to [**Signatory**].

FMT_MTD.1.1/ Cipher

The TSF shall restrict the ability to [**modify** [**none**]] the [**Encryption/Decryption Key**] to [**Signatory**].

5.1.4.5. Management function specification (FMT_SMF.1)

FMT_SMF.1.1

The TSF shall be able to perform the following security management functions: [**establishment of initial RAD and security attribute management**].

5.1.5. Protection of the TSF (FPT)

5.1.5.1. Abstract machine testing (FPT_AMT.1)

FPT_AMT.1.1 The TSF shall run a suite of tests [**during initial start-up**] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.5.2. TOE emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit [**electromagnetic radiation**] other than [**unintelligible emissions**] enabling access to [**RAD**], [**SCD**] and [**Cryptographic Keys**].

FPT_EMSEC.1.2 The TSF shall ensure [**S.OFFCARD attack**] is unable to use the following interfaces [**I/O, Vcc**] to gain access to [**RAD**], [**SCD**] and [**Cryptographic Keys**].

Application notes:

The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.

Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

5.1.5.3. Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**noise on the I/O line and voltage fall**].

5.1.5.4. Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist [**physical manipulation and physical testing**] to the [**shield, clock, voltage and random number generator**] by responding automatically such that the TSP is not violated.

Application note:

Please refer to the Security Target of CI SLECX322P [8].

5.1.5.5. TSF testing (FPT_TST.1)

FPT_TST.1.1

The TSF shall run a suite of self tests [**during initial start-up, at the conditions**] [**execution of the first command**] to demonstrate the correct operation of the TSF.

5.1.6. Trusted path/channels (FTP)

5.1.6.1. Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.2/
Transferencia de SVD

The TSF shall permit [**the remote trusted IT product (Application)**] to initiate communication via the trusted channel.

FTP_ITC.1.1/
Transferencia de
Claves de Cifrado

The TSF shall provide a communication channel between itself and a remote trusted IT product [**CCA**] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/
Transferencia de
Claves de Cifrado

The TSF shall permit [**the remote trusted IT product (Application)**] to initiate communication via the trusted channel.

FTP_ITC.1.3/
Transferencia de
Claves de Cifrado

The TSF [**or the CCA**] shall initiate communication via the trusted channel for [**cryptographic key exportation**].

FTP_ITC.1.1/
Importación de DTBC

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

FTP_ITC.1.2/
Importación de DTBC

The TSF shall permit the [**CCA**] to initiate communication via the trusted channel.

FTP_ITC.1.3/
Importación de DTBC

The TSF or the [**CCA**] shall initiate communication via the trusted channel for [**DTBC encryption**].

5.1.6.2. Trusted path (FTP_TRP.1)

FTP_TRP.1.2/OE The TSF shall permit [**the TSF or the local users**] to initiate communication via the trusted path.

FTP_TRP.1.3/OE The TSF shall require the use of the trusted path for [**initial user authentication**] [**none**].

5.2. TOE Security Assurance Requirements

As the set of security assurance requirements are already defined in the Protection Profile [6], no addition will be made to this section.

As was indicated in section 1.3 CC Compliance, the assurance level for this ST is EAL4 augmented with components AVA_VLA.4 and AVA_MSU.3.

5.3. Security Requirements for the Environment

5.3.1. Certification generation application (CGA)

5.3.1.1. Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1/CGA The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**qualified certificate**] that meets the following: [**Algorithms and Parameters for Secure Electronic Signatures [12]**].

5.3.1.2. Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/CGA The TSF shall perform [**import of the SVD**] in accordance with a specified cryptographic key access method [**import through a secure channel**] that meets the following: [**Triple-DES and AES**].

5.3.1.3. Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.2/ Importación de SVD The TSF shall permit [**the remote trusted IT product**] to initiate communication via the trusted channel.

5.3.2. Signature creation application (SCA)

5.3.2.1. Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ Hash de la SCA The TSF shall perform [**hashing of the DTBS**] in accordance with a specified cryptographic algorithm [**MD5, SHA-1 or SHA-256**] and cryptographic key sizes [**none**] that meet the following: [**RFC 1321 for MD5 and FIPS PUB 180-2 for SHA-1 and SHA-256**].

5.3.2.2. Trusted path (FTP_TRP.1)

FTP_TRP.1.2 /SCA The TSF shall permit [**the TSF or the local users**] to initiate communication via the trusted path.

FTP_TRP.1.3 /SCA The TSF shall require the use of the trusted path for [**initial user authentication**] [**none**].

5.3.3. Trusted encryption/decryption application (CCA)

5.3.3.1. Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ DTBC de la CCA The TSF shall enforce the [**SFP de Creación de Cifrado**] to be able to [**transmit**] user data in a manner protected from [**modification, deletion and insertion**] errors.

FDP_UIT.1.2/
DTBC de la CCA

The TSF shall be able to determine on receipt of user data, whether [**modification, deletion or insertion**] has occurred.

FDP_UIT.1.1/
Importación de Claves de Cifrado

The TSF shall enforce the [**SFP de Importación de Claves de Cifrado**] to be able to [**receive**] user data in a manner protected from [**modification and insertion**] errors.

FDP_UIT.1.2/
Importación de Claves de Cifrado

The TSF shall be able to determine on receipt of user data, whether [**modification or insertion**] has occurred.

5.3.3.2. Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/
DTBC de la CCA

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

FTP_ITC.1.2/
DTBC de la CCA

The TSF shall permit [**the TSF**] to initiate communication via the trusted channel.

FTP_ITC.1.3/
DTBC de la CCA

The TSF [**or the TOE**] shall initiate communication via the trusted channel for [**DTBC encryption/decryption through the SCCD**].

FTP_ITC.1.1/
Importación de Claves de Cifrado

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

FTP_ITC.1.2/
Importación de Claves de Cifrado

The TSF shall permit [**the remote trusted IT product**] to initiate communication via the trusted channel.

FTP_ITC.1.3/
Importación de Claves de Cifrado

The TSF [**or the TOE**] shall initiate communication via the trusted channel for [**cryptographic key importation**].

6. TOE SUMMARY SPECIFICATION

Security functions of the TOE are defined in the first section of this chapter.

The following section offers a list of the security assurance requirements related to the different generated documents necessary for level 4 (EAL 4 +) evaluation of the TOE.

6.1. Security Functions of the TOE

In this section the different security functions of the TOE are listed, and a table relating the security functional requirements to the security functions is presented. In this way, table 1. “Functions to functional requirements mapping” displays all of the functional requirements for the TOE: those added in this ST as well as those existent in the PP.

In sections to come, specifically 8.4.1.1, 8.4.2.1, 8.4.3.1, 8.4.4.1, 8.4.5.1, 8.4.6.1 and 8.4.7.1, a Strength Statement is performed for the different functions. At this point, it is determined that security functions SF3 “Firmar” and SF4 “Cifrar” are not affected by probabilistic or permutation effects.

SF1: Inicialización y Personalización

This security function comprises mechanisms to establish the initial security attributes, initial RAD values, application creation, generation of public/private key pair (SVD/SCD) and configuration parameters for files and objects to be created on the TOE.

The generation of these values is performed through commands involved in structure initialisation and creation processes.

The Administrator is responsible of loading the initial structures and of the creation of applications.

The generation of public/private keys can be performed either by the Administrator or the Signatory.

The Administrator alone can perform the Personalisation procedure according to the Manual del Administrador [11], where the process and requirements to be fulfilled are described for a correct operation of the TOE.

SF2: Securización

This security function provides all of the secrecy procedures supported by the TOE concerning communication with the outside world.

The access conditions required to establish a trusted channel between the TOE and the Application are generated.

SF2 provides functionality to ensure protection through authentication, integrity and confidentiality of data exchange in an external communication.

Authenticity of the channel is ensured due to the establishment of a session key derived from the authentication element unique for each application of the TOE, integrity is ensured by adding a MAC and confidentiality is reached by encrypting exchanged data.

SF3: Firmar

This security function provides all of the signature procedures supported by the TOE.

The main objective is to serve as a basis to any cryptographic operations for which it is required that the keys shall never leave the TOE.

Included in SF3 are the signature process using the private key (SCD) and the verification process using the public key (SVD).

SF4: Cifrar

This security function provides all the encryption/decryption procedures supported by the TOE.

The main objective is to serve as a basis to data encryption/decryption operations.

Cryptographic algorithms DES and AES are supported in their different operation modes for 64 and 128 bit key lengths. Different encryption/decryption schemes based on RSA with 1024 and 2048 bit key lengths may be used.

Mechanisms for symmetric key generation and security attribute establishment are included in SF4.

SF5: Autenticación

This security function provides all of the authentication procedures supported by the TOE.

The Administrator or the Signatory may be authenticated and identified by presenting a PIN (VAD).

This SF protects confidentiality of the Administrator or Signatory PIN through the PIN's hash stored in the TOE (RAD). In the case of 3 consecutive failed authentication attempts this PIN will be blocked. Each PIN has an associated PUK that will allow the PIN to be unblocked. After three failed attempts, the PUK will also become blocked.

The PIN and PUK values may be changed.

SF6: Protección del TSF

This security function provides all of the protection procedures supported by the TOE.

SF6 allows checking the integrity and reliability of the TSF executable code during initial start-up.

This SF allows TSF confidentiality by storing objects in the TOE encrypted with a master key. It avoids attacks against the SCD and other objects when the attack is based on externally observable physical phenomena of the TOE.

Protection against supply failures, failure in the IO line, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. is also granted.

SF7: Gestión de Objetos

This security function provides all of the object management procedures supported by the TOE.

This SF allows importing, exporting or destroying objects in the TOE, whether encrypted or not. These objects can be SCD, SVD, Digital Certificates, Symmetric Keys and Data Objects.

The following table maps the correspondence between the described security functions and the security functional requirements of the TOE.:

Table 1: Functions to functional requirements mapping

CORRESPONDENCE BETWEEN FUNCTIONS AND REQUIREMENTS	SF1	SF2	SF3	SF4	SF5	SF6	SF7
FCS_CKM.1.1	X						
FCS_CKM.1.1/DES				X			
FCS_CKM.1.1/AES				X			
FCS_CKM.4.1							X
FCS_CKM.4.1/DES_AES							X
FCS_COP.1.1/CORRESP			X				
FCS_COP.1.1/SIGNING			X				
FCS_COP.1.1/DES				X			
FCS_COP.1.1/AES				X			
FCS_COP.1.1/RSA				X			
FDP_ACC.1.1/SFP de Transferencia de SVD							X
FDP_ACC.1.1/SFP de Transferencia de Claves de Cifrado							X
FDP_ACC.1.1/SFP de Inicialización	X						
FDP_ACC.1.1/SFP de Personalización	X						
FDP_ACC.1.1/SFP de Creación de Firma			X				
FDP_ACC.1.1/SFP de Creación de Cifrado				X			
FDP_ACF.1.1/SFP de Inicialización	X						
FDP_ACF.1.2/SFP de Inicialización	X						
FDP_ACF.1.3/SFP de Inicialización	X						
FDP_ACF.1.4/SFP de Inicialización	X						
FDP_ACF.1.1/SFP de Transferencia de SVD							X
FDP_ACF.1.2/SFP de Transferencia de SVD							X
FDP_ACF.1.3/SFP de Transferencia de SVD							X
FDP_ACF.1.4/SFP de Transferencia de SVD							X
FDP_ACF.1.1/SFP de Transferencia de Claves de Cifrado							X
FDP_ACF.1.2/SFP de Transferencia de Claves de Cifrado							X
FDP_ACF.1.3/SFP de Transferencia de Claves de Cifrado							X
FDP_ACF.1.4/SFP de Transferencia de Claves de Cifrado							X
FDP_ACF.1.1/SFP de Personalización	X						
FDP_ACF.1.2/SFP de Personalización	X						
FDP_ACF.1.3/SFP de Personalización	X						
FDP_ACF.1.4/SFP de Personalización	X						
FDP_ACF.1.1/SFP de Creación de firma			X				
FDP_ACF.1.2/SFP de Creación de firma			X				
FDP_ACF.1.3/SFP de Creación de firma			X				
FDP_ACF.1.4/SFP de Creación de firma			X				
FDP_ACF.1.1/SFP de Creación de Cifrado				X			

CORRESPONDENCE BETWEEN FUNCTIONS AND REQUIREMENTS	SF1	SF2	SF3	SF4	SF5	SF6	SF7
FDP_ACF.1.2/SFP de Creación de Cifrado				X			
FDP_ACF.1.3/SFP de Creación de Cifrado				X			
FDP_ACF.1.4/SFP de Creación de Cifrado				X			
FDP_ETC.1.1/Transferencia de SVD							X
FDP_ETC.1.2/Transferencia de SVD							X
FDP_ETC.1.1/ Transferencia de Claves de Cifrado							X
FDP_ETC.1.2/ Transferencia de Claves de Cifrado							X
FDP_ITC.1.1/DTBC							X
FDP_ITC.1.2/DTBC							X
FDP_ITC.1.3/DTBC							X
FDP_ITC.1.1/DTBS							X
FDP_ITC.1.2/DTBS							X
FDP_ITC.1.3/DTBS							X
FDP_RIP.1.1							X
FDP_RIP.1.1/Cipher							X
FDP_SDI.2.1/Persistente						X	
FDP_SDI.2.2/Persistente						X	
FDP_SDI.2.1/Cipher						X	
FDP_SDI.2.2/Cipher						X	
FDP_SDI.2.1/DTBC						X	
FDP_SDI.2.2/DTBC						X	
FDP_SDI.2.1/DTBS						X	
FDP_SDI.2.2/DTBS						X	
FDP_UIT.1.1/Transferencia de SVD		X					
FDP_UIT.1.2/Transferencia de SVD		X					
FDP_UIT.1.1/ Transferencia de Claves de Cifrado		X					
FDP_UIT.1.2/ Transferencia de Claves de Cifrado		X					
FDP_UIT.1.1/DTBS del OE		X					
FDP_UIT.1.2/DTBS del OE		X					
FDP_UIT.1.1/DTBC		X					
FDP_UIT.1.2/DTBC		X					
FIA_AFL.1.1					X		
FIA_AFL.1.2					X		
FIA_AFL.1.1/PUK					X		
FIA_AFL.1.2/PUK					X		
FIA_ATD.1.1					X		
FIA_UAU.1.1		X			X		
FIA_UAU.1.2					X		
FIA_UAU.1.1/Cipher		X			X		
FIA_UAU.1.2/Cipher					X		
FIA_UID.1.1		X					
FIA_UID.1.2		X					

CORRESPONDENCE BETWEEN FUNCTIONS AND REQUIREMENTS	SF1	SF2	SF3	SF4	SF5	SF6	SF7
FIA_UID.1.1/Cipher		X					
FIA_UID.1.2/Cipher		X					
FMT_MOF.1.1					X		
FMT_MOF.1.1/Cipher					X		
FMT_MSA.1.1/Administrador					X		
FMT_MSA.1.1/Signatario					X		
FMT_MSA.1.1/Cipher					X		
FMT_MSA.2.1	X						
FMT_MSA.3.1	X						X
FMT_MSA.3.2	X						
FMT_MSA.3.1/Cipher	X						X
FMT_MSA.3.2/Cipher							X
FMT_MTD.1.1					X		
FMT_MTD.1.1/Cipher					X		
FMT_SMR.1.1					X		
FMT_SMR.1.2					X		
FMT_SMF.1.1	X						
FPT_AMT.1.1						X	
FPT_EMSEC.1.1						X	
FPT_EMSEC.1.2						X	
FPT_FLS.1.1						X	
FPT_PHP.1.1						X	
FPT_PHP.1.2						X	
FPT_PHP.3.1						X	
FPT_TST.1.1						X	
FPT_TST.1.2						X	
FPT_TST.1.3						X	
FTP_ITC.1.1/Transferencia de SVD		X					
FTP_ITC.1.2/Transferencia de SVD		X					
FTP_ITC.1.3/Transferencia de SVD		X					
FTP_ITC.1.1/ Transferencia de Claves de Cifrado		X					
FTP_ITC.1.2/ Transferencia de Claves de Cifrado		X					
FTP_ITC.1.3/ Transferencia de Claves de Cifrado		X					
FTP_ITC.1.1/Importación de DTBS		X					
FTP_ITC.1.2/ Importación de DTBS		X					
FTP_ITC.1.3/ Importación de DTBS		X					
FTP_ITC.1.1/Importación de DTBC		X					
FTP_ITC.1.2/ Importación de DTBC		X					
FTP_ITC.1.3/ Importación de DTBC		X					
FTP_TRP.1.1/OE		X					
FTP_TRP.1.2/OE		X					
FTP_TRP.1.3/OE		X					

6.2. Assurance Measures

This section defines the list of required documents that satisfy the security assurance requirements for the TOE.

Assurance class	Assurance components	Document
ACM class	ACM_AUT.1	Gestión de la configuración
	ACM_CAP.4	
	ACM_SCP.2	
ADO class	ADO_DEL.2	Distribución del Producto
	ADO_IGS.1	Manual de Administrador
ADV class	ADV_FSP.2	Especificación Funcional
	ADV_HLD.2	Diseño de Alto Nivel
	ADV_IMP.1	
	ADV_LLD.1	Diseño de Bajo Nivel
	ADV_RCR.1	Especificación Funcional Diseño de Alto Nivel Diseño de Bajo Nivel
	ADV_SPM.1	Declaración de Seguridad Modelo de Política de Seguridad
AGD class	AGD_ADM.1	Manual de Administrador
	AGD_USR.1	Manual de Usuario
ALC class	ALC_DVS.1	Entorno de desarrollo
	ALC_LCD.1	Ciclo de vida
	ALC_TAT.1	Manual de Herramientas
ATE class	ATE_COV.2	Manual de Pruebas
	ATE_DPT.1	
	ATE_FUN.1	
	ATE_IND.2	
AVA class	AVA_MSU.3	Declaración de Seguridad Análisis de vulnerabilidades
	AVA_SOF.1	
	AVA_VLA.4	

7. PP ASSERTIONS

7.1. Reference to PP

This Security Target complies with the Protection Profile "Secure Signature-Creation Device Type 3 Protection Profile, version 1.05" [6].

7.2. PP adaptation

Some adaptation exists due to the instantiation of operations with some of the requirements.

7.3. PP aggregates

The added security objectives and functional requirements are:

OT.Cipher_Secrecy
OT.Cipher_Auth_OE
OT.Cipher_Secure
OT.DTBC_Integrity_OE
OT.Cipher_Function
OT.Init_Cipher
OE.CCA
OE.Cipher_Transfer
FCS_CKM.1.1/DES
FCS_CKM.1.1/AES
FCS_CKM.4.1/DES_AES
FCS_COP.1.1/DES
FCS_COP.1.1/AES
FCS_COP.1.1/RSA
FDP_ACC.1.1/SFP de Creación de Cifrado
FDP_ACC.1.1/SFP de Transferencia de Claves de Cifrado
FDP_ACF.1.1/SFP de Creación de Cifrado
FDP_ACF.1.2/SFP de Creación de Cifrado
FDP_ACF.1.3/SFP de Creación de Cifrado
FDP_ACF.1.4/SFP de Creación de Cifrado
FDP_ACF.1.1/SFP de Transferencia de Claves de Cifrado
FDP_ACF.1.2/SFP de Transferencia de Claves de Cifrado
FDP_ACF.1.3/SFP de Transferencia de Claves de Cifrado
FDP_ACF.1.4/SFP de Transferencia de Claves de Cifrado
FDP_ETC.1.1/Transferencia de Claves de Cifrado
FDP_ETC.1.2/Transferencia de Claves de Cifrado
FDP_ITC.1.1/DTBC
FDP_ITC.1.2/DTBC
FDP_ITC.1.3/DTBC
FDP_RIP.1.1/Cipher
FDP_SDI.2.1/DTBC
FDP_SDI.2.2/DTBC
FDP_SDI.2.1/Cipher
FDP_SDI.2.2/Cipher

FDP_UIT.1.1/Transferencia de Claves de Cifrado
FDP_UIT.1.2/Transferencia de Claves de Cifrado
FDP_UIT.1.1/DTBC
FDP_UIT.1.2/DTBC
FIA_AFL.1.1/PUK
FIA_AFL.1.2/PUK
FIA_UAU.1.1/Cipher
FIA_UAU.1.2/Cipher
FIA_UID.1.1/Cipher
FIA_UID.1.2/Cipher
FMT_MOF1.1/Cipher
FMT_MSA.1.1/Cipher
FMT_MSA.3.1/Cipher
FMT_MSA.3.2/Cipher
FMT_MTD.1.1/Cipher
FMT_SMF.1.1
FTP_ITC.1.1/Transferencia de Claves de Cifrado
FTP_ITC.1.2/Transferencia de Claves de Cifrado
FTP_ITC.1.3/Transferencia de Claves de Cifrado
FTP_ITC.1.1/Importación de DTBC
FTP_ITC.1.2/Importación de DTBC
FTP_ITC.1.3/Importación de DTBC

FDP_UIT.1.1/DTBC de la CCA
FDP_UIT.1.2/DTBC de la CCA
FDP_UIT.1.1/Importación de Claves de Cifrado
FDP_UIT.1.2/Importación de Claves de Cifrado
FTP_ITC.1.1/Importación de Claves de Cifrado
FTP_ITC.1.2/Importación de Claves de Cifrado
FTP_ITC.1.3/Importación de Claves de Cifrado
FTP_ITC.1.1/DTBC de la CCA
FTP_ITC.1.2/DTBC de la CCA
FTP_ITC.1.3/DTBC de la CCA

8. RATIONALE

8.1. Introduction

Please refer to this section in the Protection Profile “Secure Signature-Creation Device Type 3 Protection Profile” [6].

The rationale not included in the PP and part of this TOE is now detailed.

8.2. Security objectives rationale

8.2.1. Security objectives coverage

Table 2: Security environment to security objectives mapping

THREATS ASSUMPTIONS POLICIES SECURITY OBJECTIVES	OT.Cipher_Secrecy	OT.Cipher_Auth_OE	OT.Cipher_Secure	OT.DTBC_Integrity_OE	OT.Cipher_Function	OT.Init_Cipher	OT.EMSEC_Design	OT.Lifecycle_Security	OT.Tamper_ID	OT.Tamper_Resistance	OE.CCA	OE.Cipher_Transfer	OE.HI_VAD
T.Hack_Phys	X						X		X	X			
T.Cipher_Divulg	X											X	
T.CCA_Deduce			X										
T.CCA_Misuse				X	X						X		X
T.DTBC_Forgery				X							X		
T.Key_Cipher_Forgery		X											
T.Cipher_Forgery	X	X	X				X	X	X	X	X	X	
A.CCA											X		
P.CSD					X	X							
P.Cipher			X		X								

8.2.2. Policies and security objectives sufficiency

P.CSD (The TOE as a secure cipher creation device) establishes the TOE as a data encryption/decryption Secure Device for the Signatory. This is addressed by OT.Cipher_Function and OT.Init_Cipher, ensuring that the encryption/decryption keys are under sole control of the Signatory.

P.Cipher (Secure encryption) establishes that the TOE and the CCA may be employed for data encryption using robust encryption algorithms. This is ensured by OT.Cipher_Secure. OT.Cipher_Function manages the use of these algorithms by the Signatory alone.

8.2.3. Threats and security objective sufficiency

T.Hack_Phys (Exploitation of physical vulnerabilities) deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.Cipher_Secrecy preserves the secrecy of encryption keys. Physical attacks through the TOE interfaces or observation of TOE emanations are countered by OT.EMSEC_Design. OT.Tamper_ID and OT.Tamper_Resistance counter this threat by detecting and resisting tamper attacks.

T.Cipher_Divulg (Storing,copying, and releasing of the signature-creation data) addresses the possibility of an encryption key being obtained outside the TOE. This threat is countered by OT.Cipher_Secrecy which assures the secrecy of the key during usage and storage in the TOE. The OE.Cipher_Transfer ensures this confidentiality during exchange of these keys with the CCA.

T.CCA_Deduce (Deduction of encryption/decryption key) deals with attacks on the encryption/decryption key based on public data produced by the TOE. This threat is countered by security objective OT.Cipher_Secure, which avoids key deduction through the robustness of the algorithms.

T.CCA_Misuse (Misuse of the encryption/decryption function of the TOE) addresses the misuse threat on the encryption/decryption function of the TOE so that others, different from the Signatory, may create encrypted data which the Signatory has not decided to encrypt/decrypt. OT.Cipher_Function ensures that the legitimate Signatory alone can access the encryption/decryption function. OT.DTBC_Integrity_OE together with OE.CCA counter possible misuse of the encryption function by manipulation of the channel between the CCA and the TOE. On the other hand, OE.HI_VAD provides VAD confidentiality and integrity as required by the authentication method used.

T.DTBC_Forgery (Forgery of the DTBC) addresses the threat arising from modification of the DTBC sent to the TOE for encryption, which are consequently different from the DTBC which the Signatory intends to encrypt. The TOE counters this threat through OT.DTBC_Integrity_OE by checking DTBC integrity. The IT environment of the TOE counters the threat T.DTBC_Forgery through OE.CCA.

T.Key_Cipher_Forgery (Forgery of the encryption keys) deals with the forgery of encryption keys exported by the TOE to the CCA for the creation of ciphertexts. This threat is covered by security objective OT.Cipher_Auth_OE, ensuring the authenticity of the exported keys.

T.Cipher_Forgery (Ciphertext forgery) deals with non-detection of forged ciphertexts. OT.Cipher_Secure ensures the robustness to attacks of ciphertexts. OE.CCA provides the necessary means for the CCA to send DTBC correctly to the TOE. OT.Cipher_Auth_OE ensures encryption key integrity and authenticity.

OT.Cipher_Secure, OT.Cipher_Secrecy, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance and OT.Lifecycle_Security ensure encryption key confidentiality and thus prevent forgery of ciphertexts.

8.2.4. Assumptions and security objective sufficiency

A.CCA (Trusted encryption/decryption creation application) establishes the reliability of the CCA for generating an encryption/decryption. This is addressed by OE.CCA, which ensures that if the CCA is trustworthy, then the Signatory is allowed to encrypt/decrypt data.

8.3. Security requirements rationale

8.3.1. Security requirements coverage

The following tables map the correspondence between security objectives and requirements added to the PP:

Table 3: Added functional requirement to TOE security objective mapping

TOE SECURITY FUNCTIONAL REQUIREMENTS / TOE SECURITY OBJECTIVES	OT.Cipher_Secrecy	OT.Cipher_Auth_OE	OT.Cipher_Secure	OT.DTBC_Integrity_OE	OT.Cipher_Funciton	OT.Init_Cipher
FCS_CKM.1	X					
FCS_CKM.1/DES	X					
FCS_CKM.1/AES	X					
FCS_CKM.4	X					
FCS_CKM.4/DES_AES	X					
FCS_COP.1/DES			X			
FCS_COP.1/AES			X			
FCS_COP.1/RSA			X			
FDP_ACC.1/SFP de Creación de Cifrado				X	X	
FDP_ACC.1/ SFP de Transferencia de Claves de Cifrado		X				
FDP_ACF.1/SFP de Creación de Cifrado				X	X	
FDP_ACF.1/ SFP de Transferencia de Claves de Cifrado		X				
FDP_ETC.1/Transferencia de Claves de Cifrado		X				
FDP_ITC.1/DTBC				X		
FDP_RIP.1/Cipher	X				X	
FDP_SDI.2/Persistente			X			
FDP_SDI.2/DTBC				X		
FDP_SDI.2/Cipher	X		X		X	
FDP_UIT.1/Transferencia de Claves de Cifrado		X				
FDP_UIT.1/DTBC				X		
FIAL_AFL.1					X	X

FIA_AFL.1/PUK					X	X
FIA_ATD.1					X	X
FIA_UAU.1/Cipher					X	X
FIA_UID.1/Cipher					X	X
FMT_MOF.1/Cipher	X				X	
FMT_MSA.1/Administrador						X
FMT_MSA.1/Cipher	X				X	X
FMT_MSA.2					X	
FMT_MSA.3						X
FMT_MSA.3/Cipher	X				X	X
FMT_MTD.1/Cipher	X				X	
FMT_SMR.1	X				X	
FMT_SMF.1	X				X	X
FPT_AMT.1	X		X			
FPT_FLS.1	X					
FPT_TST.1			X			
FTP_ITC.1/Transferencia de Claves de Cifrado		X				
FTP_ITC.1/Importación de DTBC				X		
FTP_TRP.1/OE					X	
SECURITY ASSURANCE REQUIREMENTS						
ADV_IMP.1	X					
AVA_SOF HIGH	X				X	
AVA_VLA.4	X		X		X	
AVA_MSU.3					X	

Table 4: Added functional requirements for the IT environment to security objectives for the environment mapping

SECURITY REQUIREMENTS FOR THE ENVIRONMENT / SECURITY OBJECTIVES FOR THE ENVIRONMENT	OE.CCA	OE.Cipher_Transfer
FDP_UIT.1/DTBC de la CCA	X	
FTP_ITC.1/DTBC de la CCA	X	
FDP_UIT.1/ Importación de Claves de Cifrado		X
FTP_ITC.1/ Importación de Claves de Cifrado		X

8.3.2. TOE security requirements sufficiency

OT.Cipher_Secrecy (Secrecy of the encryption/decryption keys)

Security functions specified by FCS_CKM.1, FCS_CKM.1/DES and FCS_CKM.1/AES ensure that the generation of encryption/decryption keys satisfies the standards for the specified algorithms.

Security functions specified by FCS_CKM.4, FCS_CKM.4/DES_AES and FDP_RIP.1/Cipher ensure that residual information on encryption/decryption keys is destroyed in case they are no longer used, leaving no residual information.

The encryption key storage integrity established by FDP_SDI.2/Cipher ensures the security of the keys regarding losses of information.

Authentication and access management functions specified by FMT_MTD.1/Cipher, FMT_MSA.1./Cipher, FMT_MSA.3/Cipher and FMT_MOF.1/Cipher ensure that the Signatory alone can use the encryption/decryption functions.

FMT_SMR.1 ensures that the Signatory alone can use the encryption keys, thus preventing an attacker from obtaining any information about them.

According to FMT_SMF.1.1, the necessary means are established to protect access to encryption keys.

FPT_AMT.1 and FPT_FLS.1 check the operating conditions of the TOE and ensure a secure state when integrity is violated, thus ensuring that the specified security functions are operative.

The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation, AVA_SOF HIGH by requesting strength of function high for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.Cipher_Auth_OE (The TOE ensures authenticity of encryption keys)

FTP_ITC.1/Transferencia de Claves de Cifrado ensures the integrity and confidentiality of keys transferred via a secure channel, and FDP_UIT.1/Transferencia de Claves de Cifrado ensures the integrity and authenticity if the encryption keys, including the asymmetric key SVD.

This objective is fulfilled by requirements FDP_ACC.1/SFP de Transferencia de Claves de Cifrado, FDP_ACF.1/SFP de Transferencia de Claves de Cifrado and FDP_ETC.1/Transferencia de Claves de Cifrado on performing authentication during encryption key exchange between the TOE and the CCA.

OT.Cipher_Secure (Security of cryptographic encryption algorithms)

Security functions specified by FCS_COP.1/DES, FCS_COP.1/AES and FCS_COP.1/RSA calculate encryption/decryption according to the standards for the specified algorithms, thus ensuring their robustness.

FPT_AMT.1 and FPT_TST.1 ensure the correct performance of security functions. FDP_SDI.2/Persistente and FDP_SDI.2/Cipher ensure the integrity of encryption keys.

AVA_VLA.4, requires that the TOE will resist high potential attacks, assuring the efficiency of the security functions.

OT.DTBC_Integrity_OE (DTBC integrity checking)

Covers DTBC integrity checking as well as non-alteration of DTBC by the TOE. This is provided by FDP_ITC.1/DTBC integrity checking mechanisms for the trusted channel. Integrity functions specified by FDP_SDI.2/DTBC check that the DTBC has not been altered by the TOE. FDP_ACC.1/SFP de Creación de Cifrado and FDP_ACF.1/SFP de Creación de Cifrado access control requirements prevent unauthorised parties from altering the DTBC.

FTP_ITC.1/Importación de DTBC and FDP_UIT.1/DTBC ensure a secure communications channel with integrity check mechanisms.

OT.Cipher_Function (Cipher generation function for the legitimate Signatory alone)

FIA_UAU.1/Cipher and FIA_UID.1/Cipher ensure that the cipher generation function is not invoked before the user is identified and authenticated.

Security functions established by FDP_ACC.1/SFP de Creación de Cifrado, FDP_ACF.1/SFP de Creación de Cifrado, FMT_MTD.1/Cipher and FMT_SMR.1 ensure that the encryption/decryption process is restricted to the Signatory.

Security functions specified by FIA_ATD.1, FMT_MOF.1/Cipher, FMT_MSA.2 and FMT_MSA.3/Cipher ensure that access to cipher generation functions remains under the sole control of the Signatory, and FMT_MSA.1/Cipher provides that the Signatory will maintain control of the corresponding security attributes.

According to FMT_SMF.1.1, security attributes are established to protect encryption keys from being used by illegitimate users.

Security functions specified by FDP_SDI.2/Cipher and FPT_TRP.1/OE ensure the integrity of stored data during their storage.

Security functions established by FDP_RIP.1./Cipher, FIA_AFL.1 and FIA_AFL.1/PUK provide protection against different attacks, suche as extraction of residual information or brute force attacks on authentication.

The assurance measures specified by AVA_MSU.3 by requesting analysis of misuse of the TOE implementation, AVA_SOF by requesting high strength level for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.Init_Cipher (Encryption key generation)

Security functions FIA_ATD.1 define RAD as the corresponding user attributes.

FIA_UAU.1/Cipher and FIA_UID.1/Cipher ensure that the authorised functions will not be invoked before the user is identified and authenticated.

The attributes of the authorised users are provided by FMT_MSA.1/Administrador, FMT_MSA.1/Cipher, FMT_MSA.3 and FMT_MSA.3/Cipher.

According to FMT_SMF.1.1, the necessary security measures are established to guarantee that authorised users alone can generate encryption keys.

Security functions specified by FIA_AFL.1 and FIA_AFL.1/PUK provide protection through authentication mechanisms for key generation.

8.3.3. TOE environment security requirements sufficiency

OE.CCA (Trusted encryption/decryption application)

Security functions specified by CCA FDP_UIT.1/DTBC and CCA FTP_ITC.1/DTBC ensure DTBC exchange integrity for the TOE.

OE.Cipher_Transfer (Encryption key secure transfer)

Security functions specified by FTP_ITC.1/Transferencia de Claves de Cifrado ensure integrity and confidentiality for encryption key exchange between the TOE and the CCA, and FDP_UIT.1/Importación de Claves de Cifrado ensures integrity for encryption key exchange between the TOE and the CCA.

8.4. TOE Summary Specification Rationale

Table 1 in section 6.1 “Security Functions of the TOE” maps IT security functions to security functional requirements for the TOE.
Section 6.2 “Assurance Measures” defines a list in which assurance measures are mapped to security assurance requirements for the TOE.

8.4.1. SF1 rationale

SF1: Inicialización y Personalización provides rationale for the security requirements of FDP_ACC.1.1/SFP de Personalización, FDP_ACF.1./SFP de Inicialización, FDP_ACF.1/SFP de Personalización, FMT_MSA.2.1, FMT_MSA.3, FMT_MSA.3.1/Cipher and FMT_SMF.1.1 since the Administrator sets RAD as well as Administrator and Signatory roles, restricting the ability to modify assigned security attributes. In this SF, the TOE is initialised with the values and structures necessary to begin using the TOE.
This security function comprises generation of asymmetric keys, thus fulfilling requirements FCS_CKM 1.1 and FDP_ACC.1.1/SFP de Inicialización.

Operating System commands for this SF are COMANDO DE INICIALIZACIÓN, CREATE FILE, DELETE FILE, UPDATE BINARY, UPDATE RECORD, GENERATE KEY PAIR, MSE-SET and STORE DATA.

8.4.2. SF2 rationale

SF2: Securización justifies the requirements of FDP_UIT.1/Transferencia de SVD, FDP_UIT.1/Transferencia de Claves de Cifrado, FDP_UIT.1/DTBS del OE, FDP_UIT.1/DTBC, FIA_UAU.1.1, FIA_UAU.1.1/Cipher, FIA_UID.1, FIA_UID.1/Cipher, FTP_ITC.1/Transferencia de SVD, FTP_ITC.1/Transferencia de Claves de Cifrado, FTP_ITC.1/Importación de DTBS, FTP_ITC.1/Importación de DTBC and FTP_TRP.1/OE, since on establishing the trusted channel supplied by TOE, it is guaranteed that it is not possible for symmetric keys, SVD, BTBC or DTBS to have been modified, deleted, inserted, etc.

Operating System commands for this SF are OPEN SCH and INIT SCH.

8.4.3. SF3 rationale

SF3: Firmar this SF can justify security requirements of FCS_COP.1.1/CORRESP, FCS_COP.1.1/SIGNING, FDP_ACC.1.1/SFP de Creación de firma, FDP_ACF.1/SFP de Creación de firma, since keys are generated according to the standard mentioned in the functional requirements as well as to the policy for signature usage. Correspondence between SVD and SCD is guaranteed, and cryptographic operations are only allowed if the trusted channel has been satisfactorily established.

Operating System commands for this SF are MSE-SET, PSO-COMPUTE DIGITAL SIGNATURE, PSO-VERIFY DIGITAL SIGNATURE and PSO_HASH.

8.4.4. SF4 rationale

SF4: Cifrar the following requirements for FCS_CKM.1.1/DES, FCS_CKM.1.1/AES, FCS_COP.1.1/DES, FCS_COP.1.1/AES, FCS_COP.1.1/RSA, FDP_ACC.1.1/SFP de Creación de Cifrado, FDP_ACF.1/SFP de Creación de Cifrado can be justified, since this security function fulfils cipher usage policies on correct establishment of the trusted channel.

Operating System commands for this SF are MSE-SET, GENERATE SYMMETRIC KEY, PSO–ENCIPHER and PSO–DECIPHER.

8.4.5. SF5 rationale

SF5: Autenticación, provides justification of the functional requirements of FIA_AFL.1, FIA_AFL.1/PUK, FIA_ATD.1.1, FIA_UAU.1, FIA_UAU.1/Cipher, FMT_MOF.1.1, FMT_MOF.1.1/Cipher, FMT_MSA.1.1/Administrador, FMT_MSA.1.1/Signatario, FMT_MSA.1.1/Cipher, FMT_MTD.1.1, FMT_MTD.1.1/Cipher, FMT_SMR.1 as this SF deals with user authentication processes through verification of RAD stored in the TOE. This way, the ability to enable certain functions for the authenticated user is restricted.

The Operating System commands for this SF are VERIFY PIN, CHANGE PIN/PUK , UNBLOCK PIN and UNPRESENT PIN.

8.4.6. SF6 rationale

SF6: Protección del TSF, justifies the functional requirements of FDP_SDI.2/Persistente, FDP_SDI.2/DTBS, FDP_SDI.2/DTBC, FDP_SDI.2/Cipher, FPT_AMT.1.1, FPT_EMSEC.1, FPT_FLS.1.1, FPT_PHP.1, FPT_PHP.3.1, FPT_TST.1 as it provides all of the protection procedures supported by the TOE.

This SF guarantees the integrity and reliability of the TSF executable code during initial start-up, as an integrity check is made on the code during initial start-up, and should the check be unsatisfactory, the TOE is blocked after informing the Administrator or Signatory.

All persistent objects may be stored encrypted inside the TOE, preventing externally observable physical phenomena attacks.

During start-up, protection against possible supply or IO line failures is guaranteed. The Operating System design protects the TOE from simple power analysis, differential power, time, etc. attacks.

8.4.7. SF7 rationale

SF7: Gestión de Objetos, this SF justifies the following requirements: FCS_CKM.4.1, FCS_CKM.4.1/DES_AES, FDP_ACC.1.1/SFP de Transferencia de SVD, FDP_ACC.1.1/SFP de Transferencia de Claves de Cifrado, FDP_ACF.1/SFP de Transferencia de SVD, FDP_ACF.1/SFP de Transferencia de Claves de Cifrado, FDP_ETC.1/Transferencia de SVD, FDP_ETC.1/Transferencia de Claves de Cifrado, FDP_ITC.1/DTBS, FDP_ITC.1/DTBC, FDP_RIP.1.1, FDP_RIP.1.1/Cipher, FMT_MSA.3.1 and FMT_MSA.3/Cipher, as it has the possibility of importing, exporting or destroying objects of the TOE. These actions can only be performed when the access conditions to each object have been satisfied.

Importing, exporting and destroying actions are carried out by commands IMPORT, EXPORT and DESTROY of the Operating System after having established a trusted channel.

8.5. PP asseriton rationale

There is compliance with PP and with the aggregates specified in section 7.3 “PP aggregates”.

8.6. Dependency rationale

8.6.1. Justification of requirement dependencies

Dependencies of the functional requirements added to the TOE are fully satisfied. This is not so for all the dependencies of the functional requirements for the TOE environment (see section 8.6.2).

Table 5: Added functional requirement dependencies and refined functional requirements

Requirement	Dependencies
Functional Requirements	
FCS_CKM.1	FCS_COP.1/SIGNING, FCS_CKM.4, FMT_MSA.2
FCS_CKM.1/DES	FCS_COP.1/DES, FCS_CKM.4/DES_AES, FMT_MSA.2
FCS_CKM.1/AES	FCS_COP.1/AES, FCS_CKM.4/DES_AES, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2
FCS_CKM.4/DES_AES	FCS_CKM.1/DES, FCS_CKM.1/AES, FMT_MSA.2
FCS_COP.1/CORRESP	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/SIGNING	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/DES	FCS_CKM.1/DES, FCS_CKM.4/DES_AES, FMT_MSA.2
FCS_COP.1/AES	FCS_CKM.1/AES, FCS_CKM.4/DES_AES, FMT_MSA.2
FCS_COP.1/RSA	FCS_CKM.1.1, FCS_CKM.4.1, FMT_MSA.2
FDP_ACC.1/ SFP de Creación de Cifrado	FDP_ACF.1/SFP de Creación de Cifrado
FDP_ACC.1/ SFP de Transferencia de Claves de Cifrado	FDP_ACF.1/SFP de Transferencia de Claves de Cifrado
FDP_ACF.1/ SFP de Creación de Cifrado	FDP_ACC.1/SFP de Creación de Cifrado, FMT_MSA.3
FDP_ACF.1/ SFP de Transferencia de Claves de Cifrado	FDP_ACC.1/SFP de Transferencia de Claves de Cifrado, FMT_MSA.3
FDP_ETC.1/Transferencia de Claves de Cifrado	FDP_ACC.1/SFP de Transferencia de Claves de Cifrado.
FDP_ITC.1/DTBC	FMT_MSA.3, FDP_ACC.1/SFP de Creación de Cifrado
FDP_RIP.1/Cipher	None.
FDP_SDI.2/DTBC	None.
FDP_SDI.2/Cipher	None.
FDP_UIT.1/Transferencia de Claves de Cifrado	FTP_ITC.1/Transferencia de Claves de Cifrado, FDP_ACC.1/SFP de Transferencia de Claves de Cifrado.
FDP_UIT.1/DTBC	FDP_ACC.1/SFP de Creación de Cifrado, FTP_ITC.1/Importación de DTBC.
FIA_AFL.1	FIA_UAU.1

FIA_AFL.1/PUK	FIA_UAU.1
FIA_UAU.1/Cipher	FIA_UID.1/Cipher.
FIA_UID.1/Cipher	None.
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1
FMT_MOF.1/Cipher	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Administrador	FDP_ACC.1/SFP de Inicialización, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Cipher	FDP_ACC.1/SFP de Creación de Cifrado, FMT_SMR.1, FMT_SMF.1
FMT_MSA.3/Cipher	FMT_MSA.1/Cipher, FMT_MSA.1/Administrador, FMT_SMR.1, FMT_SMF.1.
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Cipher	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	None
FPT_AMT.1	None
FPT_EMSEC.1	None
FPT_FLS.1	ADV_SPM.1
FPT_PHP.3	None
FPT_TST.1	FPT_AMT.1
FTP_ITC.1/Transferencia de SVD	None
FTP_ITC.1/Transferencia de Claves de Cifrado	None
FTP_ITC.1/Importación de DTBC	None
FTP_TRP.1/OE	None
Functional Requirements for the Certificate Generation Application (CGA)	
FCS_CKM.2/CGA	Dependency not supported (see section 8.6.2 for justification)
FCS_CKM.3/CGA	Dependency not supported (see section 8.6.2 for justification)
FTP_ITC.1/Importación de SVD	None
Functional Requirements for the Signature Creation Application (SCA)	
FCS_COP.1/Hash de la SCA	Dependency not supported (see section 8.6.2 for justification)
FTP_TRP.1/SCA	None
Functional Requirements for the Cipher Creation Application (CCA)	
FDP_UIT.1/DTBC de la CCA	Dependency not supported (see section 8.6.2 for justification)
FDP_UIT.1/Importación de Claves de Cifrado	Dependency not supported (see section 8.6.2 for justification)
FTP_ITC.1/DTBC de la CCA	None
FTP_ITC.1/Importación de Claves de Cifrado	None

8.6.2. Justification of unsupported dependencies

Table 6: **Unsupported dependencies**

FCS_CKM.2/CGA	The CGA generates qualified electronic signatures including the SVD imported from the TOE. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this ST.
FCS_CKM.3/CGA	The CGA imports SVD via trusted channel implemented by FTP_ITC.1/Importación de SVD. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this ST.
FCS_COP.1/Hash de la SCA	The hash algorithm implemented by FCS_COP.1/Hash de la SCA does not require any key or security management. Therefore FDP_ITC.1, FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2 are not required for FCS_COP.1/ Hash de la SCA.
FDP_UIT.1/DTBC de la CCA	Access control policy (FDP_ACC.1.1) for the CCA is outside of the scope of this ST.
FDP_UIT.1/Importación de Claves de Cifrado	Access control policy (FDP_ACC.1.1) for the CCA is outside of the scope of this ST.

ACRONYMS

CBC	Cipher Block Chaining mode
CC	Common Criteria
CCA	Cipher Creation Application
CCD	Cipher Creation Data
CDO	Cipher Data Object
CFB	Cipher Feed Back mode
CGA	Certificate Generation Application
CSP	Cryptographic Service Provider
DPA	Differential Power Analysis
DTBS	Data To Be Signed
DTBC	Data To Be Ciphered
EAL	Evaluation Assurance Level
GC	Gestión de Configuración (CM, Configuration Management).
IH	Human Interface
IT	Information Technology
MAC	Message Authentication Code
MSE	Manage Security Environment.

NVM	Non Volatile Memory.
TOE	Target Of Evaluation
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PP	Protection Profile
PSO	Perform Security Operation.
PUK	Unblock PIN
RAD	Reference Authentication Data. Reference of the PIN code for user identification and authentication (Hash stored in card)
SCA	Signature-Creation Application
SCD	Signature-Creation Data. Private Key used in an electronic signature operation
SDO	Signed Data Object
SE	Security Environment
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
SPA	Simple Power Analysis
SSCD	Secure Signature-Creation Device
SCCD	Secure Cipher-Creation Device.

ST	Security Target
SVAD	Signatory Verification Authentication Data
SVD	Signature-Verification Data. Public Key for verification of an electronic signature
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
VAD	Verification Authentication Data User’s PIN code for signing

REFERENCES

[1] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNSIL of 13 December 1999 on a Community framework for electronic signatures.

[2] ISO/IEC 15408-1:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, 1999.

[3] ISO/IEC 15408-2:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements, 1999.

[4] ISO/IEC 15408-3:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements, 1999.

[5] Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive.

[6] Annex C of CWA 14169:2002. Protection Profile - Secure Signature-Creation Device, Type 3, version 1.05 (Secure Signature Creation Device - Protection Profile).

[7] Certification Report BSI-DSZ-CC-0223-2003 for Infineon Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a24, m1484a27 and m1484b14 from Infineon Technologies AG.

[8] Infineon Technologies AG Security and Chipcard ICs Evaluation Documentation SLECX322P with RSA2048 / m1484 Security Target. Version 1.0.5. Date 06/05/2002.

[9] Especificación Funcional, Sistema Operativo M.MAR TEMDv1.0.

[10] U.S. Department of Commerce / National Bureau of Standards Data Encryption Standard (DES), FIPS PUB 46-3, 25 October 1999.

[11] Manual del Administrador, Sistema Operativo M.MAR TEMDv1.0.

[12] Algorithms and Parameters for Secure Electronic Signatures V.1.44 Draft 04/05/2001.

[13] U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197

[14] ISO/IEC 9796-1 Information Technology - Security Techniques - Digital signature scheme giving message recovery. Part 1: Mechanisms using redundancy 1999

[15] PKCS#1 v2.1: RSA Cryptography Standard. RSA Laboratories, 14/06/2002.