IDOne™ ClassIC Card

V1.0

Public Security Target

TABLE DES MATIERES

1 ST INTRODUCTION

1.1 ST IDENTIFICATION

Title: IDOne ClassIC Card – Public Security Target

Reference:

- Microcontroller: Philips Smart MX P5CT072 VOP

This Security Target deals with the evaluation of the application software, as well as the composition with the evaluation of the Integrated Circuit (IC). It claims two SSCD Protection Profiles [SSCD2] and [SSCD3].
This security target refers to the micro-controller MX P5CT072 security target [STIC] that is compliant to BSI 0002 Protection Profile [BSI-0002].
IDOne ClassIC product is derived from CNS product. The differences between both products are:

- Increase in RSA key length: 1024 up to 2048 bits
- RSA CRT key generation algorithm.

The RSA CRT algorithm is already present on the platform not used by CNS applet but is used by IAS applet in the same platform.

So with this product we can sign using RSA key from 1024 up to 2048 with 256 bits as step with one of the two algorithms RSA CRT or RSA SFM.

1.2 ST OVERVIEW

The TOE is a signature-creation device according to Directive 1999/93/EC [1999/93/EC] of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures.
The context of this ST is the Secure Signature Creation Device following the Protection Profiles ([SSCD1], [SSCD2] and [SSCD3]) developed by CEN/ISSS. These PPs are a translation of the annex concerning the Secure Signature Creation Device of the European directive [1999/93/EC].

The main objectives of this security target are:

- To describe the Target of Evaluation (TOE). This ST focuses on the Secure Signature Creation Device, designed to be embedded in a Smart card integrated circuit.
- To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by its environment.
- To describe the security objectives of the TOE and its supporting environment.
- To specify the security requirements which includes the TOE security functional requirements and the TOE security assurance requirements.
- To specify the TOE summary specification, which includes the TOE security functions specifications and the assurance measures.
- To give a rationale to this ST.

The assurance level for this product and its documentation is EAL4 augmented with:

- ADV_IMP.2: Implementation of the TSF
- AVA_MSU.3: Analysis of insecure states,
- AVA VLA.4: Highly resistant,

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

1.3 CC CONFORMANCE

This ST is built on [SSCD2] and [SSCD3] and is conformant to these PP.

This ST is CC V2.3 conformant with Part2 extended due to additional functional components as stated in [SSCD2] and [SSCD3].

1.4 REFERENCES

[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIMB-2005-08-001, version 2.3, 2005
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-2005-08-002, version 2.3, 2005
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements CCIMB-2005-08-003, version 2.3, 2005
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology CCIMB-2005-08-004, version 2.3, 2005
[CWA]	CEN/ISSS WS/E-Sign Expert Group F - Workshop Agreement CWA14169 Secure Signature-Creation Devices "EAL 4+"
[CWA-ALGO]	CEN/ISSS WS/E-Sign Expert Group F - Algorithms and Parameters for Secure Electronic Signatures
[1999/93/EC]	Directive 1999/93/EC of the European parliament and of the council of the 13 December on a Community framework for electronic signatures
[SSCD1]	Secure Signature-Creation device Protection Profile Type 1 v1.05, EAL4+ BSI -PP-0004-2002 April 2002
[SSCD2]	Secure Signature-Creation device Protection Profile Type 2 v1.04, EAL4+ BSI -PP-0005-2002 April 2002
[SSCD3]	Secure Signature-Creation device Protection Profile Type 3 v1.05, EAL4+ BSI -PP-0006-2002 April 2002
[BSI-0002]	Smartcard IC Platform Protection Profile v 1.0 BSI-PP-0002-2001 Jul 2001
[STIC]	Security Target Lite BSI-DSZ-CC-0348. Evaluation of the Philips P5CT072V0P Secure Smart Card Controller, version 1.2, 2006.
[CNS]	CNS – Carta Nazionale dei Servici – Functional Specification –1.1.2

[JCAPI]	"Java Card 2.2.1 - Application Programming Interfaces", October 21 2003, Sun Microsystems
[JCRE]	"Java Card 2.2.1-JCRE", October 21 2003, Sun Microsystems
[JCVM]	"Java Card 2.2.1-Virtual Machine Specifications", October 21 2003, Sun Microsystems
[GP]	"Global Platform Card Specification", version 2.1.1' March, 2003, Global Platform

2 TOE DESCRIPTION

This part of the ST describes the TOE as an aid to the understanding of its security requirements and addresses the product type, the intended usage and the general features of the TOE.

2.1 PRODUCT TYPE

The Target of Evaluation (TOE) is the Secure Signature Creation Device (SSCD) defined by:
The underlying Integrated Circuit;
The Operating System embedding the Java Virtual Machine (JVM);
The SSCD Application.

The Figure below gives a description of the TOE and its boundaries.

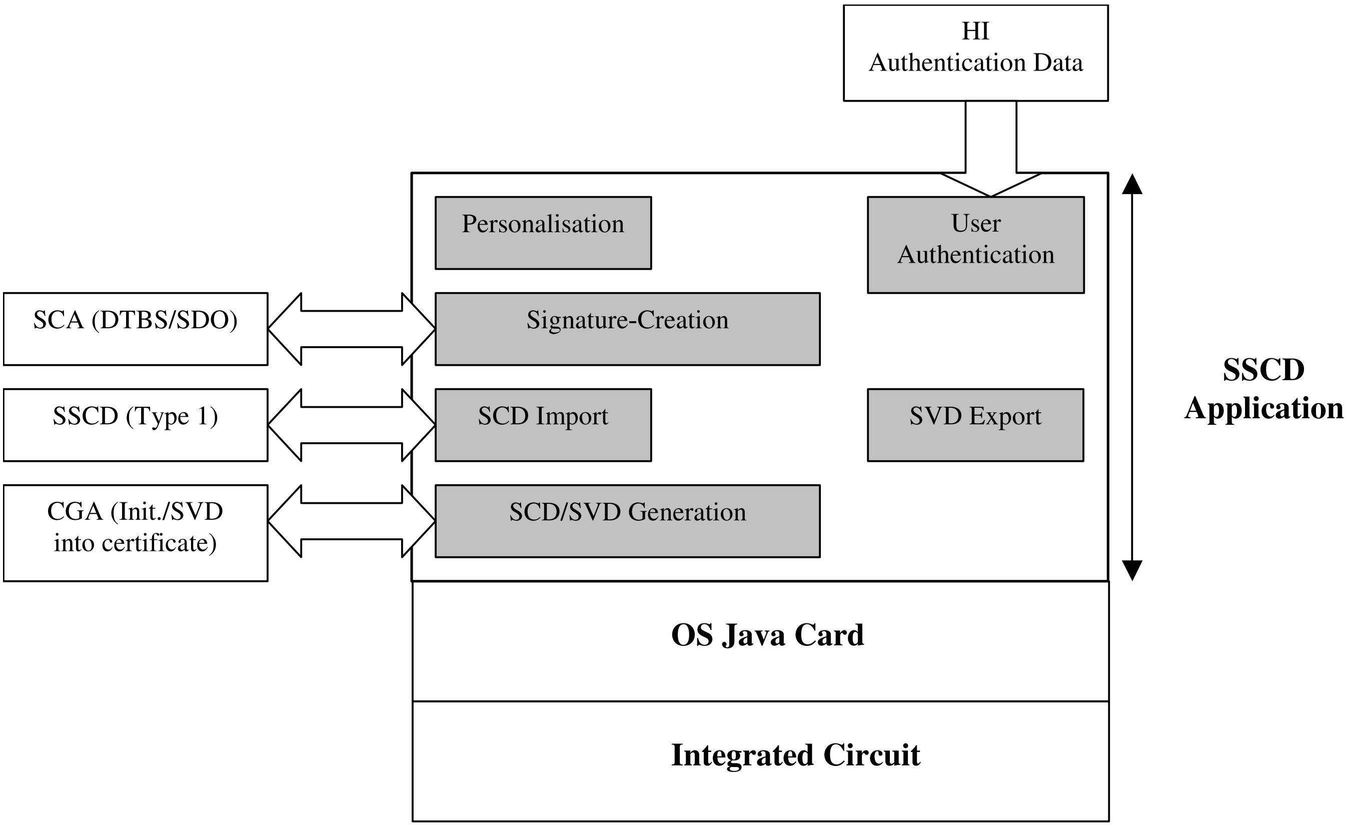

Figure 1 Secure Signature Creation Device (card) and its boundaries

2.2 TOE DESCRIPTION

2.2.1 SSCD functions

The SSCD Application provides the following functions:
Generation of SCD and SVD – The TOE ensures the secrecy of the SCD
Import of the SCD
Export of SVD
Signature Creation
Pin Authentication of the Signatory: the TOE holds the RAD that is used to verify the VAD provided by the user.
Implementation of a trusted path to a human interface device

The TOE destroys the SCD if it is no longer used for signature generation. In usage phase, the TOE allows the creation of a new SCD/SVD pair. The previous SCD must be destroyed before the creation of a new SCD/SVD pair.
The TOE implements the SSCD of type 2 and type 3, and all functions concerning the SSCD to create electronic signatures in a secure way.

2.2.2 Card description

The Card is composed of:

- An Operating System based on Java Card technology [JCRE][JCVM][JCAPI] and Global Platform technology [GP]. His main responsibilities are:

  - To provide interface between the Integrated Circuit and the applet
  - To provide to the applet, basic services to access to memories and all needed cryptographic operations
  - To ensure global management of the card (loading, installation and deletion of applets) and monitor the security of the card (data integrity and physical attacks counter-measures).

    The loading mechanism is blocked after the applet loading. Therefore no loading can be initiated after this applet loading.

- The applet is a high security product which provides the following services:

  - A highly secure and configurable framework to store sensitive and user data, based on ISO7816-4 and ISO7816-9;
  - secure messaging, based on ISO7816-4 ;
  - dynamic management of access control rules ;
  - dynamic management of confidentiality/integrity (Secure Messaging conditions) settings ;
  - onboard RSA key pair generation (up to 2048 bits), compliant with ISO7816-8 ;
  - import of Private (SCD) RSA keys
  - export of Public (SVD) RSA keys
  - Triple DES based authentication, encryption and decryption, compliant with ISO7816-4 and ISO7816-8;
  - PIN authentication;
  - RSA digital signature, compliant with ISO7816-8

2.2.3 Files and BSOs

In this applet, we consider three kinds of objects:
- Files,
- BSO (Base Security Object) and
- SEO (Security Environment Objects)

- **Files:**

The applet file system of is based on three categories of basic file components:

- The root of the file system, the Master File (MF),
- Directory files, denoted as dedicated files (DF),
- Generic data files, denoted as Elementary files (EF).

The Master File (MF) is the root of the file system and is always the initial entry point to the file system. After a reset of the card, the MF is selected.
The Dedicated Files (DFs) are similar to Folders in traditional file systems. DFs can contain Elementary Files (EFs), and/or other DFs. The MF can be considered to be a special DF that contains all the files.
The Elementary File (EF) is used for data storage. For this reason EFs are also referred to as *data files*. File access is similar to traditional file systems. To access a file (for reading, writing, or any other operation), it has to be selected.
Note that the public key SVD is stored in a file.

– **BSO:**

A Base Security Object (BSO) is a container for secret/sensitive data, including SCD and Reference Authentication Data. All BSOs are stored in folders DF.
We distinguish three kinds of BSO:

- Authentication BSO (called also TEST BSO):
  - PINs,
  - External Authentication keys; These BSO have the following type:
    - 3DES-EXT AUTH for 3DES Keys,
    - RSA KPUB EXP-EXT AUTH (exponent component) and RSA KPUB MOD-EXT AUTH (modulus component) for RSA Keys:
  - Logical BSO: used to build Boolean expression (AND/OR) of authentication data. Example: PIN1 AND (EXT AUTH2 OR PIN2)

  A PIN or an External Authentication Keys may have three different states, defined in their attribute “Status”:
    - Non Satisfied: Not verified
    - Satisfied: Verified
    - Blocked: a blocked authentication data is always Non Satisfied

- Cryptographic BSO (called also PSO BSO):
  - In this TOE, we consider only BSO corresponding to SCD; they are used for signature creation. Their type is RSA KPRI EXP-SIGN for the private exponent component and RSA KPRI MOD-SIGN for Modulus component

- Secure Messaging BSO:
  These BSO contain keys to be used for Secure Messaging. We distinguish:
  - Keys for Encryption/Decryption, of type 3DES –SM Cipher
  - Keys for Signature (MAC computation) and Verification (MAC verification), of type 3DES –SM Auth

– **SEO:**

An SEO (Security Object Environment) is a set of references to the security objects (BSO) that will be used for security operation commands. It has three components: Confidentiality (CON), Digital Signature (DS) and TEST. The DS component is used to reference the SCD to be used for digital signature.

2.2.4 Access conditions

Access Conditions are attached to a file (EF, DF or MF), or to other card objects (BSO). They tell in which status the card has to be in order to allow a specific operation on a specific object. Possible values of access conditions are:

- ALWAYS: operation always allowed
- NEVER: operation never allowed
- BSO ID: reference (ID) of a authentication BSO.

2.2.5 Secure Messaging

The Secure Messaging (SM) is used to protect the communication between the interface device (IFD) and the smart card. There are two ways to communicate data in SM format:

- SM_ENC: APDU commands with enciphered data (data confidentiality)
- SM_SIG: APDU commands with cryptographic checksum (data authentication and integrity)

It is possible to use a combination of the two (ENC followed by SIG). Indeed, it is recommended for security reasons to use SM_ENC only in conjunction with SM_SIG.

Secure Messaging are dynamically defined relatively to objects and operations. These conditions are called *Secure Messaging conditions*, and they define for

- NO SM: no secure messaging is required
- BSO ID: reference (identifier) to a BSO containing a secure messaging key.

Example: For signature creation, the corresponding key SCD has 4 Secure Messaging conditions:

- ENC_USE_IN: determine if encryption is required for incoming command
- SIG_USE_IN: determine if signature (MAC) is required for incoming command
- ENC_USE_OUT: determine if encryption is required for outgoing command
- SIG_USE_OUT: determine if signature (MAC) is required for outgoing command

2.3 SMART CARD PRODUCTS LIFE-CYCLE

The Smart card product life cycle is split up into 7 phases where the following authorities are involved:

Phase 1	Smart card software development	The smart card embedded software developer is in charge of the smart card embedded software development and the specification of IC pre-personalisation requirements.
Phase 2	IC Development	The IC designer designs the integrated circuit, develops IC firmware if applicable, provides information, software or tools to the smart card software developer, and receives the software from the developer, through trusted delivery and verification procedures. From the IC design, IC firmware and smart card embedded software, he constructs the smart card IC database, necessary for the IC photomask fabrication.
Phase 3	IC manufacturing and Testing	The IC manufacturer is responsible for producing the IC through three main steps: IC manufacturing, testing, and IC pre-personalisation.
Phase 4	IC packaging and Testing	The IC packaging manufacturer is responsible for the IC packaging_and testing.
Phase 5	Smart card product finishing process	The smart card product manufacturer is responsible for the smart card product finishing process and testing, and the smart card pre-personalisation
Phase 6	Smart card Personalisation	The Personaliser is responsible for the smart card personalisation and final tests.
Phase 7	Smart card end-usage	The smart card issuer is responsible for the smart card product delivery to the smart card end-user, and for the end of life process.

Phases 1 to 3 are included in the evaluation perimeter.

2.4 TOE INTENDED USAGE

The TOE intended usage is the Creation of Secure Signatures.

3 TOE SECURITY ENVIRONMENT

This section describes the security aspects of the environment in which the TOE is to be used. It describes the assets to be protected, the threats, the organisational security policies and the assumptions.

3.1 Subjects

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

3.2 Assets

The assets of the TOE are those defined in [SSCD2] and [SSCD3]:

1. SCD: private key used to perform an electronic signature operation. Confidentiality of the SCD must be maintained.
2. SVD: public key linked to the SCD and used to perform an electronic signature verification. Integrity of the SVD when it is exported must be maintained.
3. DTBS and DTBS-representation: set of data, or its representation which is intended to be signed. Their integrity must be maintained.
4. VAD: PIN code entered by the End User to perform a signature operation. Confidentiality and authenticity of the VAD as needed by the authentication method employed.
5. RAD: Reference Pass Phrase code used to identify and authenticate the End User. Integrity and confidentiality of RAD must be maintained. The specification references also RAD as a PIN even it is an alphanumeric code.
6. Signature-creation function of the SSCD using the SCD: The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures.
7. Electronic signature: Unforgeabilty of electronic signatures must be assured.

We detail below the representation of the Asset data in this applet:

Note on Secure Messaging conditions naming:

Conditions for Secure Messaging are named as follow:

- For outgoing commands, the condition name has the format ENC_<OPER>_OUT and SIG_<OPER>_OUT
- For incoming commands, two formats are possible for the condition name:

ENC_<OPER> and SIG_<OPER>,

Or ENC_<OPER>_IN and SIG_<OPER>_IN.

<OPER> indicates an operation: USE, CHANGE, UNBLOCK, APPEND, UPDATE, UPDATE/APPEND, READ.

Asset data	Attribute	Status
SCD SCD is stored as a BSO (Basic Security Object) of type: RSA KPRI EXP-SIGN for the private exponent component And RSA KPRI MOD-SIGN for Modulus component		
	AC_GENKEYPAIR	Access condition for SCD/SVD generation
	AC_USE	Access condition for digital signature creation. It must reference the PIN BSO corresponding to the RAD.
	ENC_USE_IN and SIG_USE_IN	Secure Messaging conditions to be satisfied by the incoming signature command
	ENC_ USE_OUT and SIG_ USE_OUT	Secure Messaging conditions to apply to send the digital signature
	AC_CHANGE	Access condition for modifying (import) a new key
	ENC_CHANGE and SIG_CHANGE	Secure Messaging conditions to be satisfied by the incoming change command
SVD SVD is stored as two records in a record file. A record for the public exponent and a record for the Modulus.		
	AC_READ	Access conditions to be satisfied for reading a SVD record
	SIG_READ_OUT and ENC_READ_OUT	Secure Messaging conditions to apply to send the SVD value
PIN (these attributes refer to all PINs including RAD) - PINs are stored as BSO of type PIN,		
	AC_USE	Access condition to be satisfied for verifying a PIN
	ENC_USE_IN and SIG_USE_IN	Secure Messaging to be satisfied by the incoming verify PIN command
	AC_CHANGE	Access condition to be satisfied for modifying a PIN value
	ENC_CHANGE and SIG_CHANGE	Secure Messaging to be satisfied by the incoming Change Reference Data command
	AC_UNBLOCK	Access condition to be satisfied for unblocking a PIN
	ENC_UNBLOCK and SIG_UNBLOCK	Secure Messaging to be satisfied by the incoming unblock PIN command

Table 1 Applet Attributes (1)

The RAD (SCD.AC_USE) is restricted to be defined as a PIN. Other access conditions (like AC_GENKEYPAIR for example) are not concerned by this restriction: they are Boolean expressions of PINs and external authentication keys.
On the other hand, to protect the Asset data during communication between the TOE and the terminal, TOE uses Secure Messaging with specific keys (of type 3DES –SM Auth and 3DES –SM Cipher). These keys are specified

as attributes (called Secure Messaging conditions) for the Asset data (example: ENC_USE_IN is an attribute of PIN and protects the VAD for confidentiality during its transmission into the card).

We complete the Asset Data by adding the External Authentication keys and the Secure Messaging Keys as Data to be managed by the TOE. We add also the Dedicated Files because the creation and update of BSO (SCD, RAD,…) are controlled by access conditions and Secure Messaging conditions associated to the Dedicated File containing the BSO.

Data	Attribute	status
DF (Dedicated File: Folder containing the BSO)		
	AC_CREATE	Access condition to create a file (to contain SVD)
	AC_APPEND	Access condition to satisfy for create a new BSO (SCD, RAD and other BSOs)
	AC_UPDATE	Access condition to satisfy for updating an existing BSO (SCD, RAD and other BSOs)
	ENC_UPDATE/APPEND and SIG_UPDATE/APPEND	Secure Messaging conditions to be satisfied by the incoming append or update command
External Authentication Keys		
	AC_USE	Access condition to be satisfied for verifying an external authentication key
	ENC_USE_IN and SIG_USE_IN	Secure Messaging to be satisfied by the incoming external authenticate command
	AC_CHANGE	Access condition to be satisfied for modifying a authentication key value
	ENC_CHANGE and SIG_CHANGE	Secure Messaging to be satisfied by the incoming external authenticate command
	AC_UNBLOCK	Access condition to be satisfied for unblocking an authentication key
	ENC_UNBLOCK and SIG_UNBLOCK	Secure Messaging to be satisfied by the incoming unblock authenticate key command
Secure Messaging Keys		
	AC_CHANGE	Access condition to be satisfied for modifying the key value
	ENC_CHANGE and SIG_CHANGE	Secure Messaging to be satisfied by the incoming CHANGE KEY DATA command
	AC_UNBLOCK	Access condition to be satisfied for unblocking a SIG secure messaging key
	ENC_UNBLOCK and SIG_UNBLOCK	Secure Messaging to be satisfied by the incoming unblock secure messaging key command

Table 2 Applet Attributes (2)

Life Cycle Definition:
The TSF data “LIFECYCLE” represents the current application state.

The application may have three different states:

- SELECTABLE: In this state, the application is ready for personalisation. The card is under the control of the Administrator.
- PESONALIZED: In this state, the card is under control of the Card Holder or Administrator.
- BLOCKED: The application is blocked.

3.3 ASSUMPTIONS

A.CGA *Trustworthy certification-generation application*
The CGA protects the authenticity of the signatory’s name and the SVD in the qualified certificate by an advanced signature of the CSP.

A.SCA *Trustworthy signature-creation application*
The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

A.SCD_Generate *Trustworthy SCD/SVD generation*
If a party other than the signatory generates the SCD/SVD-pair of a signatory, then

(a) this party will use a SSCD for SCD/SVD-generation,
(b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and
(c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory.
(d) The generation of the SCD/SVD is invoked by authorised users only
(e) The SSCD Type1 ensures the authenticity of the SVD it has created an exported

3.4 THREATS

T.Hack_Phys *Physical attacks through the TOE interfaces*
An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat addresses all the assets.

T.SCD_Divulg *Storing ,copying, and releasing of the signature-creation data*
An attacker can store, copy the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE.

T.SCD_Derive *Derive the signature-creation data*
An attacker derives the SCD from public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.

T.Sig_Forgery *Forgery of the electronic signature*
An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.Sig_Repud *Repudiation of signatures*
If an attacker can successfully threaten any of the assets, then the non-repudiation of the electronic signature is compromised. The signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.

T.SVD_Forgery *Forgery of the signature-verification data*

An attacker forges the SVD presented by the TOE. This result in loss of SVD integrity in the certificate of the signatory.

T.DTBS_Forgery *Forgery of the DTBS-representation*
An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intends to sign.

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

IC Threats: (see [STIC])

T.Leak-Inherent	Inherent Information Leakage
T.Phys-Probing	Physical Probing of the IC
T.Malfunction	Malfunction due to Environmental Stress
T.Phys-Manipulation	Physical Manipulation
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

3.5 ORGANIZATIONAL SECURITY POLICIES

P.CSP_QCert *Qualified certificate*
The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.

P.QSign *Qualified electronic signatures*
The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate and is created by a SSCD.

P.Sigy_SSCD *TOE as secure signature-creation device*
The TOE stores the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

The following policies are taken from the IC security target [STIC]:

P.Add-Components The TOE shall provide the following security functionality:
- Triple DES encryption and decryption
- Area based Memory Access Control
- Memory separation for different software parts (including IC Dedicated software and Smartcard Embedded Software)
- Special Function Register Access Control

- Protection of configuration data. The TOE prevents modification of configuration data – including configuration data for TSF – after TOE delivery. This can be used to enable or disable specific blocks on the TOE.

P.Process-TOE Protection during IC Development and Production
The IC Manufacturer must ensure that the development and production of the Smartcard Integrated Circuit (Phase 2 up to IC Delivery – phase 3) is secure so that no information is unintentionally made available for the operational phase of the IC.

P.Plat-Appl Usage of Hardware Platform
The Smartcard Embedded Software is designed so that the requirements from the following documents are met: (i) IC guidance documents such as the hardware data sheet, and the hardware application notes, and (ii) findings of the IC evaluation reports relevant for the Smartcard Embedded Software.

Application Note:
This policy was defined as an assumption in [STIC].

P.Resp-Appl Treatment of User Data
All User Data are owned by Smartcard Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as defined for the specific application context.

Application Note:
This policy was defined as an assumption in [STIC].

P.Check-Init The Embedded software shall provide a function to check initialisation data. These data are injected by the IC Manufacturer into EEPROM to provide the possibility for TOE identification and traceability.

Application Note:
This policy was defined as an assumption in [STIC].

P.Key-Function Usage of Key-dependent Functions
Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced).

Application Note:
This policy was defined as an assumption in [STIC].

P.Process-Card Protection during Packaging, Finishing and Personalisation

Application Note:
This policy was defined as an assumption in [STIC].

4 SECURITY OBJECTIVES

4.1 Security Objectives for the TOE

OT.EMSEC_Design *Provide physical emanations security*
Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.

OT.Lifecycle_Security *Lifecycle security*
The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-import or re-generation.

OT.SCD_Secrecy *Secrecy of the signature-creation data*
The secrecy of the SCD (used for signature generation) is reasonably assured against attacks with a high attack potential.

OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*
The TOE shall ensure the correspondence between the SVD and the SCD. The TOE shall verify on demand the correspondence between the SCD stored in the TOE and the SVD if it has been sent to the TOE.

OT.SVD_Auth_TOE *TOE ensures authenticity of the SVD*
The TOE provides means to enable the CGA to verify the authenticity SVD that has been exported by that TOE.

OT.Tamper_ID *Tamper detection*
The TOE provides system features that detect physical tampering of a system component, and use those features to limit security breaches.

OT.Tamper_Resistance *Tamper resistance*
The TOE prevents or resists physical tampering with specified system devices and components.

OT.Init *SCD/SVD generation*

The TOE provides security features to ensure that the generation of the SCD and the SVD is invoked by authorised users only.

OT.SCD_Unique *Uniqueness of the signature-creation data*
The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible low.

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

OT.DTBS_Integrity_TOE *Verification of the DTBS-representation integrity*
The TOE shall verify that the DTBS-representation received from the SCA has not been altered in transit between the SCA and the TOE. The TOE itself shall ensure that the DTBS representation is not altered by the TOE as well. Note, that this does not conflict with the signature-creation process where the DTBS itself could be hashed by the TOE.

OT.Sigy_SigF *Signature generation function for the legitimate signatory only*
The TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

OT.Sig_Secure *Cryptographic security of the electronic signature*
The TOE generates electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the electronic signatures. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.

IC Objectives:

We took all IC objectives present in [STIC]. A more complete description of the IC objectives is available in [STIC].

O.Leak-Inherent	Protection against Inherent Information Leakage
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunctions
O.Phys-Manipulation	Protection against Physical Manipulation
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality

O.Identification
The IC must provide means to store Initialisation Data and Pre-personalisation Data in its non-volatile memory. The Initialisation Data (or parts of them) are used for TOE identification.

O.RND
The IC will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy.

O.HW_DES3	Triple DES Functionality
O.MEM_ACCESS	Area based Memory Access Control
O.SFR_ACCESS	Special Function Register Access Control

O.MF_FW MIFARE Firewall
The IC shall provide separation between the “MIFARE Operating System” IC Dedicated Support Software and the Smartcard Embedded Software. The separation shall comprise software execution and data.

O.CONFIG Protection of configuration data
The TOE prevents modification of configuration data – including configuration data for TSF – after TOE delivery. More specifically it shall be ensured that the configuration values determined during the test phase are fixed after TOE delivery.

4.2 Security Objectives for the Environment

OE.SCD_SVD_Corresp *Correspondence between SVD and SCD*
The SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSVD Type1 shall verify the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.

OE.SCD_Transfer *Secure transfer of SCD between SSCD*
The SSCD Type1 shall ensure the confidentiality of the SCD transferred to the TOE. The SSCD Type1 shall prevent the export of a SCD that already has been used for signature generation by the SSCD Type2. The SCD shall be deleted from the SSCD Type1 whenever it is exported into the TOE.

OE.SCD_Unique *Uniqueness of the signature-creation data*
The SSCD Type1 shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible low.

OE.CGA_QCert *Generation of qualified certificates*
The CGA generates qualified certificates which include inter alia

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

OE.SVD_Auth_CGA *CGA verifies the authenticity of the SVD*

The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

OE.HI_VAD *Protection of the VAD*
If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.

OE.SCA_Data_Intend *Data intended to be signed*
The SCA

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

The following environment objectives are taken from the IC security target [STIC]:

OE.Plat-Appl Usage of Hardware Platform (development phase)
TO ENSURE THAT THE TOE IS USED IN A SECURE MANNER THE SMARTCARD EMBEDDED SOFTWARE SHALL BE DESIGNED SO THAT THE REQUIREMENTS FROM THE FOLLOWING DOCUMENTS ARE MET: (I) HARDWARE DATA SHEET FOR THE TOE, (II) TOE APPLICATION NOTES, AND (III) FINDINGS OF THE TOE EVALUATION REPORTS RELEVANT FOR THE SMARTCARD EMBEDDED SOFTWARE.

OE.Resp-Appl Treatment of User Data (development phase)
Security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as required by the security needs of the specific application context.

OE.Process-TOE Protection during IC Development and Production

OE.Process-Card Protection during Packaging, Finishing and Personalisation

O.Check-Init The Embedded software shall provide a function to check initialisation data.

Application Note:
This objective was defined as objective for environment in [STIC].

5 IT SECURITY REQUIREMENTS

We present in this section the SFR of the TOE. SFR concerning IC are presented in [STIC]. We do not copy them in this section.

5.1 TOE IT SECURITY FUNCTIONAL REQUIREMENTS

5.1.1 FCS: CRYPTOGRAPHIC SUPPORT

5.1.1.1 FCS_CKM cryptographic key management

FCS_CKM.1 Cryptographic key generation

FCS CKM.1/RSA-SFM

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA key generation named RSA SFM**] and specified cryptographic key sizes [**1024 bits or 1280 bits or 1536 bits, or 1792 bits or 2048 bits**] that meet the following [**ANSI X9.31**]

FCS CKM.1/RSA-CRT
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA CRT key generation**] and specified cryptographic key sizes [**1024 bits or 1280 bits or 1536 bits, or 1792 bits or 2048 bits**] that meet the following [**ANSI X9.31**]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1
The TSF shall destroy cryptographic keys *in case of regeneration of a new SCD or in case of re-importation of the SCD* in accordance with a specified cryptographic key destruction method [**overwriting the buffer containing the key**] that meets the following: [**no standard**].

Application note:
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 or re-imported by the TOE. The re-import and re-generation are the unique way to ask for the destruction of SCD.

FCS_CKM.4.1/External Authentication Keys
The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting the buffer containing the key**] that meets the following: [**no standard**].

Application note:
The destruction of the previous External Authentication keys is mandatory when they are updated.

FCS_CKM.4.1/Secure Messaging Keys
The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting the buffer containing the key**] that meets the following: [**no standard**].

Application note:
The destruction of the previous Secure Messaging keys is mandatory when they are updated.

5.1.1.2 FCS_ COP Cryptographic operation

FCS_COP.1 Cryptographic operation

FCS_COP.1.1/ CORRESP

The TSF shall perform [**SCD/SVD correspondence verification**] in accordance with a specified cryptographic algorithm [**RSA key computation**] and cryptographic key sizes [**1024 bits or 1280 bits or 1536 bits or 1792 bits or 2048 bits**] that meet the following: [**PKCS#1**].

FCS_COP.1.1/ SIGNING
The TSF shall perform [**Digital signature-generation**] in accordance with a specified cryptographic algorithm [**RSA using Private Key**] and cryptographic key sizes [**1024 bits or 1280 bits or 1536 bits or 1792 bits or 2048 bits**] that meet the following: [padding **PKCS #1 V1.5 Block Type 1**].

Application Note:
The bigger RSA Private key that can be imported by this applet is 2048 bits (using the command PUT DATA).

FCS_COP.1.1/ Secure Messaging Signature

The TSF shall perform [**Secure Messaging Signature**] in accordance with a specified cryptographic algorithm [**Triple DES MAC3**] and cryptographic key sizes [**128 and 192 bits**] that meet the following: [**FIPS PUB 46-3 and CNS**].

Application Note:
This algorithm is used during:

- Secure Messaging: for computation of signature (SIG OUT) of outgoing APDU commands and verification of signature (SIG IN) of received APDU commands

Application Note:
The IC implements the 3DES algorithm required in the requirement above (see FCS_COP in the IC SFR section of [STIC]).

FCS_COP.1.1/ 3DES External Authentication

The TSF shall perform [**3DES External Authentication**] in accordance with a specified cryptographic algorithm [**Triple DES MAC3**] and cryptographic key sizes [**128 and 192 bits**] that meet the following: [**FIPS PUB 46-3 and CNS**].

Application Note: This algorithm is used during:

- External Authentication: to verify the challenge sent by the terminal

Application Note:
The IC implements the 3DES algorithm required in the requirement above (see FCS_COP in the IC SFR section of [STIC]).

FCS_COP.1.1/ Secure Messaging Encryption/Decryption

The TSF shall perform [**Secure Messaging Encryption/Decryption**] in accordance with a specified cryptographic algorithm [**Triple DES CBC encryption/decryption**] and cryptographic key sizes [**128 and 129 bits**] that meet the following: [**FIPS PUB 46-3 and CNS**].

Application Note: This algorithm is used during:

- Secure Messaging: for encryption of data (ENC OUT) for outgoing APDU commands and decryption of data (ENC IN) for received APDU commands

Application Note:
The IC implements the 3DES algorithm required in the requirement above (see FCS_COP in the IC SFR section of [STIC]).

FCS_COP.1.1/ RSA External Authentication

The TSF shall perform [**RSA External Authentication**] in accordance with a specified cryptographic algorithm [**RSA using Public Key**] and cryptographic key sizes [**1024 bits or 1280 bits or 1536 bits or 1792 bits or 2048 bits**] that meet the following: [**PKCS #1**].

Application Note: This algorithm is used during RSA External Authentication to verify the challenge sent by the terminal. The bigger RSA Public key that can be imported by the applet is 2048 bits (using the command PUT DATA).

5.1.2 FDP : USER DATA PROTECTION

5.1.2.1 FDP_ACC Access Control Policy

FDP ACC.1 Subset access control

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

> Application note:
> FDP_ACC.1/SVD Transfer SFP will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

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

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

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

FDP_ACC.1.1/Signature-creation SFP
The TSF shall enforce the [**Signature-creation SFP**] on

1. [**Sending of DTBS representation by SCA**]
2. [**Signing of DTBS-representation by Signatory**].

FDP_ACC.1.1/ PIN SFP
The TSF shall enforce the [**PIN SFP**] on

1. [**create of PINs (different from RAD) by Administrator and Signatory**]
2. [**update and unblock of PINs (including RAD) by Administrator and Signatory**]

> Application note:
> RAD creation is not covered by this requirement because it is already covered by Personalisation SFP.

FDP_ACC.1.1/ External Authentication Keys SFP
The TSF shall enforce the [**External Authentication Keys SFP**] on [**create, update and unblock of External Authentication Keys by Administrator and Signatory**].

FDP_ACC.1.1/ Secure Messaging keys SFP
The TSF shall enforce the [**Secure Messaging keys SFP**] on [**create, update and unblock of Secure Messaging Keys by Administrator**].

5.1.2.2 FDP_ACF access control function

FDP_ACF.1 Security attribute based access control

Correspondence between attributes defined in SSCD Type 2 and Type 3 and applet attributes:

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

		SSCD Attribute	Applet Attribute	Explanation
General Attribute				
USER		ROLE	ROLE	Administrator, Signatory
Signature-creation attribute				
SCD operational	Name:	SCD operational	SCD.AC_USE	In this applet , “SCD operational” corresponds to the access condition SCD.AC_USE. Its status is “Yes” if and only if the access condition is satisfied.
	Associated to:	SCD	SCD	
	Status:	No, Yes	Not Satisfied (No), Satisfied (Yes)	
sent	Name:	sent by an authorised SCA	MAC (computed with SCD.SIG_USE)	“sent by an authorised SCA” corresponds to the MAC associated to

	Associated to:	DTBS	DTBS	the message; SCA is authenticated by verifying this MAC using secure messaging (in SIG mode) with the Key SCD.SIG_USE.
	Status:	No, Yes	Not Verified (No), Verified (Yes)	
Initialisation attribute (SSCD Type 2)				
SCD/SVD management (TYPE 2)	Name:	SCD/SVD management	DF.AC_APPEND DF.AC_UPDATE SCD.AC_CHANGE	In this applet, there are three ways to import an SCD: - create and define the SCD object - update the SCD value and its attributes - update the SCD value. These operations correspond respectively to the applet commands PUT DATA OCI (creation mode), PUT DATA OCI (update mode) and CHANGE KEY DATA. And they are respectively protected by the access conditions DF.AC_APPEND, DF.AC_UPDATE and SCD.AC_CHANGE. Note: DF.AC_APPEND, DF.AC_UPDATE, SCD.AC_CHANGE are viewed as attributes of USER since they are used to authenticate the USER.
	Associated to:	USER	USER	
	Status:	Authorised, Not Authorised	Satisfied (Authorised), Not Satisfied (Not Authorised)	
Secure SCD Import allowed	Name:	Secure SCD Import allowed	MAC (computed with DF.SIG_UPDATE/APPEND or SCD.SIG_CHANGE)	"Secure SCD Import allowed" corresponds to the device authentication during secure messaging (in SIG mode). The secure messaging key to use depends on the issued applet command for SCD import: - DF.SIG_UPDATE/APPEND for PUT DATA OCI (creation mode) and PUT DATA OCI (update mode) - SCD.SIG_CHANGE for CHANGE KEY DATA.
	Associated to:	SCD	SCD	
	Status:	No, Yes	Not Verified (No), Verified (Yes)	
Initialisation attribute (SSCD Type 3)				
SCD/SVD management	Name:	SCD/SVD management	SCD.AC_GENKEYPAIR	In this applet, "SCD/SVD management" corresponds to the access condition SCD.AC_GENKEYPAIR. Key generation is authorised if and only if the access condition is satisfied. Note: The SCD.AC_GENKEYPAIR is viewed as an attribute of USER since it is used to authenticate the USER.
	Associated to:	USER	USER	
	Status:	Authorised, Not Authorised	Satisfied (Authorised), Not Satisfied (Not Authorised)	

Table 3 Correspondence between attributes defined in SSCD Type 2 and Type 3 and applet attributes

SVD transfer SFP

FDP_ACF.1.1/ SVD transfer SFP
The TSF shall enforce the [**SVD transfer SFP**] to objects based on [**General attribute**]

FDP_ACF.1.2/ SVD transfer SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

> **The user with the security attribute "role" set to "Administrator” or to "Signatory" is allowed to export SVD.**

FDP_ACF.1.3/ SVD transfer SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:
[Proprietary information removed]

FDP_ACF.1.4/ SVD transfer SFP
The TSF shall explicitly deny access of subjects to objects based on the rule: [**none**]

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

Initialisation SFP

FDP_ACF.1.1/Initialisation SFP
The TSF shall enforce the [**Initialisation SFP**] to objects based on [**General attribute**] and [**Initialisation attribute**].

FDP_ACF.1.2/ Initialisation SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

> **The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to " authorised" is allowed to generate SCD/SVD pair.**

FDP_ACF.1.3/ Initialisation SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]

FDP_ACF.1.4/ Initialisation SFP
The TSF shall explicitly deny access of subjects to objects based on the rule:

> **The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.**
>
> ***[Proprietary information removed]***

SCD Import SFP

FDP_ACF.1.1/ SCD Import SFP
The TSF shall enforce the [**SCD Import SFP**] to objects based on [**General attribute**] and [**Initialisation attribute group**].

FDP_ACF.1.2/ SCD Import SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".

FDP_ACF.1.3/ SCD Import SFP
The TSF shall explicitly Authorise access of subjects to objects based on the following additional rules:
[Proprietary information removed]

FDP_ACF.1.4/ SCD Import SFP
The TSF shall explicitly deny access of subjects to objects based on the rule:

a) **The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".**
b) **The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no".**

Personalisation SFP

FDP_ACF.1.1/ Personalisation SFP
The TSF shall enforce the [**Personalisation SFP**] to objects based on [**General attribute**]

FDP_ACF.1.2/ Personalisation SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
User with the security attribute "role" set to "Administrator" is allowed to create the RAD
[Proprietary information removed]

FDP_ACF.1.3/ Personalisation SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]

FDP_ACF.1.4/ Personalisation SFP
The TSF shall explicitly deny access of subjects to objects based on the rule: [**none**]

Application Note:
The “Personalisation SFP” controls creation operation on a specific PIN that is the RAD.
In this requirement, DF is the folder where PIN has to be created.

PIN SFP
The “Personalisation SFP” controls creation operation on a specific PIN that is the RAD. The “PIN FSP” concerns:

- All other PINs (except RAD) of the application and all their related operations (creation, update, unblock and use).
- The RAD for the other operations except creation (already covered by Personalisation SFP)

FDP_ACF.1.1/ PIN SFP
The TSF shall enforce the [**PIN SFP**] to objects based on
Subjects: Signatory, Administrator
Objects: PINs
Attributes: see Table 1 Applet Attributes (1)

FDP_ACF.1.2/ PIN SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
User with the security attribute "role" set to "Administrator" or set to "Signatory" is allowed to create the PINs.
[Proprietary information removed]

FDP_ACF.1.3/ PIN SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]

FDP_ACF.1.4/ PIN SFP
The TSF shall explicitly deny access of subjects to objects based on the rule: [**none**]

Application Note:

- In this requirement, DF is the folder containing the PIN.

Signature Creation SFP

FDP_ACF.1.1/ Signature-creation SFP
The TSF shall enforce the [**Signature-creation SFP**] to objects based on [**General attribute**] and [**Signature-creation attribute**].

FDP_ACF.1.2/ Signature-creation SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".

[Proprietary information removed]

FDP ACF.1.3/ Signature-creation SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **Signature creation is only allowed in “Personalised State” life cycle**

FDP_ACF.1.4/Signature-creation SFP
The TSF shall explicitly deny access of subjects to objects based on the rule:

a) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS which is not sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".

b) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no".

External Authentication Keys SFP

FDP_ACF.1.1/ External Authentication Keys SFP
The TSF shall enforce the [**External Authentication Keys SFP**] to objects based on
Subjects: Signatory, Administrator
Objects: External Authentication Keys
Attributes: see Table 2 Applet Attributes (2)

FDP_ACF.1.2/ External Authentication Keys SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

User with the security attribute "role" set to "Administrator" or set to "Signatory" is allowed to create the External Authentication Keys.
[Proprietary information removed]

FDP_ACF.1.3/ External Authentication Keys SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]

FDP_ACF.1.4/ External Authentication Keys SFP
The TSF shall explicitly deny access of subjects to objects based on the rule: [**none**]

Secure Messaging Keys SFP

FDP_ACF.1.1/ Secure Messaging Keys SFP
The TSF shall enforce the [**Secure Messaging Keys SFP**] to objects based on Personalisation SFP

Subjects: Signatory, Administrator
Objects: Secure Messaging Keys
Attributes: see Table 2 Applet Attributes (2)

FDP_ACF.1.2/ Secure Messaging Keys SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[Proprietary information removed]

FDP_ACF.1.3/ Secure Messaging Keys SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**]

FDP_ACF.1.4/ Secure Messaging Keys SFP
The TSF shall explicitly deny access of subjects to objects based on the rule: [**none**]

5.1.2.3 FDP_ETC：Export to outside TSF control

FDP_ETC.1: Export of user data without security attributes

FDP_ETC.1.1/ SVD transfer
The TSF shall enforce the [**SVD transfer SFP**] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2/ SVD transfer
The TSF shall export the user data without the user data's associated security attributes.

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

5.1.2.4 FDP_ITC Import From outside TSF control

FDP_ITC.1: Import of user data without security attributes

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

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

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

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

FDP_ITC.1.1/DTBS
The TSF shall enforce the [**Signature-creation SFP**] when importing user data, controlled under the SFP, from outside of the TSC.

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

FDP_ITC.1.3/DTBS
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [**DTBS-representation shall be sent by an Authorised SCA**].

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

FDP_ITC.1.1/External Authentication keys
The TSF shall enforce the [**External Authentication keys SFP**] when importing user data, controlled under the SFP, from outside of the TSC.

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

FDP_ITC.1.3/ External Authentication keys
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [**none**].

FDP_ITC.1.1/ Secure Messaging keys
The TSF shall enforce the [**Secure Messaging keys Import SFP**] when importing user data, controlled under the SFP, from outside of the TSC.

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

FDP_ITC.1.3/ Secure Messaging keys
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [**none**].

5.1.2.5 FDP_RIP Residual information protection

FDP_RIP.1: Subset residual information protection

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

5.1.2.6 FDP_SDI Stored data integrity

FDP_SDI2 Stored data integrity monitoring

Persistent data
The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data"
SCD
RAD
SVD (if persistently stored by TOE)

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

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

DTBS-representation

The Protection Profiles SSCD TYPE 2 and TYPE3 specify that the DTBS representation temporarily stored by TOE have the user data attribute "integrity checked stored data".
The requirements FDP_SDI.2.1/DTBS and FDP_SDI.2.2/DTBS are not application to our TOE since the DTBS (the message to be signed) is not stored by the TOE.

5.1.2.7 FDP_UCT Inter-TSF user data confidentiality transfer protection

FDP_UCT.1 Basic data exchange confidentiality

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

Application Note: ***[Proprietary information removed]***

5.1.2.8 FDP_UIT Inter-TSF user data integrity transfer protection

FDP_UIT.1: Data exchange integrity

SVD transfer

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

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

Application Note: ***[Proprietary information removed]***

Receiver

FDP_UIT.1.1/ TOE DTBS
The TSF shall enforce the [**Signature-creation SFP**] to be able to [**receive**] the DTBS-representation in a manner protected from [**modification, deletion and insertion**] errors.

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

Application Note: ***[Proprietary information removed]***

5.1.3 FIA: IDENTIFICATION AND AUTHENTICATION

5.1.3.1 FIA_AFL Authentication failure

FIA_AFL.1 Authentication failure handling

FIA_AFL is specific to the RAD. We define a new requirement “FIA AFL.1.1/General” applicable for all authentication data (External Authentication keys, Secure Messaging Key for Signature/Verification). These different authentication data may be used to control access to different operations (examples: DF.AC_APPEND DF.AC_UPDATE, SCD.AC_CHANGE, SCD.AC_GENKEYPAIR…).

FIA AFL.1.1
The TSF shall detect when [**number N**] 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**].

> Application Note:
> The Authentication Try Limit N, defined during personalisation, must verify 1 ≤ N ≤ 3.

FIA AFL.1.1/General
The TSF shall detect when [**number N**] unsuccessful authentication attempts occur related to [**consecutive failed authentication attempts**].

FIA AFL.1.2/General
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**block the corresponding authentication data External Authentication keys, Secure Messaging Key for Signature/Verification**].

> Application Note:
> The Authentication Try Limit N, defined during personalisation, must verify 1 ≤ N ≤ 3.

5.1.3.2 FIA_ATD User attribute definition

FIA ATD.1 User attribute definition

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

5.1.3.3 FIA_UAU User authentication

FIA UAU.1 Timing of authentication

FIA UAU.1.1
The TSF shall allow
[**Identification of the user by means of TSF required by FIA_UID.1]**
[Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP_ITC.1ISCD import]
[Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE]
[Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import]
on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

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

Application note:
"Local user" mentioned in component FIA_UAU.1.1 is the user using the trusted path provided between the SGA in the TOE environment and the TOE as indicated by FTP_TRP.1/SCA and FTP TRP.1/TOE.

5.1.3.4 FIA_UID User Identification

FIA_UID.1Timing of identification

FIA UID.1.1
The TSF shall allow
[Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP_ITC.1/SCD import]
[Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE]
[Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import]
on behalf of the user to be performed before the user is identified.

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

5.1.4 FMT: SECURITY MANAGEMENT

5.1.4.1 FMT_MOF Management of functions in TSF

FMT_MOF.1 Management of security functions behaviour

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

5.1.4.2 FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1/ Administrator-Initialisation
The TSF shall enforce the [**Initialisation SFP**] to restrict the ability to [**modify**] the security attributes [**SCD / SVD management**] to [**Administrator**].

Application Note:
[Proprietary information removed]

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

Application Note:
[Proprietary information removed]

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

Application Note:
[Proprietary information removed]

FMT_MSA.1.1/ External Authentication Keys
The TSF shall enforce the [**External Authentication Keys SFP**] to restrict the ability to [**modify**] the security attributes [**related to External Authentication Keys (see** Table 2 Applet Attributes (2)**)**] to [**Administrator**]

FMT_MSA.1.1/Secure Messaging Keys
The TSF shall enforce the [**Secure Messaging Keys SFP**] to restrict the ability to [**modify**] the security attributes [**related to Secure Messaging Keys (see** Table 2 Applet Attributes (2)**)**] to [**Administrator**].

Application Note:
This requirement deals with Secure Messaging Keys used for operations on the SCD and the RAD.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1
The TSF shall ensure that only secure values are accepted for security attributes.

FMT MSA.3 Static attribute initialisation

FMT_MSA.3.1
The TSF shall enforce the [**Initialisation SFP**] and [**Signature-creation SFP**] and [**SCD Import SFP**] and [**External Authentication Keys SFP**] and [**Secure Messaging Keys SFP**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

Refinement:
[Proprietary information removed]

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

5.1.4.3 FMT_MTD Management of TSF data

FMT_MTD.1 Management of TSF data

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

Application Note: ***[Proprietary information removed]***

5.1.4.4 FMT_SMR Security management rotes

FMT_SMR.1 Security roles

FMT_SMR.1.1
The TSF shall maintain the roles [**Administrator**] and [**Signatory**].

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

5.1.5 FPT: PROTECTION OF THE TSF

5.1.5.1 FPT_AMT Underlying Abstract machine test

FPT_AMT.1 Underlying Abstract machine test

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.

> Refinement:
> In this Security Target (ST), the underlying abstract machine test is the Integrated Circuit (IC).

5.1.5.2 FPT_EMSEC TOE Emanation

FPT EMSEC.1.1 TOE Emanation

FPT_EMSEC.1.1
The TOE shall not emit [**Side channel emission**] in excess of [**limits specified by the state-of-the-art attacks on smart card IC**] enabling access to [**RAD and SCD**].

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

5.1.5.3 FPT_FLS Failure secure

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur :[**power shortage, over voltage, over and under clock frequency, integrity errors**].

5.1.5.4 FPT_PHP TSF physical Protection

FPT_PHP.1 Passive detection of physical attack

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

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

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1
The TSF shall resist [**physical manipulation and physical probing**] to the [**integrated circuit**] by responding automatically such that the TSP is not violated

> Application Note:
> This requirement is connected to the IC FPT_PHP.3 [STIC]. The IC detects physical attacks and reacts to these attacks by resetting the card or raising an exception. In these two cases, IC notifies the attack to the software.

5.1.5.5 FPT_TST TSF self test

FPT_TST.1 TSF testing

FPT_TST.1.1
The TSF shall run a suite of self-tests [**during initial start-up**] to demonstrate the correct operation of the TSF.

FPT_TST.1.2
The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

FPT_TST.1.3
The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.1.6 FTP: TRUSTED PATH / CHANNEL

5.1.6.1 FTP_ITC Inter-TSF trusted channel

FTP ITC.1 Inter-TSF trusted Channel

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

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

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

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

Application Note: ***[Proprietary information removed]***

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

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

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

Application Note:
Key to be used for secure messaging is specified in the SM condition SVD.SIG_READ_OUT.

Application note (from [SSCD2]):
FTP_ITC.1/SVD Transfer will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

Application note (from this Security Target):
In this security target, SVD is exported but never imported. Thus only “FTP_ITC.1.1/ SVD transfer” from [SSCD3] is applicable. In [SSCD2], “FTP_ITC.1.1/ SVD transfer” concerns import and export of SVD. The

part concerning the SVD export has exactly the same text than the requirement included in this Security Target.

FTP_ITC.1.1/ DTBS import
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/ DTBS import
The TSF shall permit [**the remote trusted IT product**] to initiate communication via the trusted channel.

FTP_ITC.1.3 DTBS import
The TSF shall initiate communication via the trusted channel for [**signing DTBS-representation**]

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

Application Note: ***[Proprietary information removed]***

5.1.6.2 FTP _TRP Trusted path

FTP_TRP.1 Trusted path

FTP_TRP.1.1/TOE
The TSF shall provide a communication path between itself and [**local**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

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

FTP_TRP.1.3/TOE
The TSF shall require the use of the trusted path for [**initial user authentication**].

Application Note: ***[Proprietary information removed]***

5.2 TOE SECURITY ASSURANCE REQUIREMENTS

The Assurance requirements is EAL4 augmented by components:
ADV_IMP.2 Implementation of the TSF,
AVA_MSU.3: Analysis of insecure states,
AVA VLA.4: Highly resistant.

5.2.1 CONFIGURATION MANAGEMENT (ACM)

EAL4 augmented claimed level requires the following ACM class components:
ACM AUT.1 Partial CM automation
ACM_CAP.4 Generation support and acceptance procedures
ACM_SCP.2 Problem tracking CM coverage
Refer to CC Part 3 for description.

5.2.2 DELIVERY AND OPERATION (ADO)

EAL4 augmented claimed level requires the following ADO class components:
ADO DEL.2 Detection of modification

ADO_IGS.1 Installation, generation, and start-up procedures
Refer to CC Part 3 for description.

5.2.3 DEVELOPMENT (ADV)

EAL4 augmented claimed level requires the following ADV class components:
ADV_FSP.2 Fully defined external interfaces
ADV_HLD.2 Security enforcing high-level design
ADV_IMP.2 Implementation of the TSF
ADV_LLD.1 Descriptive low-level design
ADV_RCR.1 Informal correspondence demonstration
ADV_SPM.1 Informal TOE security policy model
Refer to CC Part 3 for description.

5.2.4 GUIDANCE DOCUMENTS (AGD)

EAL4 augmented claimed level requires the following AGD class components:
AGD ADM.1 Administrator guidance
AGD_USR.1 User guidance
Refer to CC Part 3 for description.

5.2.5 LIFE CYCLE SUPPORT (ALC)

EAL4 augmented claimed level requires the following ALC class components:
ALC_DVS.1 Identification of security measures
ALC_LCD.1 Developer defined life-cycle model
ALC_TAT.1 Well-defined development tools
Refer to CC Part 3 for description.

5.2.6 TESTS (ATE)

EAL4 augmented claimed level requires the following ATE class components:
ATE_COV.2 Analysis of coverage
ATE_DPT.1 Testing: high-level design
ATE_FUN.1 Functional testing
ATE_IND.2 Independent testing- sample
Refer to CC Part 3 for description.

5.2.7 VULNERABILITY ASSESSMENT (AVA)

EAL4 augmented claimed level requires the following AVA class components:
AVA_MSU.3 Analysis and testing of insecure states
AVA_SOF.1 Strength of TOE security function evaluation
AVA VLA.4 Highly resistant
Refer to CC Part 3 for description.

5.3 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

This section describes the IT security requirements that are to be met by the IT environment of the TOE. The IT environment of the TOE is composed of the Certification Generation Application (CGA) and the Signature Creation Application (SCA).
These requirements are as stated in [SSCD2] & [SSCD3].

5.3.1 Signature key generation (SSCD Type1)

5.3.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA key generation**] and specified cryptographic key sizes [**1024 bits or 1280 bits or 1536 bits or 1792 bits and 2048 bits**] that meet the following: [**no standard**].

5.3.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1/Type1
The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**physical irreversible destruction of the stored key**] that meets the following: [**no standard**].

Application notes:
The cryptographic key SCD will be destroyed automatically after export .

5.3.1.3 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 [**RSA key computation**] and cryptographic key sizes [**1024 bits or 1280 bits or 1536 bits or 1792 bits and 2048 bits**] that meet the following: [**PKCS#1**].

5.3.1.4 Subset access control (FDP_ACC.1)

FDP_ACC.1.1/SCD Export SFP
The TSF shall enforce the [**SCD Export SFP**] on [**export of SCD by Administrator**].

5.3.1.5 Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1.1/ Sender
The TSF shall enforce the [**SCD Export SFP**] to be able to [**transmit**] objects in a manner protected from unauthorised disclosure.

5.3.1.6 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/SCD Export
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/SCD Export
The TSF shall permit [**the remote trusted IT product**] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SCD Export
The TSF or the SSCD Type2 shall initiate communication via the trusted channel for [**SCD export**].

Refinement:
The mentioned TSF is the SSCD Type 2
Application note:
If the TOE exports the SVD to a SSCD Type2 and the SSCD Type 2 holds the SVD then the trusted channel between the TOE and the SSCD type 2 will be required .

5.3.2 Certification generation application (CGA)

5.3.2.1 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: [**Triple DES 128 bits or 192 bits**].

5.3.2.2 Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/ CGA
The TSF shall perform [**import the SVD**] in accordance with a specified cryptographic key access method [**import through a secure channel**] that meets the following: [**no standard**].

5.3.2.3 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/SVD Import
The TSF shall enforce the [**SVD import SFP**] to be able to [**receive**] user data in a manner protected from [**modification and insertion**] errors.

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

5.3.2.4 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/SVD Import
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/SVD Import
The TSF shall permit [**the TSF**] to initiate communication via the trusted channel.

FTP_ITC.1.3/SVD Import
The TSF or the remote trusted IT product or the TOE shall initiate communication via the trusted channel for import SVD.

5.3.3 Signature creation application (SCA)

5.3.3.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/SCA Hash
The TSF shall perform [**hashing the DTBS**] in accordance with a specified cryptographic algorithm [**SHA-1**] and cryptographic key sizes [**none**] that meet the following: [**FIPS 180-1**].

5.3.3.2 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/SCA DTBS
The TSF shall enforce the [**Signature-creation SFP**] to be able to [**transmit**] user data in a manner protected from [**modification, deletion and insertion**] errors.

FDP_UIT.1.2/SCA DTBS

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

5.3.3.3 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SCA DTBS
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/ SCA DTBS
The TSF shall permit [**the TSF**] to initiate communication via the trusted channel.

FTP_ITC.1.3/SCA DTBS
The TSF or the remote trusted IT product shall initiate communication via the trusted channel for [**signing DTBS-representation by means of the SSCD**].

Refinement:
The mentioned TSF is the SCA

5.3.3.4 Trusted path (FTP_TRP.1)

The trusted path between the TOE and the SCA will be required only if the human interface for user authentication is not provided by the TOE itself but by the SCA.

FTP_TRP.1.1/ SCA
The TSF shall provide a communication path between itself and [**local**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2/ SCA
The TSF shall permit [**the TSF**] 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 by RAD**].

Refinement:
The mentioned TSF is the SCA

5.4 SECURITY REQUIREMENTS FOR THE NON-IT ENVIRONMENT

R.Administrator_Guide *Application of Administrator Guidance*
The implementation of the requirements of the Directive, ANNEX II "Requirements for certification service-providers issuing qualified certificates", literal (e), stipulates employees of the CSP or other relevant entities to follow the administrator guidance provided for the TOE. Appropriate supervision of the CSP or other relevant entities shall ensure the ongoing compliance.

R.Sigy_Guide *Application of User Guidance*
The SCP implementation of the requirements of the Directive, ANNEX II "Requirements for certification service-providers issuing qualified certificates", literal (k), stipulates the signatory to follow the user guidance provided for the TOE.

R.Sigy_Name *Signatory's name in the Qualified Certificate*
The CSP shall verify the identity of the person to which a qualified certificate is issued according to the Directive [1], ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (d). The CSP shall verify that this person holds the SSCD, which implements the SCD corresponding to the SVD to be included in the qualified certificate.

RE.Process-Card Protection during Packaging, Finishing and Personalisation
The Card Manufacturer (Phase 4 up to the end of Phase 6) shall use adequate security measures to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

6 TOE SUMMARY SPECIFICATION

6.1 Security Functions

SF.KEYGEN - Key generation
The TOE generates the RSA key pair SCD/SVD of size 1024 bits or 1280 bits or 1536 bits or 1792 bits and 2048 bits. This function is claimed SOF-HIGH because the RSA key generation is based on random generation.

SF.SIG - Signature creation
The TOE signs with an RSA private key, a data (DTBS) imported from outside.

SF.USER_AUTH – User Authentication
This function ensures the user authentication. Several authentication mechanisms are available:

- PIN comparison
- External Authentication using Challenge/response protocol with 3DES keys (128 or 192 bits) and MAC retail algorithm (MAC3)
- External Authentication using Challenge/response protocol with Public RSA keys (1024 bits or 1280 bits or 1536 bits or 1792 bits and 2048 bits)

This function is claimed SOF-HIGH:

- For the authentication based on PIN and
- The external authentication that is based on random generation

SF.PIN – PIN Management
This function manages operations related to PIN. It enforces access control on PIN related operations, based on access condition and secure messaging conditions.

SF.KEY – Key Management
This function manages operations related to keys. It enforces access control on key related operations, based on access condition and secure messaging conditions.

SF.SM – Secure Messaging
The TOE provides security services related to information exchanged between the TOE and external users.
It ensures:

- The integrity and/or confidentiality of received sensitive data
- and the integrity and/or confidentiality of transmitted sensitive data

This function is claimed SOF-HIGH for the mode MAC that is based on random generation.

SF.TEST - Self test
During start-up sequence, if any of the following events occurs, the card mutes itself:

- Blocked random generator
- Incorrect operation of the cryptographic module

This function is automatically executed at the start-up of the smart card.

SF.INTEGRITY - Data Integrity
The TOE checks the integrity of the cryptographic key SCD and the RAD (PIN). It is based on checksum computation and verification.

SF.PHYS - Physical attack: notification and resistance
This function provides ability for the software to react to physical attacks notified by the IC.

IC Security Functions:

We give here the security functions of the IC. In this description, the term TOE means IC.
The complete description is available in [STIC].

F.RNG: Random Number Generator
The random number generator continuously produces random numbers with a length of one byte.

F.HW-DES: Triple-DES Co-processor

F.OPC: Control of Operating Conditions

F.PHY: Protection against Physical Manipulation

F.LOG: Logical Protection

F.COMP: Protection of Mode Control

F.MEM ACC: Memory Access Control

F.SFR ACC: Special Function Register Access Control

Strength level for the TOE security functions:

IC Security Target [STIC] made a SOF claim “high” (SOF-HIGH) for all IC functions that are realised by probabilistic or permutational mechanisms: F.RNG, F.LOG, F.HW_DES.

7 Protection Profile CLAIMS

The PP [SSCD2] and [SSCD3] are claimed.

8 ACRONYMS

CC	Common Criteria
CGA	Certification Generation Application
DTBS	Data to be Signed
EAL	Evaluation Assurance Level
HI	Human Interface HW Hardware
I/0	Input/Output
OS	Operating System
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PP	Protection Profile
SCA	Signature-Creation Application
SCD	Signature-Creation Data
SDO	Signed Data Object
SOF	Strength of Function
SSCD	Secure Signature-Creation Device
SVD	Signature-Verification Data
TOE	Target of Evaluation
CRT	Chinese Reminder Theorem