Public Security Target

ID-One™ CIE Java Applet

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

TABLE OF CONTENTS

1 Introduction

1.1 Security target Reference

The Security target is identified as follows:

Title	URANIE – Public Security Target
Reference	FQR 110 7121 Ed5
Editor	Oberthur Technologies
CC version	3.1 revision 4
EAL	EAL4 augmented with AVA_VAN.5, and ALC_DVS.2

1.2 References

[ANSIX9.31]	"Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (DSA)" – ANSI X9.31-1998, American Bankers Association
[CC31-1]	"Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model" – September 2012, Version 3.1 revision 4
[CC31-2]	"Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements" – September 2012, Version 3.1 revision 4
[CC31-3]	"Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance requirements" – September 2012, Version 3.1 revision 4
[CIE]	C.I.E. – Carta di Identita Elettronica – Functional Specification – Version 2.0
[FIPS180-3]	"FIPS PUB 180-3, Secure Hash Standard" – October 2008 , National Institute of Standards and Technology
[JIL-COMP]	Joint Interpretation Library - Composite product evaluation for Smart Cards and similar devices – version 1.2
[PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard – June 14, 2002
[PP0035]	Security IC Platform Protection Profile – Version 1.0 15.06.2007
[SSCD2]	Protection Profile Type 2 - Secure Signature-Creation Device Type2 – 1.04,EAL 4+
[SSCD3]	Protection Profile SSCD Type 3 - Secure Signature-Creation Device Type3 – 1.05,EAL 4+
[7816-4]	Identification Cards/Integrated circuit cards - Part 4: Organization, security and commands for interchange – ISO/IEC 7816-4:2013,
[7816-8]	Identification Cards/Integrated circuit cards - Part 8: Commands for security operations – ISO/IEC 7816-8:2004
[7816-9]	Identification Cards/Integrated circuit cards - Part 9: Interindustry commands for card and file management – ISO/IEC 7816-9:2003
[9797-1]	Information technology/Security techniques - Message Authentication Codes (MACs) Part 1: Mechanisms using a block cipher – ISO/IEC 9797-1:2011
[11568-2]	Financial services - Key management (retail) - Part 2: symmetric ciphers, their key management and life cycle – ISO 11568-2:2012

2 Target Of Evaluation

2.1 Overview

2.1.1 TOE Type

The Target of Evaluation is a smartcard which is configured as a Secure signature creation Device (SSCD), used to create advanced or qualified signature in the sense of EC/1999/93. The TOE allows the signature creation key import (type 2) and on board signature creation key generation (type 3).

The TOE is a bare microchip with its external interfaces for communication. The physical medium on which the microchip is mounted is not part of the target of evaluation because it does not alter nor modify any security functions of the TOE.
The TOE may be used on several physical medium

- within an inlay or eCover;
- in a plastic card;
- within a USB key;
- Others;

2.1.2 Physical scope

The TOE is a composite product made up of the following components:

- A javacard applet [Applet];
- A javacard platform [PLT] composed with an IC, on which the [Applet] runs;

[PLT] and [Applet] are both developed by Oberthur Technologies. Details about the identification of these components can be found in §2.3.

The TOE is a javacard platform [PLT] on which:

- the javacard code of [Applet] has been loaded in the NVM.
- an instance of [Applet] has been created;
- the applet loading features is locked;

As the javacard platform [PLT] is in a closed configuration, no other applets than [Applet] can be loaded and can be executed on [PLT].

2.1.3 Logical scope

The logical scope of the TOE may be depicted as follows:

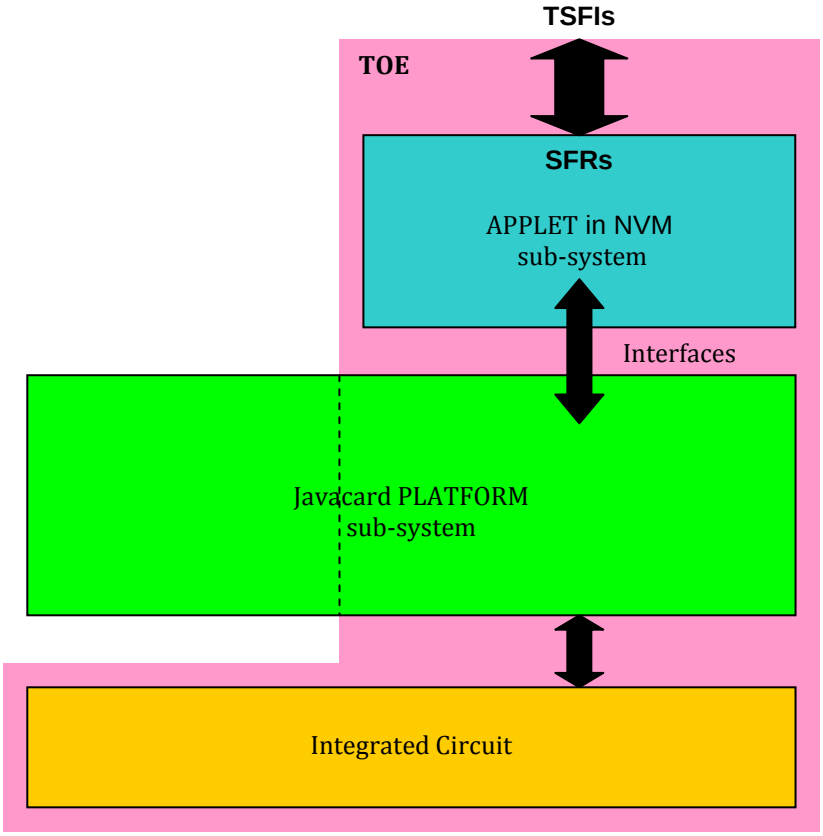


Figure 1: TOE overview

The scope of evaluation covers the following features of the TOE:

- Features covered by [SSCD2]and [SSCD3];
- Authentication mechanisms based on cryptographic scheme;
- Unblocking of RAD and authentication keys;
- Management of the authentication keys;

2.1.4 Required non-TOE hardware/software/firmware

The TOE is a Secure Signature Creation Device. It is an independent product and does not need any additional hardware/software/firmware to ensure its security.

In order to be powered up and to be able to communicate the TOE needs a card reader.

2.1.5 Usage and major security features

The TOE intended usage is to be used as a “secure signature creation device” (SSCD) of type 2 or 3, with respect to the European directive EC/1999/93.

Within the framework described by [SSCD2] and [SSCD3], the TOE allows to

- perform basic, advanced and qualified signature;
- authenticate the cardholder based on a PIN;
- authenticate one (or several) administrator(s) of the TOE, that may have special rights to administrate the SCD and SVD (generation, import), using either symmetric and/or asymmetric mechanisms, or PIN ;
- establish trusted channel, protected in integrity and confidentiality, with remote entities such as a SCA, a CGA or a SSCD type 1;

The scope of [SSCD2] and [SSCD3] is extended in several ways:

- The TOE may hold more than one SCD. Several SCDs may be used by the holder to sign documents
- SCD/SVD pairs and other cryptographic objects may be generated and/or imported after issuance at any time, and in particular, they may be updated during the TOE life cycle.
- The TOE may be used to realize digital signature in contact and/or contactless mode.
- A complete access control over object is ensured, whatever their type is: File or cryptographic objects (PIN, keys,…), ensuring it is not possible to bypass the access rules.

Depending on the use case and or the ability of the underlying javacard platform, the TOE may be used

- in contact mode (T=0 and/or T=1 protocol);
- in contactless protocol (T=CL);

2.2 Description

The TOE is a high security product that 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 settings;
- Onboard RSA key pair generation, compliant with [ISO7816-8];
- Triple DES based authentication, encryption and decryption, compliant with [ISO7816-4] and [ISO7816-8];
- RSA digital signature, compliant with [ISO7816-8];
- Contact and contactless support;

The TOE is compliant with the specification [CIE].

2.2.1 Data structure

The TOE manages several types of structures:

- A file system compliant with [7816-4]
- Base Security Objects (BSO) are containers for secret/sensitive data ;
- Security Environment Objects (SEO) are predefined sets of references to BSOs that can be used for confidentiality, digital signature and authentication.

2.2.1.1 File and File System

The TOE handles the following type of file (described in [7816-4]):

- Dedicated File
- Elementary File :
    - Transparent EF
    - Record EF: Linear Fixed, Linear Fixed TLV, Linear Variable, Linear Variable TLV, Cyclic Fixed

The Dedicated Files define the structure and the hierarchy of the file system.

The applet supports a file depth of at least 8 DFs, as long as enough memory is available on the card.

A Dedicated File is designated by its Extended File Identifier or “EFID” defined by a two-byte value.

A Dedicated File can contain:

- up to 127 Dedicated Files or Elementary Files : each EFID must be unique at the DF level.
- Base Security Objects (BSO) of all types: each BSO identifier must be unique at the DF level
- Security Environment Objects (SEO) : each SEO identifier must be unique at the DF level.

A DF can contain an arbitrary number of Base Security Objects (BSO) or Security Environment Objects (SEO).

2.2.1.2 Base Security Objects (BSO)

BSOs are a key component of the applet security architecture. They are used in cryptographic computations (PERFORM SECURITY OPERATION), in verification of access conditions and in secure communications between the card and terminal (secure messaging: C-ENC, C-SIG, R-ENC and R-SIG).

The objectives of a BSO are to:

- provide secure storage of an asset (secret/sensitive data), like PINs and cryptographic keys ;
- store the properties belonging to the asset (try counter, cryptographic algorithm, length, etc…)
- store the access conditions (AC) restricting the use, access and modification of the asset ;
- store the SM conditions (SMC) protecting the communications with the card when accessing the asset.

Thus, a BSO can reference other BSOs to define its access conditions and SM conditions.

2.2.1.3 Security Environment Objects (SEO)

A SEO is a predefined set of references to BSO that can be used in security operations. The user chooses which SEO corresponds to his needs and loads it into the current security environment.

A SEO can be considered as a security module which defines access control rules to modify the current security environment. These access control rules can be implemented by other BSOs. Thus, a SEO can reference other BSOs to implement its security policy.

2.2.2 ISO secure messaging

The TOE supports ISO secure messaging, both for incoming and outgoing data. In other words, the applet is capable of:

- Receiving incoming data protected in confidentiality (C-ENC) and/or integrity (C-SIG)
- Send outgoing data protected in confidentiality (R-ENC) and/or integrity (R-SIG)

2.2.3 Access Control Management

One of the Core features of the TOE is to provide access control management on any operations on any objects it handles (Files or BSO).

The Access conditions encoding is the compact encoding described in [7816-4], enhanced as described in [CIE].

Prior to granting access to a given operation, the TOE checks the requested access rights are fulfilled. Basically, an Access condition is granted if the security conditions are fulfilled. An access condition is a combination of security conditions based on identified keys/PIN/secrets:

- User Authentication (by PIN). It is used to authenticate the cardholder or a remote administrator
- Authentication of a remote administrator
- Mutual authentication with a remote IT
- Communication protected in integrity and confidentiality

2.2.4 Authentication of entities

The TOE allows the authentication of several entities in order to grant them some rights.

- User Authentication (by PIN). It is used to authenticate the cardholder or a remote administrator
- Authentication of a remote administrator (based on symmetric or asymmetric scheme)
- Mutual authentication with a remote IT and establishment of a trusted channel protected in integrity and confidentiality (based on symmetric scheme)

These authentication mechanisms are the cornerstone for the access control mechanisms use to grant access to resources (Files or BSO).

2.2.5 Electronic Services

The TOE supports as well several electronic services:

- Digital signature: this feature enables the cardholder to electronically signs documents. The signature may be either advanced or qualified (compliant with [SSCD2] and [SSCD3]).

2.3 Reference

The TOE is identified as follows:

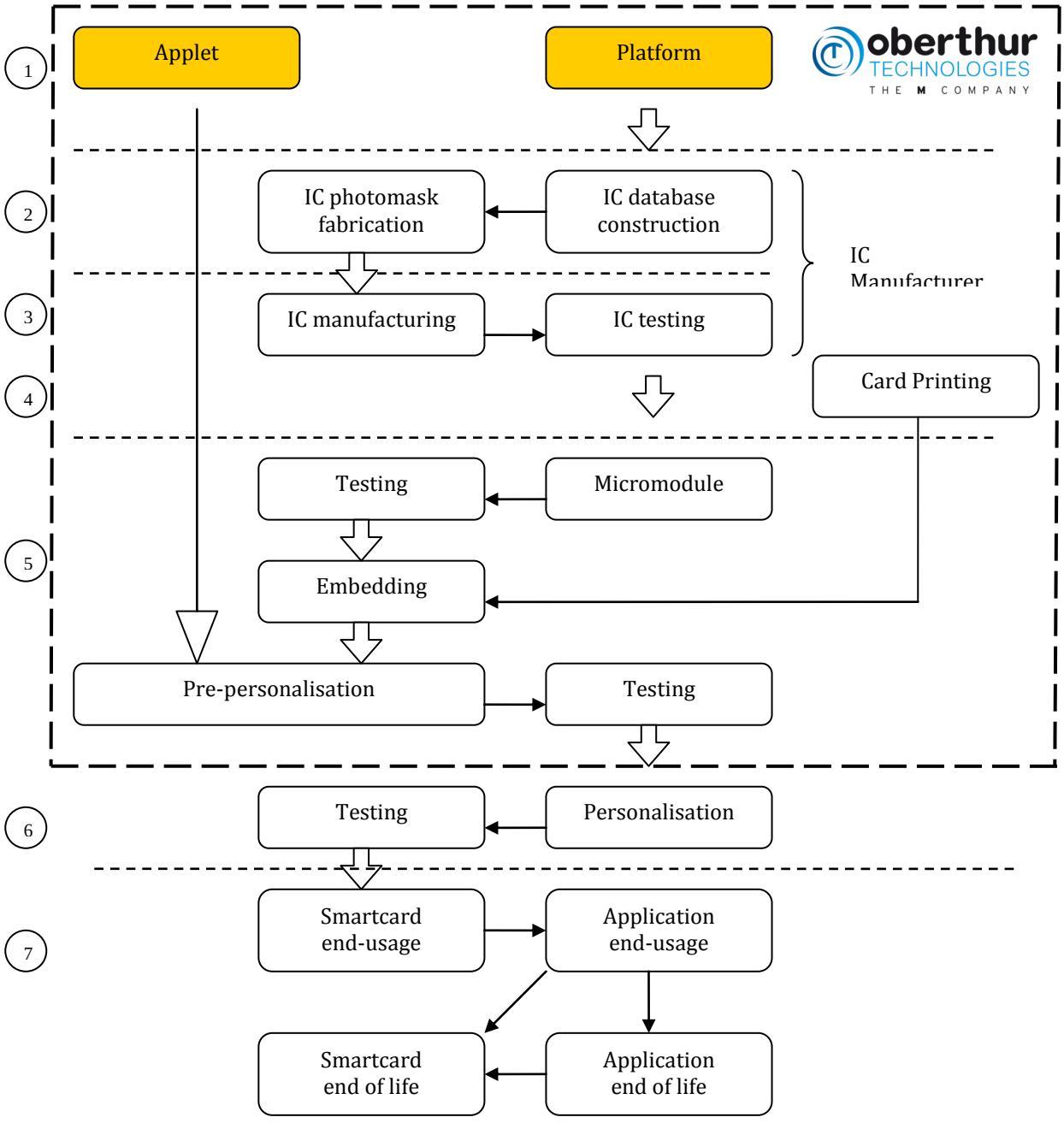
TOE name (commercial name):	ID-One™ CIE v1.0
Guidance document for preparation	FQR 110 6889 Ed 5 FQR 110 7083 Ed 3 FQR 110 7075 Ed 5
Guidance document for operational use	FQR 110 6888 Ed 3

Software identification	078386 for [Applet] 081894 for [PLT]

Name of IC	SLE77CLFX2400P (M7794)
Certificate of the IC	BSI-DSZ-CC-0917-2014

2.4 Life Cycle

With respect to the Life cycle envisioned in [PP0035], seven different phases may be sorted out. The life cycle of the composite TOE may be depicted as follows:



The point of delivery of the TOE is the end of phase 5.
At this moment, the TOE is self protected and constructed.

The point of delivery of the personalisation key used for the authentication of the administrator by the TOE in phase 6 is also the end of phase 5. The personalisation key allows the personalisation of the TOE in phase 6 by the administrator of the phase which the Administrator.

The TOE Life cycle may be splitted in three steps

- Development (phase 1 to 3);
- Production (phase 4 and 5);
- Operational state (phase 6 and 7);

2.4.1 Development

The development of the TOE takes place in phase 1 to 3. In this step, the parts of TOE are designed, tested and manufactured. This step is covered by [ALC] tasks.

2.4.1.1 Software development (phase 1)

This development environment of the Javacard Applet ([Applet]) and javacard platform ([PLT]) is enforced by OBERTHUR TECHNOLOGIES.

The confidentiality and integrity of the code of the Javacard Applet ([Applet]) and javacard platform ([PLT]) is covered by the evaluation of the development premises of OBERTHUR TECHNOLOGIES (ALC class).

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

- Access control to OBERTHUR TECHNOLOGIES offices and sensitive areas.
- Access to development data through the use of a secure computer system to design, implement and test software

2.4.1.2 Hardware development (Phase 2)

In this phase, the underlying integrated circuit is developed by the founder. This phase takes place at the manufacturing site of the founder.

2.4.1.3 IC manufacturing (phase 3)

This phase takes place at the manufacturing site of the founder. During this phase, the manufacturer prepares the IC (loading of data).

In this phase, the code of the javacard platform [PLT] may also be loaded on the IC. In such case, the confidentiality and integrity of the code of the javacard platform [PLT] is covered by the evaluation of the development premises of the founder.

In this phase, the code of the javacard platform [PLT] may also be loaded on the IC, and the [PLT] may contain the code of applet [Applet]. In such case, the confidentiality and integrity of the code is covered by the evaluation of the development premises of the founder.

In any case, at the end of phase 3, IC is self protected.

2.4.2 Production

The production environment encompasses the personalisation of the TOE and the management of the personalisation key.

During this step, the following operations are made:

- The chip is mounted on a physical layout (card, USB token...)
- The code of the javacard platform [PLT] is loaded on the IC (if it has not been made in phase 3). This code may contain the applet bytecode [Applet]
- The applet [Applet] is loaded in [PLT], if not present in the code of the javacard platform [PLT];
- The javacard platform [PLT] is personalised
- The personalisation key is loaded on the TOE
- The applet [Applet] is loaded in [PLT]

- The applet [Applet] is instantiated
- The applet [Applet] is pre-personnalized

This step is covered by [ALC] tasks.

2.4.2.1 IC packaging and initialization (phase 4)

This phase is performed by the Manufacturing Agent, which controls the TOE that is in charge of the packaging and initialization of the IC.

2.4.2.2 TOE pre-personalization (phase 5)

This phase is performed by the Manufacturing Agent, which controls the TOE. The procedures and the IT infrastructure ensure the integrity and authenticity of the keys used to get authenticated with the TOE.

This step is covered by ALC-audits and takes place in one of the following locations:

- Manufacturing site of Vitré (France);
- Manufacturing site of Shenzhen (China);

During this phase, the following operations are performed:

- The code of the javacard platform [PLT] is loaded on the IC (if it has not been made in phase 3). This code may contain the applet bytecode [Applet];
- Pre-personalisation of the javacard platform [PLT];
- Personalisation of the javacard platform [PLT];
- Loading of the code of applet [Applet] in [PLT] if not present in the code of the javacard platform [PLT];
- Loading of the personalisation key in the javacard platform [PLT];
- Create an instance of [Applet];
- Lock the javacard platform [PLT] to prohibit any further applet loading;

The point of delivery of the TOE is the end of this phase.

2.4.3 Operational state

From now on, these steps are covered by AGD.

2.4.3.1 TOE personalisation (phase 6)

The TOE is under the control of the Administrator which in charge of personalising the TOE.

All along this phase, the TOE is self-protected as it requires the authentication of the Administrator prior to any operation.

This phase may not necessarily take place in a manufacturing site, but may be performed anywhere. The Administrator is responsible for ensuring a sufficient level of security during this phase.

The javacard applet [Applet] is personalised according to [AGD_PRE].

2.4.3.2 TOE Usage (phase 7)

The TOE is under the control of the User (Signatory and/or Administrator).

During this phase, the TOE may be used to create a secure signature and manage the SCD, the SVD and the RAD.

2.4.4 Coverage of the different Life cycle state by the assurance components [AGD] & [ALC]

The following phases of the life cycle are covered as follows:

Steps	Life cycle State	TOE: covered by	Personalisation key: covered by
Development	**Phase 1**	**ALC [URANIE]**	**N/A**
	Phase 2	**ALC [IC]**	**N/A**
	Phase 3	**ALC [IC]**	**N/A**
Production	**Phase 4**	**ALC [URANIE]**	**ALC [URANIE]**
	Phase 5	**ALC [URANIE]**	**ALC [URANIE]**
TOE delivery point			
Operational	**Phase 6**	**AGD_PRE [URANIE]**	**N/A**
	TOE is constructed		
	Phase 6	**AGD_PRE [URANIE]**	**N/A**
	Phase 7	**AGD_OPE [URANIE]**	**N/A**

2.4.5 Mapping with the Users

For each of these phases, the following subjects may interact with the TOE

Life cycle phase	Subject interacting with the TOE
Phase 1	OBERTHUR TECHNOLOGIES
Phase 2	OBERTHUR TECHNOLOGIES & IC manufacturer
Phase 3	OBERTHUR TECHNOLOGIES & IC manufacturer
Phase 4	OBERTHUR TECHNOLOGIES
Phase 5	OBERTHUR TECHNOLOGIES
Phase 6	Administrator
TOE is constructed	
Phase 6	Administrator
Phase 7	Users

3 Conformance Claim

3.1 Conformance claim

This security target claims conformance to the Common Criteria version 3.1, revision 4 ([CC31-1], [CC31-2] and [CC31-3]).

The conformance to the Common Criteria is claimed as follows:

CC	Conformance rationale
Part 1	Strict Conformance
Part 2	Conformance to the extended part: - FCS.RNG.1: *"Random number generation"* - FPT_EMSEC.1: *"TOE Emanation"*
Part 3	Conformance to EAL 4, augmented with: - AVA_VAN.5: *"Advanced methodical vulnerability analysis"* - ALC_DVS.2: *"Sufficiency of security measures"*

3.2 Protection Profile

This security target claims a **demonstrable** conformance to the Secure Signature Creation Device (SSCD) Protection Profile [SSCD2] and [SSCD3].

4 Security Problem Definition

4.1 Assets

The assets to be protected by the TOE and its environment within phase 6 and 7 of the TOE's life-cycle are the user data and TSF data defined as follows:

User Data	Property	Definition
SCD	Integrity & confidentiality	Private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).
VAD	-	PIN code entered by the End User. The VAD is submitted by the Signatory to authenticate itself, and MAY also be submitted by the administrator to authenticate itself.
SVD	Integrity	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).
DTBS & DTBS-representation	Integrity	Set of data, or its representation which is intended to be signed (Their integrity must be maintained).

TSF Data	Property	Definition
RAD	Integrity & confidentiality	Reference PIN code used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained). The TOE contains at least one RAD used to authenticate the role Signatory, and MAY contain one or several RAD to authentication the role(s) Administrator.
Keys (secret or public key)	Integrity & confidentiality (only for secret keys)	Keys used to authenticate an external entity. Depending on the authentication protocol, it may be either symmetric (DEs key) or asymmetric key (RSA public portion). In the rest of the document it may also be named authentication key.

4.2 Users

The table below identifies the different users that can interact with the TOE. For each of them, this table indicates:

- The phase in which the user is active
- The matching user in the sense of [SSCD2] and [SSCD3]

Users	Remark	Phases in which it is active	Mapping with [SSCD2] & [SSCD3]	Drawn from [SSCD2]&[SSCD3]?
Signatory	Natural user to which the signature functionality is reserved	6 & 7	User Signatory	Y
Administrator	Phase 6 User in charge of the personalisation in Phase 7 User with administrative right	6 & 7	User Administrator	Y

4.3 Remote IT entity

The table below identifies the different remote IT entities that can interact with the TOE. For each of them, this table indicates the phase in which it is active.

Users	Remark	Phases in which it is active	Drawn from [SSCD2]&[SSCD3]?
SCA	*Signature creation application* This remote IT entity is only present in phase 7	7	Y
CGA	*Certificate Generation Application* In phase 6, this remote IT entity is mingled with the Administrator	6&7	Y
SSCD Type 1	*Secure Signature Creation Device of Type 1* In phase 6, this remote IT entity is mingled with the Administrator	6&7	Y

In this security target those roles are identified as Administrator.

4.4 Assumption

4.4.1 Assumption drawn from [SSCD2] and [SSCD3]

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 and exported

4.4.2 Complementary Assumption

N/A

4.5 Threats

4.5.1 Threats drawn from [SSCD2] and [SSCD3]

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 Signed Data Object 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.

4.5.2 Complementary threats

T.Key_Divulg	*Storing ,copying, and releasing of a the authentication key stored in the TOE*

An attacker can store, copy a secret authentication key stored in the TOE outside the TOE. A secret authentication key is a symmetric key used to authenticate an external entity (remote IT entity of administrator). An attacker can release a secret authentication key during storage or use in the TOE.

T.Key_Derive	*Derive a key*

An attacker derives a secret authentication key from public known data, such as the cryptogram created by means of the key or any other data communicated outside the TOE, which is a threat against the secrecy of the key.

4.6 Organizational security policies

4.6.1 Organizational security policies drawn from [SSCD2] and [SSCD3]

P.CSP_QCert	*Qualified certificate*

The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, 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.

4.6.2 Complementary organizational security policies

P.LinkSCD_Qualified Certificate	*Link between a SCD stored in the TOE and the relevant qualified certificate*

The Subject in charge of creating and updating the SCD (**Administrator**, **Administrator**, **Signatory**), or the remote IT entity involved in the updating process (the **SSCD,** the **CGA)** shall ensure an unambiguous link between the (qualified) certificate(s) and the matching SCD(s). This link might be figured out by a PKCS#15 structures, an XML structure, an identifier .linking the file containing the (qualified) certificate or the URL hosting them to the SCD(s) loaded in the TOE. In particular, it implies this link updated, each time the SCD(s) is created, imported, erased or generated.

P.TOE_Construction	*Construction of the TOE by the Administrator*

The recommendations indicated in [**AGD_PRE**] required to construct the TOE are correctly applied.

4.7 Security Objectives for the TOE

4.7.1 Security objectives of the TOE drawn from [SSCD2] and [SSCD3]

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 authorized 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.

4.7.2 Complementary security objectives of the TOE

OT.Authentication_Secure	*Secure authentication mechanisms*

The TOE provides strong mechanism to authenticate administrator and remote IT entities and also mechanisms to establish a strong trusted channel with a remote IT entity. The authentication protocols rely on cryptographic schemes that are based on symmetric and asymmetric cryptography. The TOE uses freshly generated random number in the external authentication mechanism in order to avoid replay attacks. When using secret key, the authentication protocols ensure that the cryptogram cannot be forged without the knowledge of the secret authentication key, and that it cannot be reconstructed from the authentication cryptograms. The trusted channel established with the remote IT entity ensures integrity, authenticity, and confidentiality (when required) of the data using strong encryption techniques. The trusted channel ensures protection modification of commands. Moreover the TOE ensures the authentication keys it uses are genuine by enforcing an access control over the authentication keys update, in order to ensure that only entitled entities can change key values.

OT.SCD/SVD_Management	*Management of SCD/SVD*

The TOE enables to manage SCD/SVD. Each key (pair) and RAD may be created at any time and used to perform qualified signature during the TOE life time. Several SCD, SVD, and RAD may be present on the TOE and used by the same holder. The TOE guarantees the SCD, SVD and RAD are independent from each other.

OT.Key_Lifecycle_Security	*Lifecycle security of the key(s) stored in the TOE*

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide safe destruction techniques for the authentication keys it stores in case of erasure or re-import.

OT.Key_Secrecy	*Secrecy of the key(s) stored in the TOE*

The secrecy of the secret authentication keys stored in the TOE is reasonably assured against attacks with a high attack potential.

OT.LifeCycle_Management	*Management of the life cycle*

The TOE provides a life cycle management enabling to separate its life cycle in two main phases.
The first one (phase 6) is the one during the TOE prohibits the digital signature creation function. At the end of phase 6, the Administrator switches the TOE in phase 7. This transition is irreversible leaving the TOE under the sole control of the signatory, the administrator (including the SCA, CGA, SSCD) according to the security rules set by the Administrator.

4.8 Security objectives for the Environment

4.8.1 Security objectives of the Environment drawn from [SSCD2] and [SSCD3]

OE.SCD_SVD_Corresp	*Correspondence between SVD and SCD*

The SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSCD 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.

4.8.2 Complementary security objectives of the Environment

OE.LinkSCD_QualifiedCertificate	*Link between a SCD stored in the TOE and the relevant qualified certificate*

The Subject in charge of creating and updating the SCD (**Administrator**, **Signatory**), or the remote IT entity involved in the updating process (the **SSCD,** the **CGA)** shall ensure an unambiguous link between the (qualified) certificate(s) and the matching SCD(s). This link might be figured out by a PKCS#15 structures, an XML structure, an identifier .linking the file containing the (qualified) certificate or the URL hosting them to the SCD(s) loaded in the TOE. In particular, it implies this link is updated, each time the SCD(s) is created, imported, erased or generated.

OE.AuthKey_Transfer	*Secure transfer of Authentication key(s) to the TOE*

The entity in charge of managing the authentication keys to be loaded in the TOE shall ensure

- the confidentiality, integrity and authenticity of the secret key(s) transferred to the TOE;
- The integrity and authenticity of the public key(s) transferred to the TOE;

OE.TOE_Construction	*Construction of the TOE by the Administrator*

The Administrator in charge of administrating the TOE in phase 6 shall be a trusted person and shall be skilled enough to correctly apply the recommendations indicated in [**AGD_PRE**]. These recommendations are required to construct the TOE

5 Extended Requirements

5.1 Extended Families

5.1.1 Extended Family FPT_EMSEC - TOE Emanation

5.1.1.1 Family behaviour

This family defines requirements to mitigate intelligible emanations.

5.1.1.1.1 Extended Components

Extended Component FPT_EMSEC.1

Description

The family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [CC31-2].

Component levelling:

Protection of the TSF and assets requires mitigate information leakage based on emanation.

Audit:

There are no actions defined to be auditable

Management:

There are no management activities foreseen

Hierarchical to:

No other components.

Definition

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

Dependencies: No dependencies.

5.1.2 Extended Family FCS_RNG - FCS_RNG: Random Number Generation

5.1.2.1 Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

5.1.2.1.1 Extended Components

Extended Component FCS_RNG.1

Description

A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs.

Component levelling:

Generation of random numbers requires that random numbers meet a defined quality metric

Audit:

There are no actions defined to be auditable

Management:

There are no management activities foreseen

Hierarchical to:

No other components.

Definition

FCS_RNG.1 Random Number Generation

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic hybrid] random number generator that implements: [assignment: list of security capabilities].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: a defined quality metric].

Dependencies: No dependencies.

6 Security requirements

6.1 Security Functional Requirements

6.1.1 SFR drawn from the Protection Profile

The following SFRs are drawn from [SSCD2] and [SSCD3]. They are sorted out depending on the life cycle of the TOE.

6.1.1.1 Phase 6 and 7

This chapter contains SFRs drawn for [SSCD2] and [SSCD3] that apply in both phase 6 and 7 of the life cycle.

6.1.1.1.1 FCS_CKM.1 Cryptographic key generation

FCS CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***assignment: cryptographic key generation algorithm***] and specified cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the [***assignment: list of standards***]

Assignment:

Cryptographic key generation algorithm	*Cryptographic key sizes*	*List of standards*
RSA key generation	1536 - 2048 bits	[ANSI X9.31]

6.1.1.1.2 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1

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: [***none***].

6.1.1.1.3 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 [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the following: [***assignment: list of standards***].

Assignment:

Cryptographic algorithm	Cryptographic key sizes	List of standards
PKCS #1 V1.5 Block Type 1	1024 bits or 1536 bits or 2048 bits	[PKCS#1]

6.1.1.1.4 FDP_ACC.1 Access Control Policy

FDP_ACC.1.1/SVD transfer SFP

The TSF shall enforce the [***SVD transfer SFP***] on [***import and export of SVD by User***].

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/Personalisation SFP

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

FDP_ACC.1.1/SCD Import SFP

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

6.1.1.1.5 FDP_ACF.1 Security attribute based access control

6.1.1.1.5.1 SVD transfer SFP

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

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 "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: [***none***]

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

6.1.1.1.5.2 Initialisation SFP

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

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 following additional rules:[***the user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security***

attribute "SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.]

6.1.1.1.5.3 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: [***none***]

FDP_ACF.1.4/SCD Import SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
(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".***]

6.1.1.1.5.4 Personalisation SFP

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

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***]

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 following additional rules: [***none***]

6.1.1.1.6 FDP_ETC.1: Export to outside TSF control

6.1.1.1.6.1 SVD Transfer

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 TOE.

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

6.1.1.1.7 FDP_ITC.1 Import from outside TSF control

6.1.1.1.7.1 SCD Import

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 TOE.

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

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

6.1.1.1.8 FDP_RIP.1 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: [***keys, SCD, VAD, and RAD***].

6.1.1.1.9 FDP_SDI.2 Stored data integrity

6.1.1.1.9.1 Persistent data

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

- SCD
- RAD
- SVD
- Keys

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

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

6.1.1.1.10 FDP_UCT.1 Inter-TSF user data confidentiality transfer protection

6.1.1.1.10.1 SCD Import

FDP_UCT.1.1/Receiver

The TSF shall enforce the [***SCD Import SFP***] to [***receive***] user data in a manner protected from unauthorised disclosure.

6.1.1.1.11 FDP_UIT.1 Inter-TSF user data integrity transfer protection

6.1.1.1.11.1 SVD transfer

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

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

6.1.1.1.12 FIA_AFL.1 Authentication failure

FIA AFL.1.1
The TSF shall detect when [***an administrative configurable positive integer within 1 and 15***] 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***].

6.1.1.1.13 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***]

6.1.1.1.14 FIA_UAU.1 User 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.1/SCD import***]
[***Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE to transmit the VAD***]
[***Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import in phase 7***]
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.

6.1.1.1.15 FIA_UID.1 User 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 to transmit the VAD***]
[***Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import in phase 7***]
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.

6.1.1.1.16 FMT_MSA 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***].

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 and secure SCD import allowed***] to [***Administrator***].

FMT_MSA.2.1
The TSF shall ensure that only secure values are accepted for [***SCD/SVD management, SCD operational, Key import management***].

FMT_MSA.3.1
The TSF shall enforce the [***Initialisation SFP, Signature-creation SFP, SCD Import, SFP, Key Management SFP***] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

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

6.1.1.1.17 FMT_SMR.1 Security management roles

FMT_SMR.1.1
The TSF shall maintain the roles [“***Administrator”, “Signatory”***].

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

6.1.1.1.18 FPT_EMSEC.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, SCD, keys and TSF data***] and [***none***].

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, SCD, keys and TSF data***] and [***none***].

6.1.1.1.19 FPT_FLS.1 Failure secure

FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [
Card reset or tearing,
Applet code inconsistency,
Applet lifecycle inconsistency,
Unavailability of resources,
Array overflow,
Integrity error detected on RAD, SCD, and keys
Failure detected by the underlying IC through FPT_FLS.1 (refer to the security target of the IC)].

6.1.1.1.20 FPT_PHP TSF physical Protection

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.3.1
The TSF shall resist [***physical manipulation and physical probing***] to the [***all TOE components implementing the TSF***] by responding automatically such that the SFRs are always enforced

6.1.1.1.21 FPT_TST.1 TSF self test

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

6.1.1.1.22 FTP_ITC.1 Inter-TSF trusted channel

6.1.1.1.22.1 SCD Import

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

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

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

6.1.1.1.22.2 SVD Transfer

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

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

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

6.1.1.1.23 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***].

6.1.1.2 Phase 7

This chapter contains SFRs drawn for [SSCD2] and [SSCD3] that apply in 7 of the life cycle.

6.1.1.2.1 FCS_COP.1 Cryptographic operation

FCS_COP.1.1/SIGNING

The TSF shall perform [***Digital signature-generation***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the following: [***assignment: list of standards***].

Assignment:

Cryptographic algorithm	Cryptographic key sizes	List of standards
PKCS #1 V1.5 Block Type 1	1024 bits or 1536 bits or 2048 bits	[PKCS#1]

6.1.1.2.2 FDP_ACC.1 Access Control Policy

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

6.1.1.2.3 FDP_ACF.1 Security attribute based access control

6.1.1.2.3.1 Signature Creation SFP

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

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

FDP ACF.1.3/Signature-creation SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]

FDP_ACF.1.4/Signature-creation SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
(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".]***

6.1.1.2.4 FDP_ITC.1 Import from outside TSF control

6.1.1.2.4.1 DTBS import

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 TOE.

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

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

6.1.1.2.5 FDP_SDI.2 Stored data integrity

6.1.1.2.5.1 DTBS-representation

The Protection Profiles [SSCD2] and [SSCD3] specify that the DTBS representation temporarily stored by TOE have the user data attribute "integrity checked stored data".

FDP_SDI.2.1/DTBS The TSF shall monitor user data stored in containers controlled by the TSF for [***integrity error***] on all objects, based on the following attributes: [***integrity checked stored data***].

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

6.1.1.2.6 FDP_UIT.1 Inter-TSF user data integrity transfer protection

6.1.1.2.6.1 DTBS transfer

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

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

6.1.1.2.7 FMT_MSA.1 Management of security attributes

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***].

6.1.1.2.8 FMT_MTD.1 Management of TSF data

6.1.1.2.8.1 Signatory

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

6.1.1.2.9 FMT_MOF.1 Management of functions in TSF

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

6.1.1.2.10 FTP_ITC.1 Inter-TSF trusted channel

6.1.1.2.10.1 DTBS Import

FTP_ITC.1.1/DTBS import

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

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

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

6.1.2 Additional SFRs

6.1.2.1 Phase 6

6.1.2.1.1 FMT_MTD.1 Management of TSF data

6.1.2.1.1.1 TOE State

FMT_MTD.1.1/TOE State
The TSF shall restrict the ability to [***switch***] the [***TOE from phase 6 to phase 7***] to [***Administrator***].

6.1.2.1.1.2 Administrator

FMT_MTD.1.1/Admin
The TSF shall restrict the ability to [***create***] the [***container of RAD, SCD, SVD and keys***] to [***Administrator***].

6.1.2.2 Phase 7

6.1.2.2.1 FMT_MTD.1 Management of TSF data

6.1.2.2.1.1 Association between SCD and SCD_ID

FMT_MTD.1.1/Association between SCD and SCD_ID
The TSF shall restrict the ability to [***select***] the [***SCD using a SCD_ID***] to [***Any User***].

6.1.2.3 Phase 6&7

6.1.2.3.1 FCS_COP.1 Cryptographic operation

FCS_COP.1.1/External Authentication

The TSF shall perform [***External Authentication***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic algorithm***] that meet the following: [***assignment: list of standards***].

Assignment:

Cryptographic algorithm	Cryptographic key sizes	List of standards
Encryption using Triple DES EDE in mode CBC Signature using Retail MAC	112 bits	[CIE]
RSA authentication	Maximum size of 2048 bits	[PKCS#1]

FCS_COP.1.1/Secure Messaging in Confidentiality

The TSF shall perform [***Secure Messaging in confidentiality***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the following: [***assignment: list of standards***].

Assignment:

Cryptographic algorithm	Cryptographic key sizes	List of standards
Encryption with Triple DES EDE in CBC mode	128 bits	[11568-2]

FCS_COP.1.1/Secure Messaging in Integrity

The TSF shall perform [***Secure Messaging in integrity and authenticity***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the following: [***assignment: list of standards***].

Assignment:

Cryptographic algorithm	Cryptographic key sizes	List of standards
Retail MAC MAC algorithm 3 with padding method 2 and DES bloc Cipher	112 bits	[9797-1]

6.1.2.3.2 FCS_RNG.1 Random Number Generation

FCS_RNG.1/Random Number Generation

FCS_RNG.1.1
The TSF shall provide a [***hybrid***] random number generator that implements: [***test supported by the underlying IC through FCS_RNG.1 (refer to the security target of the IC)***].

FCS_RNG.1.2
The TSF shall provide random numbers that meet [***FIPS 140-2***].

6.1.2.3.3 FDP_ACC.1 Access Control Policy

FDP_ACC.1.1/Key Management SFP

The TSF shall enforce the [***Key Management SFP***] on [***Import of key by the User***]

6.1.2.3.4 FDP_ACF.1 Security attribute based access control

6.1.2.3.4.1 Key Management SFP

FDP_ACF.1.1/Key Management SFP
The TSF shall enforce the [***Key Management SFP***] to objects based on [***Key Management group***].

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

(a) [***the user with the security attribute "role" set to "Signatory", "Administrator" and with the security attribute "Key import Management" set to "authorised" is allowed to import key]***

(b) [***if the import, is set to Never, any user will not be allowed to perform the operation***]

FDP ACF.1.3/Key Management SFP

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

FDP_ACF.1.4/Key Management SFP

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

6.1.2.3.5 FDP_ITC.1 Import from outside TSF control

6.1.2.3.5.1 Keys import

FDP_ITC.1.1/Keys

The TSF shall enforce the [***Key Management SFP***] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/Keys

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

FDP_ITC.1.3/Keys

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [***Keys shall be sent by the User with the "role" set to "Signatory", "Administrator", "SCA", "CGA", or "SSCD type 1"***].

6.1.2.3.6 FIA_AFL.1 Authentication failure

FIA_AFL apply to the authentication mechanisms based on cryptographic keys. The following authentication mechanisms are concerned:

- Authentication of the role "Administrator"
- Authentication of the remote IT entities "SCA", "CGA", "SSCD type 1"

FIA AFL.1.1/Authentication keys
The TSF shall detect when [***selection:[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]***] unsuccessful authentication attempts occur related to [***consecutive failed authentication attempts***].

FIA AFL.1.2/Authentication keys
When the defined number of unsuccessful authentication attempts has been [***met or surpassed***], the TSF shall [***assignment: list of actions***].

Assignment:

Type of entity	Entity	Selection for FIA_AFL.1.1	List of actions
User	"Administrator"	***Administrator configurable positive integer 'N'*** ***0 ≤N ≤15***	***If N= '0', no actions are taken*** ***If N != '0', the key is blocked***
User Or Remote IT entity	"SCA", "CGA", "SSCD type 1"	***Administrator configurable positive integer 'N'*** ***0 ≤N ≤15***	***If N= '0', no actions are taken*** ***If N != '0', the key is blocked***

6.1.2.3.7 FIA_ATD.1 User attribute definition

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

6.1.2.3.8 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1/Key Management
The TSF shall enforce the [***Key Management SFP***] to restrict the ability to [***modify***] the security attributes [***Key import management***] to [***Administrator***].

6.1.2.3.9 FMT_MTD.1 Management of TSF data

6.1.2.3.9.1 Unblocking of RAD and keys

FMT_MTD.1.1/Unblock
The TSF shall restrict the ability to [***unblock***] the [***RAD or keys***] to [***Administrator***].

6.1.2.3.10 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: [
(a) ***Creation and modification of RAD;***
(b) ***Enabling the signature creation function;***
(c) ***Modification of the security attribute SCD/SVD management, SCD operational, secure SCD import allowed***
(d) ***Modification of the security attribute Key import management***
(e) ***Unblocking of RAD and keys;***
(f) ***Switching from phase 6 to phase 7;***
(g) ***Creating container of RAD, SCD, SVD and keys;***
(h) ***Selecting SCD;***].

6.2 Security Assurance Requirements

This chapter defines the list of the assurance measures required for the TOE security assurance requirements. The EAL5+ is claimed.

6.2.1 Evaluation Assurance Level rationale

The following assurance packages are required:

Measures	Name
ADV	Development
AGD	Guidance
ALC	Life Cycle
ASE	Security target
ATE	Tests
AVA	Vulnerability

6.2.1.1 ADV: Development

The following components are included:

Measures	Level
ADV_ARC	1
ADV_FSP	4
ADV_IMP	1
ADV_INT	N/A
ADV_SPM	N/A
ADV_TDS	3

6.2.1.2 AGD: Guidance

The following components are included:

Measures	Level
AGD_OPE	1
AGD_PRE	1

6.2.1.3 ALC: Life cycle

The following components are included:

Measures	Level
ALC_CMC	4
ALC_CMS	4
ALC_DEL	1
ALC_DVS	2 - augmented
ALC_FLR	N/A
ALC_LCD	1
ALC_TAT	1

6.2.1.4 ASE: Security target

The following components are included:

Measures	Level
ASE_CCL	1
ASE_ECD	1
ASE_INT	1
ASE_OBJ	2
ASE_REQ	2
ASE_SPD	1
ASE_TSS	1

6.2.1.5 ATE: Tests

The following components are included:

Measures	Level
ATE_COV	2
ATE_DPT	1
ATE_FUN	1
ATE_IND	2

6.2.1.6 AVA: Vulnerability

The following components are included:

Measures	Level
AVA_VAN	5 - augmented

6.2.2 Rationale for augmentation

6.2.2.1 AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component. Independent vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication.

All the dependencies of AVA_VAN.5, listed below are fulfilled:

- ADV_ARC.1
- ADV_FSP.4
- ADV_TDS.3
- ADV_IMP.1
- AGD_OPE.1
- AGD_PRE.1
- ATE_DPT.1

6.2.2.2 ALC_DVS.2 Sufficiency of security measures

In order to protect the TOE on development Phase, the component ALC_DVS.2 was added. This latter requires security documentation justifying that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_DVS.2 does not have any dependencies.

7 TOE Summary Specification

7.1 Description

The TOE inherits all the security functions provided by the underlying integrated circuit (see the Security target). On top of these, it adds some supplemental security functions that are described hereafter.

SF.RAD_MGT

This security function is involved in the management of the RAD. It ensures the link between each RAD(s) and its associated role (Signatory and Administrator).

SF.SIG

This security function manages the signature creation service.

SF.ADM_AUTH

This security function manages the authentication of external entities by the TOE using a challenge/response protocol. It allows the authentication of the Administrator.

SF.SM

This security function ensures the establishment of a trusted channel with a remote IT entity and the protection of communication between the TOE and this external entity. As such, this security function establishs and maintains a trusted channel.

SF.KEY_MGT

This security function is involved in the management of the keys (the authentication keys, the SCDs and the SVDs).

SF.CONF

This security function manages the configuration of the TOE.

SF.SAFESTATE_MGT

This security function ensures the TOE is always in a safe state. It monitors the integrity of the TOE, its assets and the TSF data (RAD, keys, DTBS) by performing selftests. When an unexpected event occurs (loss of power, loss of integrity, tearing, event detected by the underlying IC,…), it ensures

- the TOE returns in a safe state
- all sensitive data are erased
- the TOE returns in a restrictive secure state

SF.PHYS

This security function ensures the protection of the TOE against physical manipulation aiming at getting access to its assets.