Touch&Sign2048 V1.00 - Security Target

BSI-DSZ-CC-0422

1 Revisions and Approvals

Edition	Rev.	Subject	Issued by:	Authorized by:	Date
A-3			S. Donatiello		29-Mar-2007

1.1. Copyright Notification

At the time of going to press, this paper is as thorough and correct as possible. However, information herein contained may have been updated without prior notice after this date. **ST Incard Srl** reserves the right to change the functions of its products any time without prior notice.

2 Table Of Content

1 REVISIONS AND APPROVALS 2

1.1. COPYRIGHT NOTIFICATION 2

2 TABLE OF CONTENT 3

3 LIST OF TABLE 5

4 LIST OF FIGURE 6

5 GLOSSARY 7

6 REFERENCES 10

7 CONVENTIONS 12

8 ST INTRODUCTION 13

8.1. ST IDENTIFICATION 13
8.2. ST OVERVIEW 13
8.3. CC CONFORMANCE CLAIM 14

9 TOE DESCRIPTION 15

9.1. PRODUCT TYPE 15
9.2. TOE FUNCTIONALITIES 15
9.3. TOE LIFE CYCLE 17
9.4. USER AND ADMINISTRATOR GUIDANCE 18
9.5. TOE ENVIRONMENT 18
9.5.1. Development and Production Environment 18

10 TOE SECURITY ENVIRONMENT 20

10.1. ASSETS 20
10.2. SUBJECTS 20
10.3. THREAT AGENTS 21
10.4. SECURE USAGE ASSUMPTIONS 21
10.5. ORGANIZATIONAL SECURITY POLICIES 21
10.6. THREATS TO SECURITY 22

11 SECURITY OBJECTIVES 23

11.1. SECURITY OBJECTIVES FOR THE TOE 23
11.2. SECURITY OBJECTIVES FOR THE ENVIRONMENT 24
11.2.1. Additional security objective for the non-IT environment 24

12 IT SECURITY REQUIREMENTS 25

12.1. TOE SECURITY FUNCTIONAL REQUIREMENTS 25
12.2. TOE SECURITY ASSURANCE REQUIREMENTS 32
12.3. IT ENVIRONMENT SECURITY REQUIREMENTS 33
12.3.4. Non-IT Environment Security requirements 34

13 TOE SUMMARY SPECIFICATION 35

13.1. TOE SECURITY FUNCTIONS 36
13.1.1. Identification and authentication 36
13.1.2. Access Control 38
13.1.3. Key Management and Cryptography 39
13.1.4. Secure Messaging 41
13.1.5. Stored Data Protection 41
13.1.6. Test 43
13.1.7. Failure 43

13.1.8. TOE Life Cycle ... 44
13.1.9. TOE HARDWARE ... 44
13.2. ASSURANCE MEASURES ... 45

14 SSCD PP CLAIMS ... 46

14.1. PP REFERENCE ... 46
14.2. PP TAILORING ... 46
14.3. PP ADDITIONS ... 46

15 RATIONALE ... 47

15.1. SECURITY OBJECTIVES RATIONALE ... 47
15.1.1. Security Objectives Coverage. ... 47
15.1.2. Security Objectives Sufficiency. ... 47
15.1.2.2. Additional assumptions and Security Objective Sufficiency ... 48
15.2. SECURITY REQUIREMENTS RATIONALE ... 48
15.2.1. Security Requirements coverage ... 48
15.2.2. TOE Security Requirements sufficiency ... 49
15.2.3. Rationale for extensions ... 49
15.2.4. Assurance Requirements Suitability ... 49
15.3. TOE SUMMARY SPECIFICATION RATIONALE ... 52
15.3.2. TOE Security Functions rationale ... 53
15.4. TOE STRENGTH OF FUNCTION CLAIM ... 74
15.5. PP CLAIMS RATIONALE ... 74
15.6. FUNCTIONAL REQUIREMENTS DEPENDENCIES ... 74

3 List of Table

Table 1: Operation performed on TOE SFRs 25
Table 2: Assurance Requirements - EAL 4 extended with AVA_MSU.3 and AVA_VLA.4 32
Table 3: Operation performed on ENVIRONMENT SFRs 33
Table 4: List of TOE security functions 36
Table 5: Threats, Assumptions and Policy to Security objective mapping 47
Table 6: Assurance Measures assignment 51
Table 7: Functional requirements and TOE security function rational 71
Table 8: Functional requirements to TOE security functions mapping 72
Table 9: Functional requirements to TOE security functions mapping (continued) 73

4 List of Figure

Figure 1: TOE boundaries 15
Figure 2: TOE components........ 16
Figure 3: TOE life cycle 17

5 Glossary

This section gives definitions and explanations related to frequently used terms and acronyms.

TERM	DEFINITION
Administrator	Means an user that performs TOE initialization, TOE personalization, or other TOE administrative functions
Advanced electronic signature	(Defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements: a) it is uniquely linked to the signatory; b) it is capable of identifying the signatory; c) it is created using means that the signatory can maintain under his sole control, and d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Authentication data	The information used to verify the claimed identity of a user.
Authorized user	A user who may, in accordance with the TSP, perform an operation.
Card manufacturer	ST Incard Srl
Certificate	Means an electronic attestation, which links the SVD to a person and confirms the identity of that person. (Defined in the Directive [1], article 2.9)
Certificate Generation Application (CGA)	Means a collection of application elements, which requests the SVD from the SSCD for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair by the SSCD, if the requested SVD has not been generated by the SSCD yet. The CGA verifies the authenticity of the SVD by means of a) the SSCD proof of correspondence between SCD and SVD and b) checking the sender and integrity of the received SVD.
Certification-service-provider (CSP)	An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.
Chip Manufacturer	ST Microelectronics Spa.
Data to be signed (DTBS)	Means the complete electronic data to be signed (including both user message and signature attributes).
Data to be signed representation (DTBSR)	Means the data sent by the SCA to the TOE for signing and is a) a hash-value of the DTBS or b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or c) the DTBS. The SCA indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.
Directive	The Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] is also referred to as the ‘Directive’ in the remainder of the Security Target.
Local User	User using the trusted path provided between the SCA in the TOE environment and the TOE.
Netlink	Interoperable health card scheme defined by G8 group
PERSO_MODE flag	Flag used to control TOE state transition. Default configuration value for PERSO_MODE flag is set equal to PERSONALIZATION in order to force the TOE in *SC personalization* state at the beginning of TOE Operational phase.

TERM (CONT.)	DEFINITION
Personal Identification Number (PIN)	Value transmitted from the smartcard reader to Touch&Sign2048 V1.00 and used for signatory's authentication.
Qualified certificate	Means a certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive (defined in the Directive, article 2.10), here reported: Qualified certificates must contain: (a) an indication that the certificate is issued as a qualified certificate; (b) the identification of the certification-service-provider and the State in which it is established; (c) the name of the signatory or a pseudonym, which shall be identified as such; (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended; (e) signature-verification data which correspond to signature-creation data under the control of the signatory; (f) an indication of the beginning and end of the period of validity of the certificate; (g) the identity code of the certificate; (h) the advanced electronic signature of the certification-service-provider issuing it; (i) limitations on the scope of use of the certificate, if applicable; and (j) limits on the value of transactions for which the certificate can be used, if applicable.
Reference Authentication Data (RAD)	Means data persistently stored by the TOE for verification of the authentication attempt as authorized user.
Secure Signature Creation Device (SSCD or the TOE described in this Security Target)	Means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex Touch&Sign2048 V1.00 of the Directive [1]. (SSCD is defined in the Directive [1], article 2.5 and 2.6).
Signatory	Means a person who holds a SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. (Defined in the Directive [1], article 2.3).
Signature Creation Application (SCA)	Means the application used to create an electronic signature, excluding the SSCD, i.e., the SCA is a collection of application elements a) to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision, b) to send a DTBS-representation to the TOE, if the signatory indicates by specific unambiguous input or action the intend to sign, c) to attach the qualified electronic signature generated by the TOE to the data or provides the qualified electronic signature as separate data.
Signature Creation Data (SCD)	Means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. (Defined in the Directive [1], article 2.4).
Signature Verification Data (SVD)	Means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (Defined in the Directive[1], article 2.7)
Signed Data Object (SDO)	Means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.
SSCD PP	Secure Signature Creation Device Protection Profile [6]
ST ROM	ST Microelectronics ROM code running in ISSUER MODE, i.e. when the smartcard is delivered to the card manufacturer
Verification Authentication Data (VAD)	Means authentication data provided as input by knowledge. For Touch&Sign2048 V1.00 this is synonym of PIN.

ACRONYMS	DEFINITION
AC	Access Conditions
BSO	Base Security Object
CC	Common Criteria
CGA	Certificate Generation Application
CRT	Chinese Remainder Theorem
CSP	Certification Service Provider
DF	Directory file
DTBS	Data to be signed
DTBSR	Data to be signed representation
EAL	Evaluation Assurance Level
HPC	Health Professional Card
IC	Integrated Circuit
IFD	Interface Device, i.e. the smartcard reader
IT	Information Technology
MAC	Message Authentication Code
MAP	Modular Arithmetic Processor
MUT_{KEY}	Cryptographic key used for mutual authentication between the TOE and an external application/device
OS	Operating System
PP9806	Protection Profile [7]
RAD	Reference Authentication Data
RAD_A	Reference Authentication Data stored by the TOE and used to verify the claimed identity of the administrator
RAD_S	Reference Authentication Data stored by the TOE and used to verify the claimed identity of the signatory
SC	Smartcard
SCA	Signature Creation Application
SCD	Signature Creation Data
SDO	Signed Data Object
SF	Security Function
SFP	Security Function Policy
SM	Secure Messaging
SOF	Strength of Function
SSCD (the TOE)	Secure Signature Creation Device
SSCD PP	Protection Profile [6]
ST	Security Target
STM	STMicroelectronics
SVD	Signature Verification Data
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VAD	Verification Authentication Data

6 References

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

[2] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 - Part 1: Introduction and general model, CCIMB-2005-08-001

[3] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 - Part 2: Security functional requirements, CCIMB-2005-08-002

[4] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 - Part 3: Security assurance requirements, CCIMB-2005-08-003

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

[6] CWA 14169 - Annex C Protection Profile-Secure Signature - Creation Device Type 3, version: 1.05, EAL4+, March 2002 (BSI-PP-0006-2002 EAL 4+).

[7] Protection Profile PP9806 -Smartcard - Integrated Circuit, version: 2.0, EAL4+, September 1998.

[8] CWA 14355- Guidelines for the implementation of Secure Signature - Creation Devices version 0.91, Dec 17, 2001.

[9] ST Microelectronics, ST19WR66 Security Target, SMD_ST19WR66_ST_05_001_V01.02

[10] DCSSI DCSSI ST19WR66I Microcontroller – Certification Report 2006/18

[11] ISO/IEC 7816
Part 3 Signal and transmission protocols
Second Edition 1997
Part 4 Interindustry commands for interchange
Second Edition 2005
Part 5 Numbering System and registration procedure for application identifiers
First Edition 1994
Part 8 Security related interindustry commands
Edition 1998
Part 9 Additional interindustry commands and security attributes
First Edition 2001

[12] ISO/IEC 14443-2 Identification Cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal – 2001-07-1

[13] ISO/IEC 14443-3 Identification cards – Contactless integrated circuit(s) card – Proximity cards – Part 3: Initialization and anticollision First edition 2001-02-01

[14] ISO/IEC 14443-4 Identification Card – Contactless integrated circuit card – Proximity card – part 4 – Transmission Protocol – 1/02/2001

[15] ISO/IEC 14888-3 Information technology - Security techniques - Digital signatures with appendix - Part 3 : Certificate-based mechanisms 15-12-1999

[16] ISO/IEC 9797-1 Information technology - Security techniques – Message Authentication Codes (MACs) - Part 1 : Mechanisms using a block cipher - First Edition 15-12-1999

[17] FIPS 113: Computer Data Authentication (FIPS PUB 113), NIST, 30 May 1985

[18] FIPS 140-2: Security Requirements for Cryptographic Modules (FIPS PUB 140-2), NIST, 1999

[19] BSI-AIS31: A proposal for functionality classes and evaluation methodology for true (physical) random number generators. W. Killmann,, W. Schindler BSI Ver.3.1 25.09.2001

[20] FIPS 180-1: Secure Hash Standard (FIPS PUB 180-1), NIST, 17 April 1995

[21] FIPS 180-2: Secure Hash Standard 1 August 2002

[22] PKCS #1 v1.5: RSA Encryption Standard – RSA Laboratories – 1 Nov 1993

[23] FIPS PUB 46-3: Data Encryption Standard – 5 Oct 1999

[24] NETLINK – Requirements for Interoperability – Ref. NK/2/ZI/A/3/2.2.1 – Ver.2.2.1 – 24 Nov 2000

[25] ST19WR66 Data Sheet – DS_19WR66/0507 V1 August 2005

[26] ST19X Cryptographic Library LIB4 V2.0 – User Manual UM_19X_LIB4V2/0503V2

[27] ST19X E-DES Enhanced DES Library - User Manual - UM_19XV2_EDESLIB/0203V1.1

[28] ST19W AES library – User Manual – UM_19W_AES/0304VP1

[29] ST19X-19W Security application manual – APM_19X-19W_SECU/0312V1.7

[30] ST19X-19W Security application manual – Addendum to V1.7 AD_APM_19X-19W_SECUV1.7/0405V4

[31] ST19X-19W Security application manual – Addendum-2 to V1.7 AD2_APM_19X-19W_SECUV1.7/0407V1

[32] Published in Federal Gazette No 58, pp 1913-1915 of 23 March 2006 - Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway - Notification in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance of 2 January 2006 (overview of suitable algorithms)

7 Conventions

The document follows the rules and conventions laid out in Common Criteria 2.3 [2], Annex B “Specification of Security Targets”.
As stated in § 7, this Security Target is compliant to Protection Profile [6], which in the following will be referred to as [SSCD PP].
Admissible algorithms and parameters for algorithms for secure signature-creation devices referred hereafter are derived from document [5].

8 ST Introduction

8.1. ST Identification

[1] Here are the labeling and descriptive information necessary to control and identify the ST and the TOE to which it refers.

Title:	Touch&Sign2048 V1.00 - Security Target
Assurance Level:	EAL 4 augmented with AVA_MSU.3 and AVA_VLA.4.
Strength of Functions:	SOF High
Authors:	Saverio Donatiello (ST Incard srl)
CC Version:	2.3 [2],[3],[4]
PP Conformance:	SSCD Protection Profile Type 3 [SSCD PP] [6].
Version:	A-3
General Status:	Final
Related ST:	ST19WR66 Security Target [9].

8.2. ST Overview

[2] This document provides a complete and consistent statement of the security enforcing functions and mechanisms of Touch&Sign2048 V1.00 device (hereafter referred to as the TOE, i.e. the Target of Evaluation).

[3] The Security Target details the TOE security requirements and the countermeasures proposed to address the perceived threats to the assets protected by the TOE.

[4] Touch&Sign2048 V1.00 is a multifunctional smartcard product implementing a type 3 Secure Signature-Creation Device as described in [SSCD PP] [6] § 2.1.

[5] Main Touch&Sign2048 V1.00 functionalities cover following areas

- Cryptographic key generation and secure management
- Secure signature generation with secure management of data to be signed
- Identification and Authentication of trusted users and applications
- Data storage and protection from modification or disclosures, as needed
- Secure exchange of sensitive data between the TOE and a trusted applications
- Secure exchange of sensitive data between the TOE and a trusted human interface device

[6] Touch&Sign2048 V1.00 was developed on a STMicroelectronics microcontroller: ST19WR66I ICC, a hardware platform offering 224Kb ROM, 6Kb RAM, 66Kb of EEPROM and cryptographic support, especially designed for secure application based on high performance Public and Secret key algorithms (i.e. RSA, DES, TripleDES, AES-128). The chip includes a Modular Arithmetic Processor (MAP), based on an 1088-bit processor architecture, and a DES accelerator, both designed to speed up cryptographic calculations. The hardware also includes a true random number generator (TRNG) compliant to both [18] and P2 class of [19]. Furthermore the hardware also includes two external interfaces for I/O transmissions; one contact interface ISO/IEC 7816 compliant and one contactless interface ISO/IEC 14443 compliant.

[7] HW platform has been certified under the French Scheme (see [10], ST19WR66I Certification Report) and it is compliant with PP9806 Protection Profile for smartcard integrated circuit [7]. Therefore references are made in this document to ST19WR66 Security Target [9].

8.3. CC conformance claim

[8] This ST is conformant with Common Criteria (CC) Version 2.3 Part 1[2].

This ST is conformant with Common Criteria (CC) Version 2.3 Part 2 (ISO/IEC 15408:2005 Evaluation Criteria for Information Technology Security; Part 2: Security functional requirements [1]) with extension “FPT_EMSEC.1” made in the SSCD Protection Profile [SSCD PP] [6].

This ST is conformant with Common Criteria (CC) Version 2.3 Part 3 (ISO/IEC 15408:2005 Evaluation Criteria for Information Technology Security; Part 3: Security Assurance Requirements [4]) based only on CC Part 3 assurance components.

This ST is compliant with the SSCD Protection Profile [SSCD PP] [6].

The TOE assurance level claim is EAL 4 augmented with AVA_MSU.3 and AVA_VLA.4.

The TOE meets the SSCD Type 3 Protection Profile [SSCD PP] [6].

The TOE is conformant with Common Criteria Version 2.3, with part 2 and part 3 augmented as stated in [SSCD PP] [6].

The minimum strength of function level for the SFR is SOF-high.

9 TOE Description

[9] This part of the ST describes the TOE as an aid to the understanding of its security requirements, and addresses the product. The scope and boundaries of the TOE are described in general terms both in a physical way (hardware and/or software components/modules) and a logical way (IT and security features offered by the TOE).

9.1. Product type

[10] The Target Of Evaluation (TOE) is the Secure Signature Creation Device (SSCD) defined by:

- The SSCD Application Touch&Sign2048 V1.00
- The devices drivers Touch&Sign2048 V1.00
- The Integrated Circuit and its libraries ST19WR66I
- User and Administrator guidance

9.2. TOE functionalities

[11] Touch&Sign2048 V1.00 multifunctional smartcard product is intended to provide all capabilities required to devices involved in creating qualified electronic signatures (see next figure to identify main TOE functional components and interfaces with TOE environment and TOE boundaries):

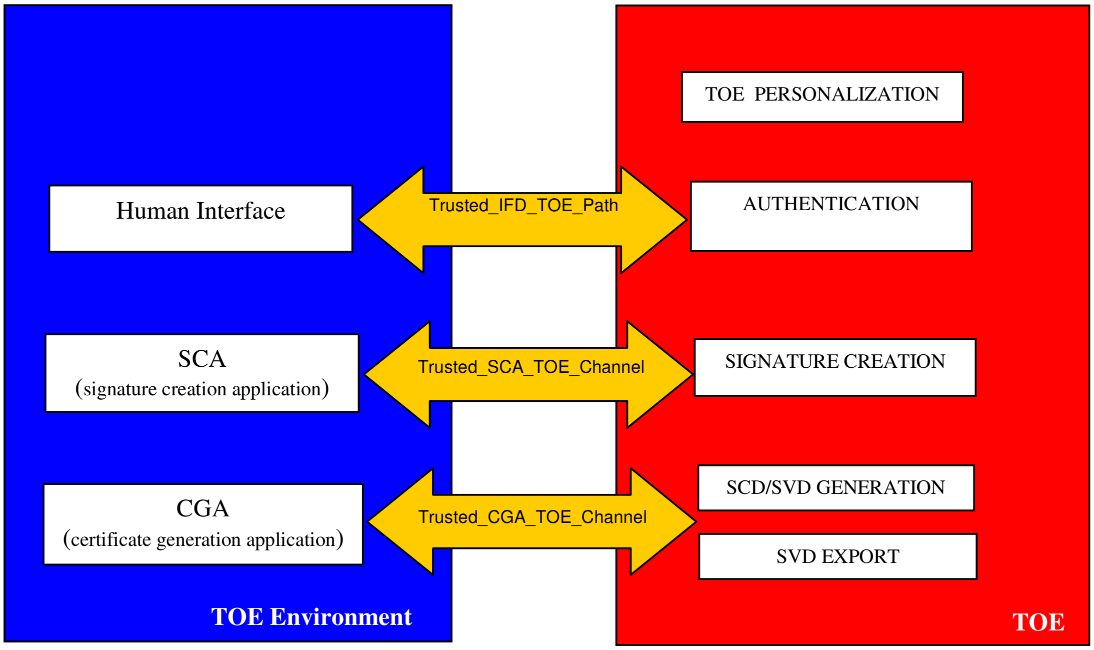

Figure 1: TOE boundaries

[12] The CGA, the SCA and the Human Interface are part of the immediate environment of the TOE.

[13] The TOE is securely personalized by a trusted and competent administrator according to Administrator Guidance: during TOE personalization, the administrator is responsible for Touch&Sign2048 V1.00 File System creation and configuration via a Personalization application.

[14] After its personalization, the TOE is ready to be:

- Securely used for signature under sole control of one specific user (the *signatory* in the remainder of the document);

- Securely administered by an authorized Administrator.

[15] The TOE is able to generate its own signature keys (the SCD/SVD pair): an authorized Administrator uses the CGA to initiate SCD/SVD generation and to ask the SSCD to export the SVD for generation of the corresponding certificate.

[16] The TOE holds the SVD and, before exporting the SVD to a CGA for certification purposes, it provides a trusted channel in order to maintain its integrity.

[17] The TOE is able to perform the signature operation using the RSA cryptographic algorithm and the parameters agreed as suitable according to [5].

[18] The signatory must be authenticated before signatures creation is allowed: for this reason he sends his authentication data (a PIN) to the TOE using a trusted path between the interfaces device (IFD) used, i.e. a smartcard reader, and the TOE.

[19] The smartcard reader is also used:

- by the Signatory or the Administrator to change his Reference Authentication Data (RAD) held by the TOE against which the TOE verifies a user PIN;
- by the Administrator to unblock the Signatory's Reference Authentication Data, when needed.

[20] The data to be signed (DTBS) or their representation (DTBSR) are transferred by the SCA to the TOE only over a trusted channel in order to maintain their integrity. The same channel is used to return the signed data object (SDO) from the TOE to the SCA (see [SSCD PP] § 2.1).

[21] The TOE, when requested by the SCA, is able to generate data to be signed representation (DTBSR) using a hash function agreed as suitable according to [5].

[22] As depicted in the next figure, Touch&Sign2048 V1.00 embedded SW is structured on two layers consisting of the devices drivers and the SSCD application, in which SW functions are implemented as APDU commands compliant with ISO/IEC 7816- part 4 and 8 (see [11]).

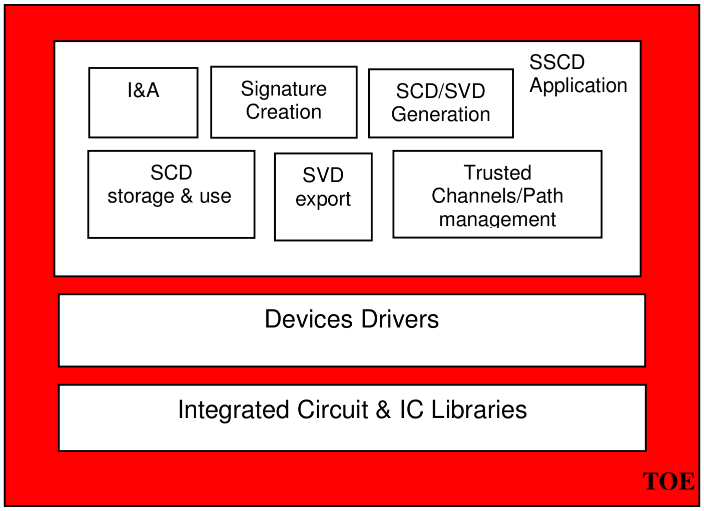

Figure 2: TOE components

9.3. TOE life cycle

[23] The typical TOE lifecycle is shown in Figure 3. Basically, it consists of a *design and development* phase and an *operational* phase.

[24] As already stated, Touch&Sign2048 V1.00 HW platform design and development has been certified respect to PP 9806 [7], that includes the state 1 delivery, the state 2 and the state 3.

[25] TOE lifecycle states within the scope of the evaluation are those covered by [SSCD PP], which refers to the operational phase. This phase represents installation, generation, start-up and operation in the CC terminology.

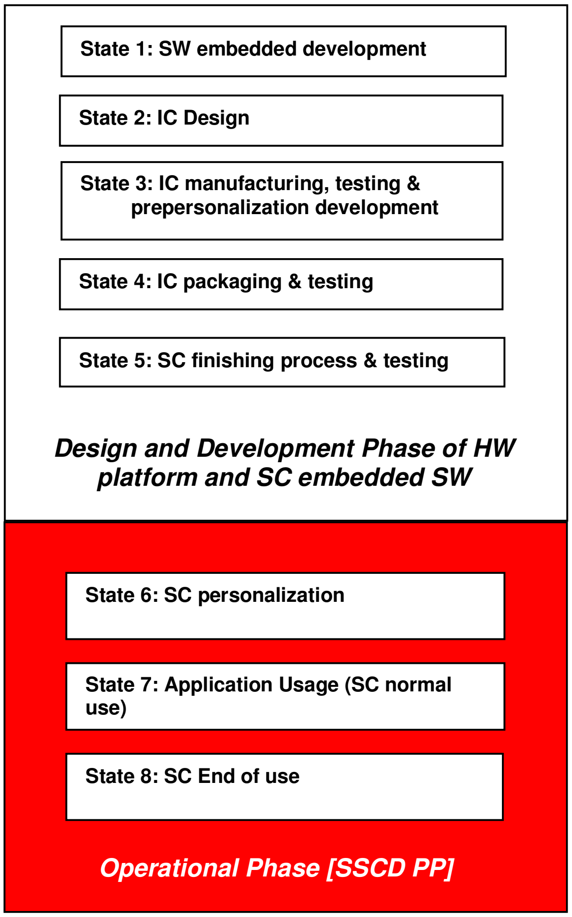
State 1: SW embedded development
State 2: IC Design
State 3: IC manufacturing, testing & prepersonalization development
State 4: IC packaging & testing
State 5: SC finishing process & testing
Design and Development Phase of HW platform and SC embedded SW
State 6: SC personalization
State 7: Application Usage (SC normal use)
State 8: SC End of use
Operational Phase [SSCD PP]

Figure 3: TOE life cycle

[26] The TOE implements a mechanism in order to recognize its operational phase.

[27] The TOE is delivered from *chip manufacturer* (ST Microelectronics) to *card manufacturer* (ST Incard srl) after the completion of the state 4 **"IC Packaging and & Testing".**

[28] The TOE is delivered to the *card manufacturer* with a secret Reference Authentication Data called Manufacturer Transport Secure Code (MTSC) to be used for *card manufacturer* identification and authentication.

[29] The TOE operational phase starts after Touch&Sign2048 V1.00 smartcard OS and its HW platform have been successfully designed, developed, manufactured and tested.

[30] The TOE operational phase is entered at completion of the state 5 **" SC finishing process & Testing"** after the structure of the TOE file system has been loaded in the TOE memory according to TOE Administration Guidance.

[31] The TOE is in *SC personalization* state at the beginning of TOE Operational phase.

[32] In the state 6 **"SC personalization"** the TOE administrator is responsible for:

- TOE file system configuration according to TOE Administration Guidance
- Set the TSF data Access conditions and Secure Messaging conditions according to TOE Administration Guidance

The TOE security is granted in the other states of TOE operational phase.

[33] Moreover, in the state 6 **"SC personalization"** the TOE administrator is in particular responsible for:

- Changing the default RAD_A value;
- Creating the SCD/SVD pair and setting their Access Conditions and Secure Messaging conditions in order to grant that the SCD will be used for signing purposes only by the legitimate Signatory;
- Exporting the SVD for certification purposes;
- Creating Reference Authentication Data to be used for Signatory identification purpose (RAD_S) and setting its Access Conditions and Secure Messaging conditions;
- Importing the cryptographic keys to be used for Secure Messaging (SM_{keys});

[34] After completion of **"SC personalization"** state, the administrator put the TOE in state 7 **"SC Normal use"**, where the TOE could be used either by the Signatory or the Administrator.

[35] In state 7 **"SC Normal use"** the TOE allows the Signatory to:

- Change the RAD_S value used by the TOE for his identification and authentication;
- Use the SCD for signing DTBS data.

[36] In state 7 **"SC Normal use"** the TOE allows the Administrator to:

- Change the RAD_A value used by the TOE for his identification and authentication;
- Creation of a new SCD/SVD pair with secure destruction of previously created SCD/SVD pair managed by the TOE;
- Export the SVD for certification purposes.

[37] When a failure occurs in state 7 **"SC Normal use"**, the TOE manages the fault and, according to its severity, enters in one of the following states:

- If a chip integrity violation occurred, the TOE enters the state 8 **"SC end of use"**, where, after having performed all actions needed for its secure disposal, the TOE is no more able to process any APDU command;
- If the failure cannot be recovered, the TOE enters the state 8 **"SC end of use"**, where the TOE signing application is no more available;
- In all other cases in which the failure is recovered, the TOE turns back in the state 7 **"SC Normal use"**.

9.4. User and Administrator guidance

The user and administrator guidance is a TOE manual which describes all the TOE functionalities, life cycle, application interface, personalization, initialization and secure usage recommendations. The guidance is delivered by the TOE manufacturer to the TOE administrator and is the basic reference documentation for a right and secure TOE management.

9.5. TOE Environment

9.5.1. Development and Production Environment

[38] The TOE described in this ST is developed in the following environments:

STATE	DESCRIPTION	ENVIRONMENT
1	Embedded Software (OS and application) Development	ST Incard
2	IC Design	ST Rousset, ST AMK
3	IC manufacturing and testing	ST Rousset
4	IC Packaging and testing	ST-Bouskoura, ST Incard

10 TOE Security Environment

[39] Following paragraphs describe the security aspects of the environment in which the TOE is intended to be used.

10.1. Assets

[40] With regard to Touch&Sign2048 V1.00 implementation, assets that need to be protected by the TOE are here defined according to [SSCD PP] [6] § 3. The following table summarizes them for clarity:

ASSET ACRONYM	ASSET DESCRIPTION	SECURITY NEED
SCD:	Private key used to perform an electronic signature operation.	Confidentiality.
SVD:	Public key linked to the SCD and used to perform an electronic signature verification.	Integrity, when it is exported.
DTBS(R):	Set of data, or its representation which is intended to be signed.	Integrity.
VAD:	PIN code entered by the End User to perform a signature operation.	Confidentiality and authenticity as needed by the authentication method employed.
RAD$_A$:	Reference PIN code used to identify and authenticate the Administrator.	Integrity and confidentiality.
RAD$_S$:	Reference PIN code used to identify and authenticate the Signatory.	Integrity and confidentiality.
	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.
	Electronic signature	Not forgery (Integrity).

10.2. Subjects

[41] In [SSCD PP] [6] § 3 are defined subjects that can operate with the TOE, here reported for clarity:

SUBJECTS	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 initialization, TOE personalization or other TOE administrative functions.
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.

10.3. Threat agents

[42] In [SSCD PP] [6] § 3 are defined malicious subjects that aim to attack the TOE, here reported for clarity:

THREAT AGENT	DEFINITION
S.OFFCARD	Attacker. A human or process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker is to access Application sensitive information. The attacker has a **high level potential attack** and **knows no secret**.

10.4. Secure usage Assumptions

[43] The same defined in [SSCD PP] [6] § 3.1, with the following addition:

ASSUMPTION	DEFINITION
A.PERSONALIZATION	It is assumed that TOE personalization takes place with the observance of physical and procedural measures granting the integrity, confidentiality and availability of the TOE personalization data. In particular it is assumed that symmetric keys used to implement the trusted channels and path by the secure messaging mechanism are securely imported and stored by the SCA and the CGA applications.
A.MANAGE	It is assumed that the TOE is personalized (in *SC personalization* state) and administered (in *SC normal use*) according to the Administration documentation by a competent individual who is responsible for the security of TOE assets and who is trusted not to abuse his privileges. In particular, it is assumed that TOE Administrator follows the TOE Administration documentation for TOE secure disposal after it entered the *SC end of use* state.
A.VAD	It is assumed that information needed for positive identification and authentication by the TOE are delivered to TOE users in a secure manner.

10.5. Organizational Security Policies

[44] As defined in [SSCD PP] [6] § 3.3.

10.6. Threats to Security

[45] Threats are here reported for clarity as they are defined in [SSCD PP] [6] § 3.2.

T.TYPE	THREAT
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 no repudiation of the electronic signature is compromised. This result in 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 to the CGA. 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 intended 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.

11 Security Objectives

11.1. Security objectives for the TOE

[46] Following table summarizes which are the security objectives for the TOE, as they are defined in [SSCD PP] [6] § 4.1.

OT.TYPE	TOE OBJECTIVE
OT.EMSEC_Design	*Provide physical emanations security* The TOE is designed and built in such a way as to control the production of intelligible emanations within specified limits.
OT.Lifecycle_Security	*Lifecycle security* The TOE detects flaws during the initialization, personalization and operational usage. The TOE provides safe destruction techniques for the SCD in case of 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 ensures the correspondence between the SVD and the SCD generated by the TOE itself. The TOE verifies the correspondence between the SCD stored by the TOE and the SVD sent to the TOE on demand.
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 ensures 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.DTBS_Integrity_TOE	*Verification of the DTBS-representation integrity* The TOE verifies 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 resists to 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.

11.2. Security objectives for the environment

As defined in [SSCD PP] [6] § 4.2 with the addition of the paragraph 11.2.1.

11.2.1. Additional security objective for the non-IT environment

OE.Op_Phase	*TOE operational phase security* The security of the TOE itself, of personalization data to be loaded into the TOE and of related verification authentication data (VAD) is ensured by S.Admin, S.User and S.Signatory in the TOE's non-IT environment throughout the TOE's operational phase, i.e. in personalization, normal use and end of use, and during delivery between operational lifecycle states

12 IT Security Requirements

[47] Here are defined the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE.

12.1. TOE Security Functional Requirements

[48] The TOE consists of a combination of hardware and software components implementing the specific TOE Security Functions (TSF) for the functional requirements defined in the PP.

[49] Following table lists each TOE Security Functional Requirement (SFR) included in this Security Target and identifies which Common Criteria operations (assignment (A), selection (S), refinement (R), and/or iteration (I)) have been applied to the requirement relative to the SSCD Protection Profile [SSCD PP] [6] .

COMPONENT	NAME	A	S	R	I
FCS_CKM.1.1	Cryptographic Key Generation	×			
FCS_CKM.4.1	Cryptographic Key Destruction	×			
FCS_COP.1.1/CORRESP	Cryptographic Operation: SCD/SVD correspondence verification	×			
FCS_COP.1.1/SIGNING	Cryptographic Operation : digital signature generation	×			
FIA_AFL.1.1	Authentication Failure handling	×			
FMT_MSA.1.1 Administrator	Management of security attributes	×			
FMT_MSA.3.1	Static Attribute Initialization			×	
FMT_SMF.1.1	Specification of Management Functions	×			
FMT_MTD.1.1	Management of TSF data	×			
FPT_AMT.1.1	Abstract Machine Testing		×		
FPT_EMSEC.1.1	TOE Emanation	×			
FPT_EMSEC.1.2	TOE Emanation	×			
FPT_FLS.1.1	Failure with preservation of secure state	×			
FPT_PHP.3.1	Resistance to physical attack	×			
FPT_TST.1.1	TSF Testing		×		
FTP_ITC.1.2/SVD Transfer	Trusted Path/Channel		×		
FTP_TRP.1.2/TOE	Trusted Path		×		
FTP_TRP.1.3/TOE	Trusted Path	×	×		

Table 1: Operation performed on TOE SFRs

[50] This paragraph fully restates TOE security functional requirements (see [SSCD PP] [6] in § 5.1) for clarity: operations completed in this ST are shown in ***bold italics***.

12.1.2.	CRYPTOGRAPHIC SUPPORT (FCS)	
12.1.2.1.	**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*** and specified cryptographic key sizes ***of 1024 and 2048 bits*** that meet the following: ***RSA*** ([5] par. 4.5.2.2)
12.1.2.2.	**Cryptographic key destruction (FCS_CKM.4)**	
	FCS_CKM.4.1[1]	The TSF shall destroy cryptographic keys in case of regeneration of a new SCD in accordance with a specified cryptographic key destruction method ***physical irreversible destruction of the stored key value*** that meets the following standard ***none***.
12.1.2.3.	**Cryptographic operation (FCS_COP.1)**	
	FCS_COP1.1/CORRESP	The TSF shall perform SCD/SVD correspondence verification in accordance with a specified cryptographic algorithm ***RSA*** and cryptographic key sizes ***1024 and 2048 bits*** that meet the following: ***RSA*** ([5] par. 4.5.2).
	FCS_COP1.1/SIGNING	The TSF shall perform digital signature-generation in accordance with a specified cryptographic key generation algorithm ***RSA*** and specified cryptographic key sizes ***1024 and 2048 bits*** that meet the following: ***PKCS #1 v1.5: RSA Encryption Standard – RSA Laboratories – 1 Nov 1993 [22].***

[1] The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.

12.1.3.	USER DATA PROTECTION (FDP)	
12.1.3.1.	**Subset access control (FDP_ACC.1)**	
	FDP_ACC.1.1/SVD Transfer SFP	The TSF shall enforce the SVD Transfer SFP on export of SVD by User.
	FDP_ACC.1.1/ Initialization SFP	The TSF shall enforce the Initialization SFP on generation of SCD/SVD pair by User.
	FDP_ACC.1.1/Personalization SFP	The TSF shall enforce the Personalization SFP on creation of RAD by Administrator.
	FDP_ACC.1.1/Signature-creation SFP	The TSF shall enforce the Signature-creation SFP on: 1. sending of DTBS-representation by SCA, 2. signing of DTBS-representation by Signatory.
12.1.3.2.	**Security attribute based access control (FDP_ACF.1)**[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.
	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 "authorized" is allowed to generate SCD/SVD pair.
	FDP_ACF.1.3/Initialisation SFP	The TSF shall explicitly authorize 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 authorized" is not allowed to generate SCD/SVD pair.
	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 authorize access of subjects to objects based on the following additional rules: none.

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

USER, SUBJECT OR OBJECT THE ATTRIBUTE IS ASSOCIATED WITH	ATTRIBUTE	STATUS
GENERAL ATTRIBUTE GROUP		
User	Role	Administrator, signatory
INITIALIZATION ATTRIBUTE GROUP		
User	SCD/SVD management	Authorized/not authorized
SIGNATURE CREATION ATTRIBUTE GROUP		
SCD	SCD operational	No, yes
DTBS	Sent by an authorized SCA	No, yes

	FDP_ACF.1.4/ SVD Transfer SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: none.
	Personalization SFP	
	FDP_ACF.1.1/ Personalization SFP	The TSF shall enforce the Personalization SFP to objects based on General attribute.
	FDP_ACF.1.2/ Personalization SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute “role” set to “Administrator” is allowed to create the RAD.
	FDP_ACF.1.3/ Personalization SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
	FDP_ACF.1.4/ Personalization SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: none.
	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 group.
	FDP_ACF.1.2/ Signature-creation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute “role” set to “Signatory” is allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute “SCD operational” is set to “yes”.
	FDP_ACF.1.3/ Signature-creation SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
	FDP_ACF.1.4/ Signature-creation SFP	The TSF shall explicitly deny access of subjects to objects based on the 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”.
12.1.3.3.	**Export of user data without security attributes (FDP_ETC.1)**	
	FDP_ETC.1.1/SVD Transfer	The TSF shall enforce the SVD Transfer 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.

12.1.3.4.	**Import of user data without security attributes (FDP_ITC.1)**	
	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[3]	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: DTBS-representation shall be sent by an authorized SCA.
12.1.3.5.	**Subset residual information protection (FDP_RIP.1)**	
	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, RAD.
12.1.3.6.	**Stored data integrity monitoring and action (FDP_SDI.2)[4]**	
	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.
	FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored within the TSC for integrity error on all objects, based on the following attributes: integrity checked stored data.
	FDP_SDI.2.2/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.
12.1.3.7.	**Data exchange integrity (FDP_UIT.1)**	
	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.
	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.

12.1.4. IDENTIFICATION AND AUTHENTICATION (FIA)

[3] 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.

[4] Note that The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data":

1. SCD
2. RAD
3. SVD

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

12.1.4.1.	**Authentication failure handling (FIA_AFL.1)**	
	FIA_AFL.1.1	The TSF shall detect when ***3*** 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.
12.1.4.2.	**User attribute definition (FIA_ATD.1)**	
	FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: RAD.

12.1.4.3.	**Timing of authentication (FIA_UAU.1)**	
	FIA_UAU.1.1	The TSF shall allow 1. Identification of the user by means of TSF required by FIA_UID.1. 2. Establishing a trusted path between local user[5] and the TOE by means of TSF required by FTP_TRP.1/TOE. 3. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import. on behalf of the user to be performed before the user is 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.
12.1.4.4.	**Timing of identification (FIA_UID.1)**	
	FIA_UID.1.1	The TSF shall allow 1. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE. 2. 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.

12.1.5.	**SECURITY MANAGEMENT (FMT)**	
12.1.5.1.	**Management of security functions behaviour (FMT_MOF.1)**	
	FMT_MOF.1.1	The TSF shall restrict the ability to enable the signature-creation function to Signatory.
12.1.5.2.	**Management of security attributes (FMT_MSA.1)**	
	FMT_MSA.1.1 Administrator	The TSF shall enforce the Initialization SFP to restrict the ability to modify the security attributes SCD/SVD management to Administrator.
	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.
12.1.5.3.	**Secure security attributes (FMT_MSA.2)**	
	FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.
12.1.5.4.	**Static attribute initialization (FMT_MSA.3)**	

[5] The "Local user" mentioned in component FIA_UAU.1.1 is the user using the trusted path provided between the SCA in the TOE environment and the TOE as indicated by FTP_TRP.1/SCA and FTP_TRP.1/TOE.

	FMT_MSA.3.1	The TSF shall enforce the Initialization SFP and Signature-creation SFP to provide restrictive default values for security attributes that are used to enforce the SFP. Refinement The security attribute of the SCD “SCD operational” is set to “no” after generation of the SCD.
	FMT_MSA.3.2	The TSF shall allow the Administrator to specify alternative initial values to override the default values when an object or information is created.
12.1.5.5.	**Management of TSF data (FMT_MTD.1)**	
	FMT_MTD.1.1	The TSF shall restrict the ability to modify the RAD to Signatory.
12.1.5.6.	**Specification of Management Functions (FMT_SMF.1)**	
	FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: ***Identification and Authentication management, access condition management.***
12.1.5.7.	**Security roles (FMT_SMR.1)**	
	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.

12.1.6.	PROTECTION OF THE TSF (FPT)	
12.1.6.1.	**Abstract machine testing (FPT_AMT.1)**	
	FPT_AMT.1.1	The TSF shall run a suite of tests ***during initial start-up*** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.
12.1.6.2.	**TOE Emanation (FPT_EMSEC.1)**	
	FPT_EMSEC.1.1	The TOE should not emit ***Side Channel Current*** in excess of ***States of Art limits*** enabling access to RAD and SCD
	FPT_EMSEC.1.2 [6]	The TSF shall ensure ***all users*** are unable to use the following interface ***external contacts*** to gain access to RAD and SCD.
12.1.6.3.	**Failure with preservation of secure state (FPT_FLS.1)**	
	FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: ***Power shortage, over voltage, over and under clock frequency, integrity problems***.
12.1.6.4.	**Passive detection of physical attack (FPT_PHP.1)**	
	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.
12.1.6.5.	**Resistance to physical attack (FPT_PHP.3)**	
	FPT_PHP.3.1	The TSF shall resist ***operating changes by the environment, and physical integrity,*** to the ***clock, voltage supply and shield layers*** by responding automatically such that the TSP is not violated.

[6] The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.
Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

12.1.6.6.	**TSF Testing (FPT_TST.1)**	
	FPT_TST.1.1	The TSF shall run a suite of self-tests ***during initial start-up or when calling a sensitive module*** to demonstrate the correct operation of the TSF.
	FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
	FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

12.1.7.	TRUSTED PATH/CHANNELS (FTP)	
12.1.7.1.	**Inter-TSF trusted channel (FTP_ITC.1)**	
	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.
	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 SCA to initiate communication via the trusted channel.
	FTP_ITC.1.3/DTBS Import	The TSF or the SCA shall initiate communication via the trusted channel for signing DTBS-representation.
12.1.7.2.	**Trusted path (FTP_TRP.1)**	
	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***.

12.2. TOE Security Assurance Requirements

[51] TOE assurance requirements are those stated in [SSCD PP] [6] § 5.2, here reported in tabular form:

ASSURANCE CLASS	ASSURANCE COMPONENTS
ACM	ACM_AUT.1 - ACM_CAP.4 - ACM_SCP.2
ADO	ADO_DEL.2 - ADO_IGS.1
ADV	ADV_FSP.2 - ADV_HLD.2 - ADV_IMP.1 - ADV_LLD.1 - ADV_RCR.1 - ADV_SPM.1
AGD	AGD_ADM.1 - AGD_USR.1
ALC	ALC_DVS.1 - ALC_LCD.1 - ALC_TAT.1
ATE	ATE_COV.2 - ATE_DPT.1 - ATE_FUN.1 - ATE_IND.2
AVA	AVA_MSU.3 - AVA_SOF.1 - AVA_VLA.4

Table 2: Assurance Requirements - EAL 4 extended with AVA_MSU.3 and AVA_VLA.4

12.3. IT Environment Security requirements

[52] Following table lists each IT Environment Security Functional Requirement (SFR) included in this Security Target and identifies which Common Criteria operations (assignment (A), selection (S), refinement (R), and/or iteration (I)) have been applied to the requirement relative to the SSCD Protection Profile [SSCD PP] [6].

COMPONENT	NAME	A	S	R	I
FCS_CKM.2.1/CGA	Cryptographic Key Distribution	×			
FCS_CKM.3.1/CGA	Cryptographic Key access	×			
FCS_COP.1.1/SCA Hash	Cryptographic Operation	×			
FTP_ITC.1.2/ SVD import	Inter-TSF trusted channel		×		
FTP_TRP.1.2/SCA	Trusted Path		×		
FTP_TRP.1.3/SCA	Trusted Path	×	×		

Table 3: Operation performed on ENVIRONMENT SFRs

[53] Following paragraph fully restates security requirements for the IT environment presented in [SSCD PP] [6] § 5.3 for clarity.

[54] Numbering of SFRs in this ST is the same proposed in [SSCD PP] [6]: operations completed in this ST are shown in ***bold italics***.

12.3.2.	**CERTIFICATION GENERATION APPLICATION (CGA)**	
12.3.2.1.	**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:: ***AES-128, DES and Triple DES with 2 or 3 kesy.***
12.3.2.2.	**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: ***none***.
12.3.2.3.	**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.
12.3.2.4.	**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 remote trusted IT product*** to initiate communication via the trusted channel.
	FTP_ITC.1.3/ SVD import	The TSF or the TOE shall initiate communication via the trusted channel for import SVD.

12.3.3.	SIGNATURE CREATION APPLICATION (SCA)	
12.3.3.1.	**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*** or ***SHA-256*** and cryptographic key sizes none that meet the following: ***to be the Secure Hash Algorithm, SHA-1 or SHA-256 as specified in the standard [20][21].***
12.3.3.2.	**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.
12.3.3.3.	**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 TOE shall initiate communication via the trusted channel for signing DTBS-representation by means of the SSCD.
12.3.3.4.	**Trusted path (FTP_TRP.1)**	
	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.***

12.3.4. Non-IT Environment Security requirements

[55] As defined in § 5.4 of [SSCD PP] [6].

13 TOE Summary Specification

[56] This section contains a high-level specification of each TOE Security Function (TSF) that contributes to satisfaction of the Security Functional Requirements of chapter 12.

[57] The specifications cover following major areas: identification and authentication, access controls, key management, data transfer over trusted path and channels, stored data protection, test management, failure management and TOE life cycle management.

[58] Following table lists the SFRs not mentioned in the [SSCD PP] [6] but included in this Security Target.

FMT_SMF.1

[59] The Table 8 shows that all the SFRs are satisfied by at least one TSF and that every TSF is used to satisfy at least one SFR.

.

13.1. TOE Security Functions

This part lists the TOE Security Functions. They are grouped as shown in the table below:

FAMILY	SECURITY FUNCTION	DESCRIPTION
Identification and Authentication	SF.AUTH SF.RAD	Authentication functions RAD management
Access Control	SF.AC	Access Control
Key Management and Cryptography	SF.KEY_GEN SF.HASH SF.MAC SF.SIGN	Key Generation Hash computation MAC computation Crypto functions
Secure Messaging	SF.SM	Secure Messaging
Stored Data Protection	SF.OBS_A SF.INT_A SF.DATA_ERASE SF.TRANSACTION	Un-observability TOE logical integrity Secure destruction of the data Anti-tearing function
Test	SF.TEST	Self Test and Audit
Failure	SF.EXCEPTION	Error message and exception
TOE life cycle	SF.LIFE_CYCLE	TOE life state management
TOE HARDWARE	SF.HARDWARE	TOE Cryptographic support, TRNG and physical protection

Table 4: List of TOE security functions

13.1.1. *Identification and authentication*

SF.AUTH
[60] This function updates the security status, after a successful external authentication. The external authenticate requires a challenge generated by the TOE by means of a random number generator implemented in the IC which is compliant with [18]. The internal authenticate requires a challenge generated by the IFD. Both internal and external authentications use Triple DES with 2 or 3 keys, AES-128 or RSA with 512-bit, 768-bit, 1024-bit and 2048-bit key length. An authentication failure counter related to the authentication key is decreased after each unsuccessful authentication, when the counter decrease to zero than the related authentication key is blocked and no more authentications are allowed with that key. The authentication failure counter initial value is 3. The user authentication is realized with a PIN, whose minimum length is set to 6 characters. The maximum PIN retry counter is set to the value 3. When this limit is reached the TSF block the relevant RAD. The character set is composed by all the symbols that can be represented using two hexadecimal digits. This function is realized by a permutation mechanism. This function implements the mutual authentication as defined in the HPC functionality for Netlink scheme (see [24]). The crypto algorithm support is provided by the IC crypto library functionality included in the TSF **SF.HARDWARE.** The strength of this function is SOF High.

MAPPED TOE SFRs				
FDP	FDP	FIA	FMT	FTP
ETC.1.1 SVD Transfer	ACC.1.1 Signature Creation SFP	AFL.1.1	MTD.1.1	ITC.1.1 SVD Transfer
ETC.1.2 SVD Transfer	ACF.1.2 Initialization SFP	AFL.1.2	SMF.1.1	ITC.1.2 SVD Transfer
ITC.1.1. DTBS	ACF.1.4 Initialization SFP	UAU.1.1		ITC.1.3 SVD Transfer
ITC.1.2. DTBS	ACF.1.2 SVD Transfer SFP	UAU.1.2		ITC.1.1 DTBS Import
ITC.1.3. DTBS	ACF.1.2 Personalization SFP	UID.1.1		ITC.1.2 DTBS Import
ACC.1.1 SVD Transfer SFP	ACF.1.2 Signature Creation SFP	UID.1.2		ITC.1.3 DTBS Import
ACC.1.1 Initialization SFP	ACF.1.4 Signature Creation SFP			TRP.1.1 TOE
ACC.1.1 Personalization SFP				TRP.1.2 TOE
				TRP.1.3 TOE

SF.RAD

[61] This function controls all operations related to the Reference Authentication Data (RAD) management. It includes the verification, unblock, and change of the RAD.

[62] Verification

- In case a user is successfully identified, the TOE verify that his VAD corresponds to RAD related to the user claimed identity;

- If the user claimed to be the Administrator, his VAD is checked by the TOE against RAD_A value: if the comparison succeed the user is uniquely identified and authenticated as the Administrator;

- If the user claimed to be the Signatory, his VAD is checked by the TOE with RAD_S value: if the comparison succeeds the user is uniquely identified and authenticated as the Signatory.

- In case the verification is not successful, the TOE records this condition decrementing the Retry Counter of the RAD. When the value of the Retry Counter reaches 0, the RAD's state is Blocked. A blocked RAD is no more available for verification.

[63] Unblock

- The Unblock function can be performed only if the security status satisfies the security attributes for this command.

- The Unblock function resets the RAD retry counter to its initial value, fixed to.3.

- After a successful unblocks, the RAD may be used for verification.

[64] Change

- This function replaces the RAD stored in the TOE with a new RAD sent by the IFD.

- The Change function can be performed only if the security status satisfies the security attributes for this command.

MAPPED TOE SFRs		
FDP	FIA	FMT
ACC.1.1 SVD Transfer SFP	AFL.1.1	MTD.1.1
ACC.1.1 Initialization SFP	AFL.1.2	
ACC.1.1 Personalization SFP		
ACC.1.1 Signature Creation SFP		
ACF.1.2 Initialization SFP		
ACF.1.4 Initialization SFP		
ACF.1.2 SVD Transfer SFP		

ACF.1.2 Personalization SFP		
ACF.1.2 Signature Creation SFP		
ACF.1.4 Signature Creation SFP		

13.1.2. Access Control

SF.AC

[65] This function compares the security status to process commands and / or to access files and data objects. The security status represents the current state possibly achieved after completion of the answer to reset and a possible protocol and parameter selection and / or a single command or a sequence of commands possibly performing authentication procedures. The security attributes, when they exist, define which actions are allowed, and under which conditions. For example:

- To authorized user is allowed generate the SCD/SVD key pair
- To authorized user is allowed export the SVD
- To the "Administrator" is allowed the management of the SCD/SVD security attributes
- To the "Administrator" is allowed the creation of the RAD_S
- To the "Signatory" is allowed sign DTBS-representation
- To the "Signatory" is allowed change in ***"active"*** the operational state of the SCD

MAPPED TOE SFRs			
FDP	FDP	FMT	FIA
ACC.1.1 SVD Transfer SFP	**ACF.1.3 SVD Transfer SFP**	**MOF.1.1.**	**ATD.1.1**
ACC.1.1 Initialization SFP	**ACF.1.4 SVD Transfer SFP**	**MSA.1.1 Administrator**	
ACC.1.1 Personalization SFP	**ACF.1.1 Personalization SFP**	**MSA.1.1 Signatory**	
ACC.1.1 Signature Creation SFP	**ACF.1.2 Personalization SFP**	**MSA.2.1**	
ACF.1.1 Initialization SFP	**ACF.1.3 Personalization SFP**	**MSA.3.1**	
ACF.1.2 Initialization SFP	**ACF.1.4 Personalization SFP**	**MSA.3.2**	
ACF.1.3 Initialization SFP	**ACF.1.1 Signature Creation SFP**	**MTD.1.1**	
ACF.1.4 Initialization SFP	**ACF.1.2 Signature Creation SFP**	**SMF.1.1**	
ACF.1.1 SVD Transfer SFP	**ACF.1.3 Signature Creation SFP**	**SMR.1.1**	
ACF.1.2 SVD Transfer SFP	**ACF.1.4 Signature Creation SFP**	**SMR.1.2**	

13.1.3. Key Management and Cryptography

SF.KEY_GEN

[66] The TSF SF.KEY_GEN implements the following main functions:

- SCD/SVD exp/mod or CRT format generation
- SCD/SVD correspondence
- SCD/SVD storing

This function generates the SCD/SVD pair according to the RSA algorithm (see [5], [22]), using a length of 1024 or 2048 bits.

The SVD is generated and stored in the TOE in the format **(n, e)** where **n** is the RSA modulus and **e** the RSA public exponent.

The SCD is generated and stored in the TOE in two alternative formats:

1. modulus/exponent format **(n, d)** where **n** is the RSA modulus and **d** the RSA private exponent
2. CRT format **(p, q, dP, dQ, qInv)** where **p** is the first factor, **q** is the second factor, **dP** is the first factor's CRT exponent, **dQ** is the second factor's CRT exponent and **qInv** is the CRT coefficient.

SCD of 2048-bit are generated and stored in the TOE exclusively in CRT format.

The function checks the SCD/SVD correspondence.

The RSA key generation support is provided by the IC crypto library functionality included in the TSF **SF.HARDWARE.** The crypto library makes available the basic functionalities for a RSA key generation of various bit length, this include prime generation, primality test, private key exponent and module generation.

MAPPED TOE SFRs		
FCS		
CKM.1.1		
COP.1.1 correspondence		

SF.HASH

[67] This function generates a hashing of data, using the algorithm SHA-1 or SHA-256 (see [20] and [21]). The obtained hash (160 bits) or (256-bit) is stored in the TOE and may be used for another computation.

The TOE can complete the hashing process on imported data and on intermediate hash result.

The function manages all the operation concerning the crypto library initialization, the pre, the intermediary and the post hash computation

The SHA-256 algorithm is implemted by the TSF without the support of the IC crypto library.

The SHA-1 algorithm support is provided by the IC crypto library functionality included in the TSF **SF.HARDWARE.**

The strength of this function is SOF High.

MAPPED TOE SFRs		
FCS		
COP.1.1 signing		

SF.MAC

[68] The function generates and verifies a MAC, using a DES, Triple DES with 2 or 3 keys or AES-128, as defined in the standards [16] and [17].

The function implements the SPA/DPA/DFA countermeasures as required in [30], [31].

The crypto algorithm support is provided by the IC crypto library functionality included in the TSF **SF.HARDWARE.** The HW EDES/AES crypto libraries make available all the basic functionalities for DES, TripleDES and AES-128 algorithm computations which include library initialization, key and data loading.

MAPPED TOE SFRs		
FDP	FTP	FTP
SDI.2.1. DTBS	**ITC.1.1 SVD Transfer**	**TRP.1.1 TOE**
SDI.2.2. DTBS	**ITC.1.2 SVD Transfer**	**TRP.1.2 TOE**
UIT.1.1 SVD Transfer	**ITC.1.3 SVD Transfer**	**TRP.1.3 TOE**
UIT.1.2 SVD Transfer	**ITC.1.1 DTBS Import**	
UIT.1.1 TOE DTBS	**ITC.1.2 DTBS Import**	
UIT.1.2 TOE DTBS	**ITC.1.3 DTBS Import**	

SF.SIGN

[69] This function signs imported data, using a RSA 1024 or 2048 bits private key in conformance with the algorithm RSA (see [22]). If the private key is stored in the TOE in CRT format then the Chinese Remainder Theorem is applied to perform the RSA algorithm.

The function implements the SPA/DPA/DFA countermeasures as required in [26].

The crypto algorithm support is provided by the IC crypto library functionality included in the TSF **SF.HARDWARE.** The HW crypto library makes available the basic functionalities for digital signature computation using RSA algorithm, which include library initialization and modular exponentiation.

MAPPED TOE SFRs		
FCS		
COP.1.1 signing		

13.1.4. Secure Messaging

SF.SM

[70] This function establishes a secure channel between the TOE and the IFD.

The goal is to protect [part of] any command-response pair to and from the card by ensuring two basic security functions: data confidentiality and data authentication.

The confidentiality is obtained by the encipherment of the transmitted message. This operation the Triple DES algorithm with 2 or 3 Keys (see [23]).

The command authentication uses a cryptogram based on MAC. In case of an unsuccessful authentication the command is refused.

An authentication failure counter related to the secure channel authentication key is decreased after each unsuccessful command authentication, when the counter decrease to zero than the related secure channel authentication key is blocked and no more command authentications are allowed with that key. The authentication failure counter initial value is 3.

The crypto algorithm support is provided by the IC crypto library functionality included in the TSF **SF.HARDWARE.**

The strength of this function is SOF High.

MAPPED TOE SFRS		
FDP	FTP	FTP
SDI.2.1. DTBS	**ITC.1.1 SVD Transfer**	**TRP.1.1 TOE**
SDI.2.2. DTBS	**ITC.1.2 SVD Transfer**	**TRP.1.2 TOE**
UIT.1.1 SVD Transfer	**ITC.1.3 SVD Transfer**	**TRP.1.3 TOE**
UIT.1.2 SVD Transfer	**ITC.1.1 DTBS Import**	
UIT.1.1 TOE DTBS	**ITC.1.2 DTBS Import**	
UIT.1.2 TOE DTBS	**ITC.1.3 DTBS Import**	

13.1.5. Stored Data Protection

SF.OBS_A

[71] This function addresses the TOE emanation security functional requirements.

This function is mostly realized by Integrated Circuit design and implementation of the TSF.

This function provides mechanism to avoid information leakage.

Although most functionalities are provided by HW components, countermeasures are required to be implemented in software by TSF which include “clock management” and other HW extra security functionalities management like Slow/Fast Cycle CPU mode, noise generation etc. as described in [29] chap. 3.7.

The basic mechanisms required to prevent data disclosure are provided by the IC data unobservability functionality included in the TSF **SF.HARDWARE.**

MAPPED TOE SFRS		
FPT		
EMSEC.1.1.		
EMSEC.1.2		

SF.INT_A
[72] This function addresses the TOE logical integrity. It includes the TOE die integrity, the integrity of the TSF code and the integrity of sensitive data like cryptographic keys, authentication data and DTBS. If an integrity error is found, depending on the origin, the TOE may abort the current operation and may change the TOE life cycle state. The TOE die integrity is fully implemented in HW through integrity mesh sensors. In case of a die integrity condition a TOE EEPROM flash programming is automatic started. The TSF code integrity is supported by SF.INT_A through the implementation of some check APDU The sensitive data integrity is partially supported by HW and SF.INT_A. The HW through the EEPROM ECC mechanism detects and report to SF.INT_A integrity failures. The TSF manages the failure condition. The basic mechanisms required to assure TOE die and sensitive data integrity are provided by the IC data integrity functionality included in the TSF **SF.HARDWARE.**

MAPPED TOE SFRS		
FDP	FPT	FPT
SDI.2.1. Persistent	PHP.1.1	TST.1.2
SDI.2.2. Persistent	PHP.1.2	TST.1.3

SF.DATA_ERASE
[73] This function is responsible to erase the data. It includes mainly two types of operations: - Erase the data before starting a new working session. - Erase the data before allocation and after deallocation of sensitive data

MAPPED TOE SFRS		
FCS	FDP	
CKM.4.1	RIP.1.1	

SF.TRANSACTION

[74] This function is responsible to manage the transaction of the TOE, and addresses the requirement of secure state of the TOE data.

A transaction is a logical set of updates of persistent data. It is important for transactions to be *atomic*: either all of the data fields are updated, or none are.

MAPPED TOE SFRs		
FPT		
FLS.1.1		

13.1.6. Test

SF.TEST

[75] This function ensures the tests of TOE functionality. It includes the Integrated Circuit and its environment.

Depending on the test, it is executed at power-up or before/after sensitive operation.

Upon detection of an anomaly, the TOE ends the working session or changes its life cycle state.

At TOE power-up and reset, the function implements all the tests of each HW component as required in [29].

MAPPED TOE SFRs		
FPT	FPT	
AMT.1.1	**PHP.1.2**	
FLS.1.1	**PHP.3.1**	
PHP.1.1	**TST.1.1**	

13.1.7. Failure

SF.EXCEPTION

[76] This function addresses the exception management. The reasons of these exceptions are: range of operating conditions, integrity errors, life cycle and TOE internal audit failure.

Upon detection, depending on the exception reason, the current operation is aborted; the TOE life cycle is changed.

The basic mechanisms required to assure a suitable exception management are provided by the IC sensors and IC Security Manager functionalities included in the TSF **SF.HARDWARE.**

MAPPED TOE SFRs		
FDP	FPT	FPT
SDI.2.1. Persistent	**FLS.1.1**	**PHP.1.2**
SDI.2.2. Persistent	**PHP.1.1**	**PHP.3.1**

13.1.8. TOE Life Cycle

SF.LIFE_CYCLE

[77] This function manages the TOE life cycle, as described in chapter *9.3 TOE life cycle*.
It ensures the detection of the current state and the switching of the state.
The change of state is irreversible.

MAPPED TOE SFRs		
FDP	FPT	FPT
SDI.2.1. Persistent	**FLS.1.1**	**PHP.1.2**
SDI.2.2. Persistent	**PHP.1.1**	**PHP.3.1**

13.1.9. TOE HARDWARE

SF.HARDWARE

[78] The TSF manages all functionalities implemented by the IC platform ST19WR66I. This includes:

- **IC CRYPTO LIBRARIES**: performs symmetric and asymmetric crypto operations. The algorithms supported are AES-128, DES, Triple DES with key up to 196-bit and RSA with module up to 2176-bit. Other supported functions are the RSA key pair generation with module up to 2176-bit and the SHA-1 hash function [26][27][28].
- **IC TRNG (Generators of Unpredictable Number)**: generates random numbers up to 1088-bit useful for crypto computation. The generator is compliant with FIPS-142 [18] and AIS31 [19].
- **IC SENSORS**: detects physical integrity and critical operating conditions of the IC (Voltage, Clock frequency) [25].
- **IC Security Manager**: detects memory access violation, bad CPU usage, bad EEPROM use etc. [25].
- **IC data integrity**: allows the integrity verification of TOE die and TOE ROM memory. Moreover, it corrects single bit fail in the TOE EEPROM memory [25].
- **IC data unobservability**: implementes mechanisms to prevent data disclosure [25].

The strength of this function is SOF High.

MAPPED TOE SFRs		
FTP	FPT	FCS
ITC.1.1 SVD Transfer	**FLS.1.1**	**COP.1.1 signing**
ITC.1.2 SVD Transfer	**PHP.1.1**	**CKM.1.1**
ITC.1.3 SVD Transfer	**TST.1.2**	**COP.1.1 correspondence**
ITC.1.1 DTBS Import	**TST.1.3**	
ITC.1.2 DTBS Import	**PHP.1.2**	
ITC.1.3 DTBS Import	**PHP.3.1**	
TRP.1.1 TOE	**EMSEC.1.1.**	
TRP.1.2 TOE	**EMSEC.1.2**	
TRP.1.3 TOE		

FDP	FDP	FDP
SDI.2.1. DTBS	UIT.1.2 TOE DTBS	ITC.1.3. DTBS
SDI.2.2. DTBS	ETC.1.1 SVD Transfer	ACF.1.2 Signature Creation SFP
UIT.1.1 SVD Transfer	ETC.1.2 SVD Transfer	ACF.1.4 Signature Creation SFP
UIT.1.2 SVD Transfer	ITC.1.1. DTBS	SDI.2.1. Persistent
UIT.1.1 TOE DTBS	ITC.1.2. DTBS	SDI.2.2. Persistent

13.2. Assurance Measures

[79] Appropriate assurance measures have been and are being employed to meet the assurance requirements for the Common Criteria EAL4 evaluation level augmented with AVA_VLA.4 and AVA_MSU.3 components.

14 SSCD PP Claims

[80] Touch&Sign2048 V1.00 conforms to the requirements of SSCD PP [6].

14.1. PP reference

[81] The ST is in compliance with the SSCD PP [6], identified as follows:

Title:	Protection Profile — Secure Signature-Creation Device Type 3
Authors:	Wolfgang Killmann, Herbert Leitold, Reinhard Posch, Patrick Sallé, Bruno Baronnet
Vetting Status:	
CC Version:	2.1 Final
General Status:	Approved by WS/E-SIGN on 2001-11-30
Version Number:	1.05
Registration:	BSI-PP-0006-2002
Keywords:	Secure signature-creation device, electronic signature

14.2. PP tailoring

[82] Tables in chapter 12 identifies each SFR for this Security Target and the tailoring operations performed relative to [SSCD PP] [6]. The tailoring is identified ***bold italics*** within the text of each SFR. All of the tailoring operations performed are in conformance with the assignment and selections in [SSCD PP] [6].

14.3. PP additions

[83] This Security Target includes one additional security objective for the non-IT environment **OE.Op_Phase** in 11.2.1.

[84] This Security Target includes one additional TOE security functional requirement **FMT_SMF.1** in 12.1.5.6.

[85] Due to the fact that both TOE Administrator and Signatory are identified and authenticated using the same mechanism, i.e. the verification of their PIN against a stored RAD, RAD Asset of [SSCD PP] [6] has been split in RAD_A and $RAD_{S,}$ which have the same security need.

[86] **A.PERSONALIZATION** states that the TOE personalization must be performed in the observance of proper physical and procedural measures.

[87] **A.MANAGE** states that the TOE secure personalization in *SC Personalization* state and its secure disposal, after having entered *SC End of Use* state, are managed under responsibility of competent and trusted Administrator, according to the Administration Documentation.

[88] **A.VAD** covers the procedural measures needed for the secure distribution of PIN codes to related TOE users.

15 Rationale

15.1. Security Objectives Rationale

15.1.1. Security Objectives Coverage.

[89] As for [SSCD PP] [6] § 6.2.1 and the additional objectives and assumptions.

Threats - Assumptions - Policies / Security objectives	OT.EMESEC_Design	OT.Lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OE.CGA_QCert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend	OE.OP_Phase
T.Hack_Phys	√			√			√	√									
T.SCD_Divulg				√													
T.SCD_Derive									√			√					
T.SVD_Forgery						√								√			
T.DTBS_Forgery										√						√	
T.SigF_Misuse										√	√				√	√	
T.Sig_Forgery	√	√		√	√	√	√	√				√	√	√		√	
T.Sig_Repud	√	√		√	√	√	√	√	√	√	√	√	√	√		√	
A.CGA													√	√			
A.SGA																√	
A.Personalization																	√
A.Manage																	√
A.VAD																	√
P.CSP_QCert					√								√				
P.QSign											√	√	√			√	
P.Sigy_SSCD			√						√		√						

Table 5: Threats, Assumptions and Policy to Security objective mapping

15.1.2. Security Objectives Sufficiency.

[90] As for [SSCD PP] [6] § 6.2.2 with the addition of the paragraph 15.1.2.2.

15.1.2.2. Additional assumptions and Security Objective Sufficiency

[91] **A.PERSONALIZATION (TOE personalization data integrity, confidentiality and availability)** establishes the trustworthiness of the personalization data, RAD, secret Key etc., stored in the TOE. This is addressed by the security objective for the non-IT environment OE.Op_Phase (*TOE operational phase security*), which ensures the security of the TOE during personalization.

[92] **A.MANAGE (TOE lifecycle state management)** enforces the security required during the whole operational phase of the TOE. It establishes that the TOE's operational phase is under the full control of competent user and trusted TOE administrator. This is addressed by the security objective for the non-IT environment OE.Op_Phase (*TOE operational phase security*), which ensures the security of the TOE by proper administration and proper usage.

[93] **A.VAD (TOE VAD delivery)** establishes that a secure user VAD delivery enforces the security needed for the identification and authentication procedures. This is addressed by the security objective for the non-IT environment OE.Op_Phase (*TOE operational phase security*), which ensures that only authorized and legitimate TOE users receive the VAD required to use the signature generation TOE functionality.

15.2. Security Requirements Rationale

15.2.1. Security Requirements coverage

[94] There is one additional security objective (security objective for the Non-IT environment), OE.OP_Phase.

The additional objective is covered to Non-IT environment security requirements as shown in the following completion of table 6.3 of [SSCD_PP]. With this completion the ST fully complies with [SSCD PP] [6] § 6.3.1.

Environment Security Requirement / Environment Security objectives	**OE.CGA_QCert**	**OE.HI_VAD**	**OE.SCA_Data_Intend**	**OE.SVD_Auth_CGA**	**OE.OP_Phase**
FCS_CKM.2/CGA	x				
FCS_CKM.3/CGA	x				
FCS_COP.1/SCA Hash			x		
FDP_UIT.1/SVD Import				x	
FTP_ITC.1/SVD Import				x	
FDP_UIT.1/SCA DTBS			x		
FTP_ITC.1/SCA DTBS			x		
FTP_TRP.1/SCA		x			
R.Sigy_Name	x				
R.Administrator_Guide					x
R.Sigy_Guide					x

[95] This Security Target includes one additional TOE security functional requirement **FMT_SMF.1** in 12.1.5.6. This Security Target fully complies with [SSCD PP] [6] § 6.3.1 with the following line added to the table 6.2 in [SSCD PP] [6] § 6.3.1.

TOE Security Functional Requirement / TOE Security objectives	OT.EMESEC_Design	OT.Lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FMT_SMF.1			√	√							√	

15.2.2. TOE Security Requirements sufficiency

[96] This Security Target fully complies with [SSCD PP] [6] § 6.3.2.1 with the additions to the justification for **OT.Init**, **OT.SCD_Secrecy** and **OT.Sigy_SigF** to reflect the additional TOE security functional requirement **FMT_SMF.1**

[97] **OT.Init (SCD/SVD generation):** The management specification for Identification and Authentication and access control is provided by **FMT_SMF.1**

[98] **OT.SCD_Secrecy (Secrecy of signature-creation data):** The management specification for Identification and Authentication and access control is provided by **FMT_SMF.1**

[99] **OT.Sigy_SigF (Signature generation function for the legitimate signatory only):** The management specification for Identification and Authentication and access control is provided by **FMT_SMF.1**

[100] This Security Target fully complies with [SSCD PP] [6] § 6.3.2.2 with the following addition, the justification for **OE.OP_Phase**

OE.OP_Phase adresse the requirements to the S.Admin, S.User and S.Signatory in the TOE's non-IT environment throughout the TOE's operational phase to ensure the security of the TOE itself, of personalization data to be loaded into the TOE and of related verification authentication data (VAD). These requirements are included in the particular guidance documents and followed by the subject roles as provided by **R.Administrator_Guide** and **R.Sigy_Guide**.

15.2.3. Rationale for extensions

[101] As for [SSCD PP] [6] § 6.6

15.2.4. Assurance Requirements Suitability

[102] According to [SSCD PP] [6], the target assurance level is EAL4 augmented by AVA_MSU.3 and AVA_VLA.4 assurance components.

[103] The TOE includes the ST19WR66I ICC HW platform, which is evaluated against [PP9806] [7] and BSI-PP-002-2001 with assurance level EAL5 augmented by AVA_VLA.4, ADV_MSU.3 and ALC_DVS.2 assurance components.

Table 6 summarizes the assurance measures assignment.

TOE Security Assurance Requirements			Assurance Measures Document Delivery Reference
ASE		Security Target	TOUCH&SIGN2048_ST
ADV	FSP.2	Fully defined external interfaces	TOUCH&SIGN2048_FSP
	HLD.2	Security enforcing high-level design	TOUCH&SIGN2048 HLD
	IMP.1	Subset of the implementation of the TSF	TOUCH&SIGN2048_IMP
	LLD.1	Descriptive low-level design	TOUCH&SIGN2048_LLD
	RCR.1	Informal correspondence demonstration	TOUCH&SIGN2048_RCR
	SPM.1	Informal TOE security policy model	TOUCH&SIGN2048_SPM
ACM	AUT.1	Partial CM automation	TOUCH&SIGN2048_ACM_ConfigurationList TOUCH&SIGN2048_ACM_PLAN
	CAP.4	Generation support and acceptance procedures	
	SCP.2	Problem tracking CM coverage	
ADO	DEL.2	Detection of modification	TOUCH&SIGN2048_ADO
	IGS.1	Installation, generation, and start-up procedures	
AGD	ADM.1	Administrator guidance	TOUCH&SIGN2048_AG
	USR.1	User guidance	
ALC	DVS.1	Identification of security measures	TOUCH&SIGN2048_ALC_DVS_GSP TOUCH&SIGN2048_ALC_DVS_LSP
	LCD.1	Developer defined life-cycle model	TOUCH&SIGN2048_ALC_LCD
	TAT.1	Well-defined development tools	TOUCH&SIGN2048_ALC_TAT
ATE	COV.2	Analysis of coverage	TOUCH&SIGN2048_ATE_DPT TOUCH&SIGN2048_ATE_SF_AC_VTD TOUCH&SIGN2048_ATE_SF_AUTH_VTD TOUCH&SIGN2048_ATE_SF_DATA_ERASE_VTD TOUCH&SIGN2048_ATE_SF_EXCEPTION_VTD TOUCH&SIGN2048_ATE_SF_HASH_VTD TOUCH&SIGN2048_ATE_SF_INT_A_VTD TOUCH&SIGN2048_ATE_SF_KEY_GEN_VTD TOUCH&SIGN2048_ATE_SF_LIFE_CYCLE_VTD TOUCH&SIGN2048_ATE_SF_MAC_VTD TOUCH&SIGN2048_ATE_SF_OBS_A_VTD TOUCH&SIGN2048_ATE_SF_RAD_VTD TOUCH&SIGN2048_ATE_SF_SIGN_VTD TOUCH&SIGN2048_ATE_SF_SM_VTD TOUCH&SIGN2048_ATE_SF_TEST_VTD TOUCH&SIGN2048_ATE_SF_TRANSACTION_VTD
	DPT.1	Testing: high-level design	
	FUN.1	Functional testing	

	IND.2	Independent testing – sample	TOUCH&SIGN2048_ATE_SF_TRANSACTION_VTD TOUCH&SIGN2048_ATE_TSR TOUCH&SIGN2048_ATE_VTP
AVA	AVA_MSU.3	Analysis and testing for insecure states	TOUCH&SIGN2048_MSU
	AVA_SOF.1	Strength of TOE security function evaluation	TOUCH&SIGN2048_SOF
	AVA_VLA.4	Highly resistant	TOUCH&SIGN2048_VLA

Table 6: Assurance Measures assignment

15.3. TOE Summary Specification Rationale

[104] The TOE summary specification rationale is intended to show that the TOE security functions and assurance measures are suitable to meet the TOE security (functional and assurance) requirements.

[105] To show that the selection of TOE security functions and assurance measures are suitable to meet TOE security requirements (functional and assurance), it is important to demonstrate the following:

[106] 1) that the combination of specified TOE IT security functions work together so as to satisfy the TOE security functional requirements;

[107] 2) that the strength of TOE function claims made are valid, or that assertions that such claims are unnecessary are valid.

[108] 3) that the claim is justified that the stated assurance measures are compliant with the assurance requirements.

15.3.2. *TOE Security Functions rationale*

Following Tables demonstrates that TOE Security Functions address at least one SFR and that for each SFR the TOE Security Functions are suitable to meet the SFR, and the combination of TOE Security functions work together so as to satisfy the SFR:

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
FCS	CKM.1.1	[109] **SF.KEY_GEN** grants the FCS_CKM.1.1 satisfaction specifying that the TOE correctly internally generate the SCD/SVD key pair of length 1024 or 2048 bit in modulus-exponent or CRT representation for the RSA algorithms. [110] **SF.HARDWARE** contributes to FCS_CKM.1.1 satisfaction. The function acts as a support mechanism in the SCD/SVD key pair generation.
	CKM.4.1	[111] **SF.DATA_ERASE** grants the FCS_CKM.4.1 satisfaction specifying that the TOE correctly erase the data before allocation and after deallocation of sensitive data. Once the data are erased from memory is not more possible to retrieve them.
	COP.1.1/CORRESP	[112] **SF.KEY_GEN** grants the FCS_COP.1.1/CORRESP satisfaction specifying that the TOE moreover to correctly produce RSA SCD/SVD key pair of length 1024 or 2048 bit, performs a check to verify the SCD/SVD correspondence. [113] **SF.HARDWARE** contributes to FCS_CKM.1.1 satisfaction. The function acts as a support mechanism in the SCD/SVD key pair correspondence check.
	COP.1.1/SIGNING	[114] **SF.SIGN** grants the FCS_COP.1.1/SIGNING satisfaction specifying that the TOE correctly perform a digital signature generation using a key of length 1024 or 2048 bit and the RSA algorithms. [115] **SF.HASH** contributes to FCS_COP.1.1/SIGNING satisfaction. This function generates a hashing of data, using the algorithm SHA-1.or SHA-256. SOF-High claim of SF.HASH is adequate for FCS_COP.1.1/SIGNING according to [32]. [116] **SF.HARDWARE** contributes to FCS_CKM.1.1 satisfaction. The function acts as a support mechanism in the digital signature generation processing.
FDP	ACC.1.1 SVD Transfer SFP	[117] **SF.AC** contributes to FDP_ACC.1.1 SVD Transfer SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed transfer SVD for certification purposes. This function compares the security status required to process the command and allows or denies the SVD transfer. [118] **SF.AUTH** grants the FDP_ACC.1.1 SVD Transfer SFP satisfaction. This function addresses the user authentication by the TOE allowing or denying the SVD transfer. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACC.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [119] **SF.RAD** contributes to FDP_ACC.1.1 SVD Transfer SFP satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	ACC.1.1 Initialization SFP	[120] **SF.AC** contributes to FDP_ACC.1.1 Initialization SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed generate the SCD/SVD key pair. This function compares the security status required to process the command and allows or denies the SCD/SVD key pair generation. [121] **SF.AUTH** grants the FDP_ACC.1.1 Initialization SFP satisfaction. This function addresses the user authentication by the TOE allowing or denying the SCD/SVD key pair generation. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACC.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [122] **SF.RAD** contributes to FDP_ACC.1.1 Initialization SFP satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.
	ACC.1.1 Personalization SFP	[123] **SF.AC** contributes to FDP_ACC.1.1 Personalization SFP satisfaction. The function specifies that, during TOE Operational phase only to the “Administrator” is allowed create the RAD$_S$. This function compares the security status required to process the command and allows or denies the RAD$_S$ creation. [124] **SF.AUTH** grants the FDP_ACC.1.1 Personalization SFP satisfaction. This function addresses the “Administrator” authentication by the TOE allowing or denying the RAD$_S$ creation. The “Administrator” authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACC.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [125] **SF.RAD** contributes to FDP_ACC.1.1 Personalization SFP satisfaction. The function acts as a support mechanism in the “Administrator” authentication process. The function performs a match between a VAD and the RAD$_A$ stored in the TOE. The function is executed in a secure manner.
	ACC.1.1 Signature Creation SFP	[126] **SF.AUTH** grants the FDP_ACC.1.1 Signature Creation SFP satisfaction. The function grants that only to the “Signatory” is allowed to sign the DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication. Moreover this function addresses the “Signatory” authentication by the TOE allowing or denying the DTBS sign functionality. The “Signatory” authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACC.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [127] **SF.AC** contributes to FDP_ACC.1.1 Signature Creation SFP satisfaction. The function specifies that, during TOE Operational phase only to the “Signatory” is allowed sign DTBS-representation. This function compares the security status required to process the command and allows or denies the DTBS-representation signing. [128] **SF.RAD** contributes to FDP_ACC.1.1 Signature Creation SFP satisfaction. The function acts as a support mechanism in the “Signatory” authentication process. The function performs a match between a VAD and the RADs stored in the TOE. The function is executed in a secure manner.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	ACF.1.1 Initialization SFP	[129] **SF.AC** contributes to FDP_ACF.1.1 Initialization SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed generate the SCD/SVD key pair. This function compares the security status required to process the command and allows or denies the SCD/SVD key pair generation.
	ACF.1.2 Initialization SFP	[130] **SF.AC** contributes to FDP_ACF.1.2 Initialization SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed generate the SCD/SVD key pair. This function compares the security status required to process the command and allows or denies the SCD/SVD key pair generation. [131] **SF.AUTH** grants the FDP_ACF.1.2 Initialization SFP satisfaction. This function addresses the user authentication by the TOE allowing or denying the SCD/SVD key pair generation. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [132] **SF.RAD** contributes to FDP_ACF.1.2 Initialization SFP satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.
	ACF.1.3 Initialization SFP	[133] **SF.AC** contributes to FDP_ACF.1.3 Initialization SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed generate the SCD/SVD key pair. This function compares the security status required to process the command and allows or denies the SCD/SVD key pair generation.
	ACF.1.4 Initialization SFP	[134] **SF.AC** contributes to FDP_ACF.1.4 Initialization SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed generate the SCD/SVD key pair. This function compares the security status required to process the command and allows or denies the SCD/SVD key pair generation. [135] **SF.AUTH** grants the FDP_ACF.1.4 Initialization SFP satisfaction. This function addresses the user authentication by the TOE allowing or denying the SCD/SVD key pair generation. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [136] **SF.RAD** contributes to FDP_ACF.1.4 Initialization SFP satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.
	ACF.1.1 SVD Transfer SFP	[137] **SF.AC** grants the FDP_ACF.1.1 SVD Transfer SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed transfer SVD for certification purposes. This function compares the security status required to process the command and allows or denies the SVD transfer.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	ACF.1.2 SVD Transfer SFP	[138] **SF.AC** contributes to FDP_ACF.1.2 SVD Transfer SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed transfer SVD for certification purposes. This function compares the security status required to process the command and allows or denies the SVD transfer. [139] **SF.AUTH** grants the FDP_ACF.1.2 SVD Transfer SFP satisfaction. This function addresses the user authentication by the TOE allowing or denying the SVD transfer. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [140] **SF.RAD** contributes to FDP_ACF.1.2 SVD Transfer SFP satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.
	ACF.1.3 SVD Transfer SFP ACF.1.4 SVD Transfer SFP	[141] **SF.AC** grants the FDP_ACF.1.3 SVD Transfer SFP and FDP_ACF.1.4 SVD Transfer SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed transfer SVD for certification purposes. This function compares the security status required to process the command and allows or denies the SVD transfer.
	ACF.1.1 Personalization SFP	[142] **SF.AC** grants to FDP_ACF.1.1 Personalization SFP satisfaction. The function specifies that, during TOE Operational phase only to the “Administrator” is allowed create the RAD_S. This function compares the security status required to process the command and allows or denies the RAD_S creation.
	ACF.1.2 Personalization SFP	[143] **SF.AC** contributes to FDP_ACF.1.2 Personalization SFP satisfaction. The function specifies that, during TOE Operational phase only to the “Administrator” is allowed create the RAD_S. This function compares the security status required to process the command and allows or denies the RAD_S creation. [144] **SF.AUTH** grants the FDP_ACF.1.2 Personalization SFP satisfaction. This function addresses the “Administrator” authentication by the TOE allowing or denying the RAD_S creation. The “Administrator” authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [145] **SF.RAD** contributes to FDP_ACF.1.2 Personalization SFP satisfaction. The function acts as a support mechanism in the “Administrator” authentication process. The function performs a match between a VAD and the RAD_A stored in the TOE. The function is executed in a secure manner.
	ACF.1.3 Personalization SFP ACF.1.4 Personalization SFP	[146] **SF.AC** grants to FDP_ACF.1.3 Personalization SFP and FDP_ACF.1.4 Personalization SFP satisfaction. The function specifies that, during TOE Operational phase only to the “Administrator” is allowed create the RAD_S. This function compares the security status required to process the command and allows or denies the RAD_S creation.
	ACF.1.1 Signature Creation SFP	[147] **SF.AC** grants to FDP_ACF.1.1 Signature Creation SFP satisfaction. The function specifies that, during TOE Operational phase only to the “Signatory” is allowed sign DTBS-representation. This function compares the security status required to process the command and allows or denies the DTBS-representation signing.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	ACF.1.2 Signature Creation SFP	[148] **SF.AUTH** grants the FDP_ACF.1.2 Signature Creation SFP satisfaction. The function grants that only to the "Signatory" is allowed to sign the DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication. Moreover this function addresses the "Signatory" authentication by the TOE allowing or denying the DTBS sign functionality. The "Signatory" authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1.because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [149] **SF.AC** contributes to FDP_ACF.1.2 Signature Creation SFP satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed sign DTBS-representation. This function compares the security status required to process the command and allows or denies the DTBS-representation signing. [150] **SF.RAD** contributes to FDP_ACF.1.2 Signature Creation SFP satisfaction. The function acts as a support mechanism in the "Signatory" authentication process. The function performs a match between a VAD and the RADs stored in the TOE. The function is executed in a secure manner. [151] **SF.HARDWARE** contributes to FDP_ACF.1.2 Signature Creation SFP satisfaction. The function acts as a support mechanism in the SCA authentication processing.
	ACF.1.3 Signature Creation SFP	[152] **SF.AC** grants to FDP_ACF.1.3 Signature Creation SFP satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed sign DTBS-representation. This function compares the security status required to process the command and allows or denies the DTBS-representation signing.
	ACF.1.4 Signature Creation SFP	[153] **SF.AUTH** grants the FDP_ACF.1.4 Signature Creation SFP satisfaction. The function grants that only to the "Signatory" is allowed to sign the DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication. Moreover this function addresses the "Signatory" authentication by the TOE allowing or denying the DTBS sign functionality. The "Signatory" authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [154] **SF.AC** contributes to FDP_ACF.1.4 Signature Creation SFP satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed sign DTBS-representation. This function compares the security status required to process the command and allows or denies the DTBS-representation signing. [155] **SF.RAD** contributes to FDP_ACF.1.4 Signature Creation SFP satisfaction. The function acts as a support mechanism in the "Signatory" authentication process. The function performs a match between a VAD and the RADs stored in the TOE. The function is executed in a secure manner. [156] **SF.HARDWARE** contributes to FDP_ACF.1.4 Signature Creation SFP satisfaction. The function acts as a support mechanism in the SCA authentication processing.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	ETC.1.1 SVD Transfer	[157] **SF.AUTH** grants the FDP_ETC.1.1 SVD Transfer satisfaction. The function grants that the SVD is transferred only towards an authorized CGA. This function addresses the CGA authentication. No security attributes is transferred or visible externally to the TCS. [158] **SF.HARDWARE** contributes to FDP_ETC.1.1 SVD Transfer satisfaction. The function acts as a support mechanism in the CGA authentication processing.
	ETC.1.2 SVD Transfer	[159] **SF.AUTH** grants the FDP_ETC.1.2 SVD Transfer satisfaction. The function grants that the SVD is transferred only towards an authorized CGA. This function addresses the CGA authentication. No security attributes is transferred or visible externally to the TCS. [160] **SF.HARDWARE** contributes to FDP_ETC.1.2 SVD Transfer satisfaction. The function acts as a support mechanism in the CGA authentication processing.
	ITC.1.1. DTBS	[161] **SF.AUTH** grants the FDP_ITC.1.1 DTBS satisfaction. The function grants that the TOE signs only DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication. [162] **SF.HARDWARE** contributes to FDP_ITC.1.1. DTBS satisfaction. The function acts as a support mechanism in the SCA authentication processing.
	ITC.1.2. DTBS	[163] **SF.AUTH** grants the FDP_ITC.1.2 DTBS satisfaction. The function grants that the TOE signs only DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication. [164] **SF.HARDWARE** contributes to FDP_ITC.1.2. DTBS satisfaction. The function acts as a support mechanism in the SCA authentication processing.
	ITC.1.3. DTBS	[165] **SF.AUTH** grants the FDP_ITC.1.3 DTBS satisfaction. The function grants that the TOE signs only DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication. [166] **SF.HARDWARE** contributes to FDP_ITC.1.3. DTBS satisfaction. The function acts as a support mechanism in the SCA authentication processing.
	RIP.1.1	[167] **SF.DATA_ERASE** grants the FDP_RIP.1.1 satisfaction making unavailable any residual information related to the SCD/RAD/VAD.This function erase the sensitive data before starting a new working session, before allocation and after deallocation.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	SDI.2.1. Persistent	[168] **SF.INT_A** grants the FDP_SDI.2.1 Persistent satisfaction. This function addresses the TOE data integrity. When an integrity error is found an exception rises. The TOE aborts the current operation and may change the TOE life cycle state. The TOE notifies the abnormal condition externally. [169] **SF.EXCEPTION** contributes to FDP_SDI.2.1 Persistent satisfaction. The function acts as a support mechanism for the TOE's internal data integrity. The function addresses the exception management. [170] **SF.LIFE_CYCLE** contributes to FDP_SDI.2.1 Persistent satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes. [171] **SF.HARDWARE** contributes to FDP_SDI.2.1 Persistent satisfaction. The function acts as a support mechanism in the data integrity detection and reporting of exception events.
	SDI.2.2. Persistent	[172] **SF.INT_A** grants the FDP_SDI.2.2 Persistent satisfaction. This function addresses the TOE data integrity. When an integrity error is found an exception rises. The TOE aborts the current operation and may change the TOE life cycle state. The TOE notifies the abnormal condition externally. [173] **SF.EXCEPTION** contributes to FDP_SDI.2.2 Persistent satisfaction. The function acts as a support mechanism for the TOE's internal data integrity. The function addresses the exception management. [174] **SF.LIFE_CYCLE** contributes to FDP_SDI.2.2 Persistent satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes. [175] **SF.HARDWARE** contributes to FDP_SDI.2.2 Persistent satisfaction. The function acts as a support mechanism in the reporting of exception events related to operating condition and internal data integrity failures.
	SDI.2.1. DTBS	[176] **SF.SM** grants the FDP_SDI.2.1 DTBS satisfaction. The DTBS integrity is checked before its use. When an integrity error is found the TOE aborts the current operation and notifies the condition externally. The SOF-High claim of SF.SM is adequate for FDP_SDI.2.1 DTBS because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful DTBS integrity attack. [177] **SF.MAC** contributes to FDP_SDI.2.1 DTBS satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [178] **SF.HARDWARE** contributes to FDP_SDI.2.1 DTBS satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	SDI.2.2. DTBS	[179] **SF.SM** grants the FDP_SDI.2.2 DTBS satisfaction. The DTBS integrity is checked before its use. When an integrity error is found the TOE aborts the current operation and notifies the condition externally. The SOF-High claim of SF.SM is adequate for FDP_SDI.2.2 DTBS because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful DTBS integrity attack. [180] **SF.MAC** contributes to FDP_SDI.2.2 DTBS satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [181] **SF.HARDWARE** contributes to FDP_SDI.2.2 DTBS satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.
	UIT.1.1 SVD Transfer	[182] **SF.SM** grants the FDP_UIT.1.1 SVD Transfer satisfaction. To prevent the data to be altered the TOE protects the transmitted data using integrity and authentication mechanisms. The SOF-High claim of SF.SM is adequate for FDP_ UIT.1.1 SVD Transfer because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful SVD integrity attack. [183] **SF.MAC** contributes FDP_UIT.1.1 SVD Transfer satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [184] **SF.HARDWARE** contributes to FDP_UIT.1.1 SVD Transfer satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.
	UIT.1.2 SVD Transfer	[185] **SF.SM** grants the FDP_UIT.1.2 SVD Transfer satisfaction. To prevent the data to be altered the TOE protects the transmitted data using integrity and authentication mechanisms. The SOF-High claim of SF.SM is adequate for FDP_ UIT.1.2 SVD Transfer because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful SVD integrity attack. [186] **SF.MAC** contributes FDP_UIT.1.2 SVD Transfer satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [187] **SF.HARDWARE** contributes to FDP_UIT.1.2 SVD Transfer satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	UIT.1.1 TOE DTBS	[188] **SF.SM** grants the FDP_UIT.1.1 TOE DTBS satisfaction. The DTBS integrity is checked before its use. When an integrity error is found the TOE aborts the current operation and notifies the condition externally. The SOF-High claim of SF.SM is adequate for FDP_UIT.1.1 TOE DTBS because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful DTBS integrity attack. [189] **SF.MAC** contributes to FDP_UIT.1.1 TOE DTBS satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [190] **SF.HARDWARE** contributes to FDP_UIT.1.1 TOE DTBS satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.
	UIT.1.2 TOE DTBS	[191] **SF.SM** grants the FDP_UIT.1.2 TOE DTBS satisfaction. The DTBS integrity is checked before its use. When an integrity error is found the TOE aborts the current operation and notifies the condition externally. The SOF-High claim of SF.SM is adequate for FDP_UIT.1.2 TOE DTBS because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful DTBS integrity attack. [192] **SF.MAC** contributes to FDP_UIT.1.2 TOE DTBS satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [193] **SF.HARDWARE** contributes to FDP_UIT.1.2 TOE DTBS satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.
FIA	AFL.1.1	[194] **SF.AUTH** grants the FIA_AFL.1.1 satisfaction. This function addresses the user authentication. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [195] **SF.RAD** contributes to FIA_AFL.1.1 satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	AFL.1.2	[196] **SF.AUTH** grants the FIA_AFL.1.2 satisfaction. This function addresses the user authentication. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [197] **SF.RAD** contributes to FIA_AFL.1.2 satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. When the user authentication attempts reach the 3 consecutive retries then the relevant RAD is blocked. The function is executed in a secure manner.
	ATD.1.1	[198] **SF.AC** grants the FIA_ATD.1.1 satisfaction. This function specifies that it is possible define in the TOE, relate to each user profile, security attributes based on RAD. These attributes are valid and active for the whole TOE Operational phase.
	UAU.1.1	[199] **SF.AUTH** grants the FIA_UAU.1.1 satisfaction. The TOE requires that a user is successfully identified and authenticated before allowing any command execution on behalf of that user. In particular, before identifying and authenticating a user, the TOE allows only the execution of an ***"AUTHENTICATION"*** command in order to establish a trusted channel/path. The SOF-High claim of SF.AUTH is adequate for FIA_UAU.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
	UAU.1.2	[200] **SF.AUTH** grants the FIA_UAU.1.2 satisfaction. The TOE requires that a user is successfully identified and authenticated before allowing any command execution on behalf of that user. In particular, before identifying and authenticating a user, the TOE allows only the execution of an ***"AUTHENTICATION"*** command in order to establish a trusted channel/path. The SOF-High claim of SF.AUTH is adequate for FIA_UAU.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
	UID.1.1	[201] **SF.AUTH** grants the FIA_UID.1.1 satisfaction. The TOE requires that a user is successfully identified and authenticated before allowing any command execution on behalf of that user. In particular, before identifying and authenticating a user, the TOE allows only the execution of an ***"AUTHENTICATION"*** command in order to establish a trusted channel/path. The SOF-High claim of SF.AUTH is adequate for FIA_UID.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
	UID.1.2	[202] **SF.AUTH** grants the FIA_UID.1.2 satisfaction. The TOE requires that a user is successfully identified and authenticated before allowing any command execution on behalf of that user. In particular, before identifying and authenticating a user, the TOE allows only the execution of an ***"AUTHENTICATION"*** command in order to establish a trusted channel/path. The SOF-High claim of SF.AUTH is adequate for FIA_UID.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
FMT	MOF.1.1.	[203] **SF.AC** grants the FMT_MOF.1.1 satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed sign DTBS-representation. This function compares the security status required to process the command and allows or denies the DTBS-representation signing.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	MSA.1.1 Administrator	[204] **SF.AC** grants the FMT_MSA.1.1 Administrator satisfaction. The function specifies that, during TOE Operational phase only to the "Administrator" is allowed the management of the SCD/SVD security attributes. This function compares the security status required to process the command and allows or denies the SCD/SVD security attributes management.
	MSA.1.1 Signatory	[205] **SF.AC** grants the FMT_MSA.1.1 Signatory satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed to change in ***"active"*** the operational state of the SCD. This function compares the security status required to process the command and allows or denies the SCD operational state change.
	MSA.2.1	[206] **SF.AC** grants the FMT_MSA.2.1 satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed to set and change security attributes. Moreover the function specifies that the security attribute change is possible only when the change doesn't compromise the TOE security state. This function compares the security status required to process the command and allows or denies the set or the change of the security attributes.
	MSA.3.1	[207] **SF.AC** grants the FMT_MSA.3.1 satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed to set and change security attributes. This function compares the security status required to process the command and allows or denies the set or the change of the security attributes. When the SCD is generated the authorized user shall set the SCD's security attribute "SCD operational" to "no".
	MSA.3.2	[208] **SF.AC** grants the FMT_MSA.3.2 satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed to set and change security attributes. This function compares the security status required to process the command and allows or denies the set or the change of the security attributes. At object creation time the "Administrator" decides the security attributes related to the created object.
	MTD.1.1	[209] **SF.AUTH** grants the FMT_MTD.1.1 satisfaction. The function grants that only to the "Signatory is allowed change the RAD$_S$. This function addresses the "Signatory" authentication by the TOE allowing or denying the RAD change functionality. The "Signatory" authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FMT_MTD.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [210] **SF.AC** contributes to FMT_MTD.1.1 satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed change the RAD$_S$. This function compares the security status required to process the command and allows or denies the change of the RAD$_S$. [211] **SF.RAD** contributes to FMT_MTD.1.1 satisfaction. The function acts as a support mechanism in the "Signatory" authentication process. The function performs a match between a VAD and the RADs stored in the TOE. The function is executed in a secure manner.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	SMF.1.1	[212] **SF.AUTH** grants the FMT_SMF.1.1 satisfaction. The function specifies that, during TOE Operational phase a user must be successfully identified and authenticated before allowing any command execution on behalf of that user. [213] **SF.AC** contributes to the FMT_SMF.1.1 satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed to have access to TOE's resources. Each TOE's resources has security attributes assigned. This function compares the security status required to process the command on the relevant TOE's resource and allows or denies the execution of the command.
	SMR.1.1	[214] **SF.AC** grants the FMT_SMR.1.1 satisfaction. The function specifies that, during TOE Operational phase only to users with role set to "Signatory" or "Administrator" is allowed to interact with the TOE
	SMR.1.2	[215] **SF.AC** grants the FMT_SMR.1.2 satisfaction. The function specifies that, during TOE Operational phase only to users with role set to "Signatory" or "Administrator" is allowed to interact with the TOE.
FPT	AMT.1.1	[216] **SF.TEST** grants the FPT_AMT.1.1 satisfaction This function specifies that, during the whole TOE Operational phase, at each TOE start-up, a suit of TOE's internal components tests are performed.
	EMSEC.1.1	[217] **SF.OBS_A** grants the FPT_EMESEC.1.1 satisfaction. This function assures that, during the whole TOE Operational phase, the TOE will not emit electrical signals that an attacker can easily exploit to gain access to the RAD and SCD stored in the TOE. This function is mainly implemented by IC platform mechanisms. [218] **SF.HARDWARE** contributes to FPT_EMESEC.1.1 satisfaction. The function acts as support mechanism preventing sensititive data to be disclose.
	EMSEC.1.2	[219] **SF.OBS_A** grants the FPT_EMESEC.2.1 satisfaction. This function assures that, during the whole TOE Operational phase, the TOE will not permit the user to gain access to the RAD and SCD stored in the TOE through external physical contacts. [220] **SF.HARDWARE** contributes to FPT_EMESEC.1.2 satisfaction. The function acts as support mechanism preventing sensititive data to be disclose.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	FLS.1.1	[221] **SF.TEST** grants the FPT_FLS.1.1 satisfaction. This function is mainly implemented by IC platform mechanisms. The function assures that the TOE is operative only when the physical operating parameters are in the accepted range. On test fail an exception rises. The TOE aborts the current operation and may change the TOE life cycle state. [222] **SF.EXCEPTION** contributes to FPT_FLS.1.1 satisfaction. The function acts as a support mechanism for the TOE's operating condition and internal data integrity. The function addresses the exception management. [223] **SF.LIFE_CYCLE** contributes to FPT_FLS.1.1 satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes. [224] **SF.TRANSACTION** contributes to FPT_FLS.1.1 satisfaction. The function acts as a support mechanism. The function addresses the atomicity of the TOE transactions. [225] **SF.HARDWARE** contributes to FPT_FLS.1.1 satisfaction. The function acts as a support mechanism in the reporting of exception events related to operating condition and internal data integrity failures.
	PHP.1.1	[226] **SF.TEST** grants the FPT_PHP.1.1 satisfaction. This function detects the TOE chip integrity violation. When an integrity error is detected an exception rises. The TOE aborts the current operation and may change the TOE life cycle state. [227] **SF.INT_A** contributes to FPT_PHP.1.1 satisfaction. This function addresses the TOE data integrity. [228] **SF.EXCEPTION** contributes to FPT_PHP.1.1 satisfaction. The function acts as a support mechanism for the TOE's operating condition and internal data integrity. The function addresses the exception management. [229] **SF.LIFE_CYCLE** contributes to FPT_PHP.1.1 satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes. [230] **SF.HARDWARE** contributes to FPT_PHP.1.1 satisfaction. The function acts as a support mechanism in the reporting of exception events related to operating condition and internal data integrity failures.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	PHP.1.2	[231] **SF.TEST** grants the FPT_PHP.1.2 satisfaction. This function detects the TOE chip integrity violation. When an integrity error is detected an exception rises. The TOE aborts the current operation and may change the TOE life cycle state. [232] **SF.INT_A** contributes to FPT_PHP.1.2 satisfaction. This function addresses the TOE data integrity. [233] **SF.EXCEPTION** contributes to FPT_PHP.1.2 satisfaction. The function acts as a support mechanism for the TOE's operating condition and internal data integrity. The function addresses the exception management. [234] **SF.LIFE_CYCLE** contributes to FPT_PHP.1.2 satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes. [235] **SF.HARDWARE** contributes to FPT_PHP.1.2 satisfaction. The function acts as a support mechanism in the reporting of exception events related to operating condition and internal data integrity failures.
	PHP.3.1	[236] **SF.TEST** grants the FPT_PHP.3.1 satisfaction. This function detects the TOE environmental physical operating conditions. When a physical operating condition is detected out the range an exception rises. The TOE aborts the current operation and may change the TOE life cycle state. [237] **SF.EXCEPTION** contributes to FPT_PHP.3.1 satisfaction. The function acts as a support mechanism for the TOE's operating condition and internal data integrity. The function addresses the exception management. [238] **SF.LIFE_CYCLE** contributes to FPT_PHP.3.1 satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes. [239] **SF.HARDWARE** contributes to FPT_PHP.3.1 satisfaction. The function acts as a support mechanism in the reporting of exception events related to operating condition and internal data integrity failures.
	TST.1.1	[240] **SF.TEST** grants the FPT_TST.1.1 satisfaction. This function executes a suite of tests to establish the correct functionality of the TOE. The tests are executed at TOE power-up or before/after sensitive operations.
	TST.1.2	[241] **SF.INT_A** grants the FPT_TST.1.2 satisfaction. This function addresses the TOE integrity as well the TSF code and data integrity. When an integrity error is found the TOE notifies the condition externally. The authorized users are aware about the abnormal TOE condition. [242] **SF.HARDWARE** contributes to FPT_TST.1.2 satisfaction. The function acts as a support mechanism in the detection of TOE data integrity failures.
	TST.1.3	[243] **SF.INT_A** grants the FPT_TST.1.3 satisfaction. This function addresses the TOE integrity as well the TSF code and data integrity. When an integrity error is found the TOE notifies the condition externally. The authorized users are aware about the abnormal TOE condition. [244] **SF.HARDWARE** contributes to FPT_TST.1.2 satisfaction. The function acts as a support mechanism in the detection of TOE data integrity failures.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
FTP	ITC.1.1 SVD Transfer	[245] **SF.AUTH** grants the FTP_ITC.1.1 SVD Transfer satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product CGA. This function addresses the CGA authentication. [246] **SF.SM** grants the FTP_ITC.1.1 SVD Transfer satisfaction. The function establishes a trusted channel with a remote IT product CGA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure. The SOF-High claim of SF.SM is adequate for FTP_ITC.1.1 SVD Transfer because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful attacks to the confidentiality and integrity of the exchanged data. [247] **SF.MAC** contributes to FTP_ITC.1.1 SVD Transfer satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [248] **SF.HARDWARE** contributes to FTP_ITC.1.1 SVD Transfer satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.
	ITC.1.2 SVD Transfer	[249] **SF.AUTH** grants the FTP_ITC.1.2 SVD Transfer satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product CGA. This function addresses the CGA authentication. After positive authentication the data communication can start via the trusted channel. [250] **SF.SM** grants the FTP_ITC.1.2 SVD Transfer satisfaction. The function establishes a trusted channel with a remote IT product CGA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure. The SOF-High claim of SF.SM is adequate for FTP_ITC.1.2 SVD Transfer because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful attacks to the confidentiality and integrity of the exchanged data. [251] **SF.MAC** contributes to FTP_ITC.1.2 SVD Transfer satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [252] **SF.HARDWARE** contributes to FTP_ITC.1.2 SVD Transfer satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	ITC.1.3 SVD Transfer	[253] **SF.AUTH** grants the FTP_ITC.1.3 SVD Transfer satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product CGA. This function addresses the CGA authentication. After positive authentication the data communication can start via the trusted channel. The trusted channel can be used to export the SVD. [254] **SF.SM** grants the FTP_ITC.1.3 SVD Transfer satisfaction. The function establishes a trusted channel with a remote IT product CGA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure. The SOF-High claim of SF.SM is adequate for FTP_ITC.1.3 SVD Transfer because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful attacks to the confidentiality and integrity of the exchanged data. [255] **SF.MAC** contributes to FTP_ITC.1.3 SVD Transfer satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [256] **SF.HARDWARE** contributes to FTP_ITC.1.3 SVD Transfer satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.
	ITC.1.1 DTBS Import	[257] **SF.AUTH** grants the FTP_ITC.1.1 DTBS Import satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product SCA. This function addresses the SCA authentication. [258] **SF.SM** grants the FTP_ITC.1.1 DTBS Import satisfaction. The function establishes a trusted channel with a remote IT product SCA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure. The SOF-High claim of SF.SM is adequate for FTP_ITC.1.1 DTBS Import because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful attacks to the confidentiality and integrity of the exchanged data. [259] **SF.MAC** contributes to FTP_ITC.1.1 DTBS Import satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [260] **SF.HARDWARE** contributes to FTP_ITC.1.1 DTBS Import satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	ITC.1.2 DTBS Import	[261] **SF.AUTH** grants the FTP_ITC.1.2 DTBS Import satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product SCA. This function addresses the SCA authentication. After positive authentication the data communication can start via the trusted channel. [262] **SF.SM** grants the FTP_ITC.1.2 DTBS Import satisfaction. The function establishes a trusted channel with a remote IT product SCA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure. The SOF-High claim of SF.SM is adequate for FTP_ITC.1.2 DTBS Import because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful attacks to the confidentiality and integrity of the exchanged data. [263] **SF.MAC** contributes to FTP_ITC.1.2 DTBS Import satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [264] **SF.HARDWARE** contributes to FTP_ITC.1.2 DTBS Import satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.
	ITC.1.3 DTBS Import	[265] **SF.AUTH** grants the FTP_ITC.1.3 DTBS Import satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product SCA. This function addresses the SCA authentication. After positive authentication the data communication can start via the trusted channel. The trusted channel can be used to import the DTBS. [266] **SF.SM** grants the FTP_ITC.1.3 DTBS Import satisfaction. The function establishes a trusted channel with a remote IT product SCA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure. The SOF-High claim of SF.SM is adequate for FTP_ITC.1.3 DTBS Import because secure channel functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful attacks to the confidentiality and integrity of the exchanged data. [267] **SF.MAC** contributes to FTP_ITC.1.3 DTBS Import satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [268] **SF.HARDWARE** contributes to FTP_ITC.1.3 DTBS Import satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	TRP.1.1 TOE	[269] **SF.AUTH** grants the FTP_TRP.1.1 TOE satisfaction. The function grants that the TOE establishes a trusted path with a local user. This function addresses the user authentication. [270] **SF.SM** grants the FTP_TRP.1.1 TOE satisfaction. The function establishes a trusted path with a local user. The function assures that the data exchanged on the trusted path are protected against modifications or disclosure. The SOF-High claim of SF.SM is adequate for FTP_TRP.1.1 TOE because trusted path functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful attacks to the confidentiality and integrity of the exchanged data. [271] **SF.MAC** contributes to FTP_TRP.1.1 TOE satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [272] **SF.HARDWARE** contributes to FTP_TRP.1.1 TOE satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.
	TRP.1.2 TOE	[273] **SF.AUTH** grants the FTP_TRP.1.2 TOE satisfaction. The function grants that the TOE establishes a trusted path with a local user. This function addresses the user authentication. After positive authentication the data communication can start via the trusted path. [274] **SF.SM** grants the FTP_TRP.1.2 TOE satisfaction. The function establishes a trusted path with a local user. The function assures that the data exchanged on the trusted path are protected against modifications or disclosure. The SOF-High claim of SF.SM is adequate for FTP_TRP.1.2 TOE because trusted path functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful attacks to the confidentiality and integrity of the exchanged data. [275] **SF.MAC** contributes to FTP_TRP.1.2 TOE satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [276] **SF.HARDWARE** contributes to FTP_TRP.1.2 TOE satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	TRP.1.3 TOE	[277] **SF.AUTH** grants the FTP_TRP.1.3 TOE satisfaction. The function grants that the TOE establishes a trusted path with a local user. This function addresses the user authentication. After positive authentication the data communication can start via the trusted path. The trusted path can be used to exchange data related to the user authentication e.g. the user PIN. [278] **SF.SM** grants the FTP_TRP.1.3 TOE satisfaction. The function establishes a trusted path with a local user. The function assures that the data exchanged on the trusted path are protected against modifications or disclosure. The SOF-High claim of SF.SM is adequate for FTP_TRP.1.3 TOE because trusted path functionality based on TripleDES algorithm with 2 or 3 keys combined with a maximum authentication failure counter related to the secure channel authentication key with initial value set to 3, prevents from successful attacks to the confidentiality and integrity of the exchanged data. [279] **SF.MAC** contributes to FTP_TRP.1.3 TOE satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES, the Triple DES and the AES-128 algorithms. [280] **SF.HARDWARE** contributes to FTP_TRP.1.3 TOE satisfaction. The function acts as support mechanism during the useage of symmetric crypto algorithms.

Table 7: Functional requirements and TOE security function rational

TOE Security Functions		I & A		Key and Crypto				Stored Data Protection				TST, FAIL, LIFE CYCLE, AC, SM,HW					
		SF.AUTH	SF.RAD	SF.KEY_GEN	SF.HASH	SF.MAC	SF.SIGN	SF.OBS_A	SF.INT_A	SF.DATA_ERASE	SF.TRANSACTION	SF.TEST	SF.EXCEPTION	SF.LIFE_CYCLE	SF.AC	SF.SM	SF.HARDWARE
FCS	CKM.1.1			√													√
	CKM.4.1									√							
	COP.1.1 corresp			√													√
	COP.1.1 signing				√		√										√
FDP	ACC.1.1 SVD Transfer SFP	√	√												√		
	ACC.1.1 Initialization SFP	√	√												√		
	ACC.1.1 Personalization SFP	√	√												√		
	ACC.1.1 Sign. Creation SFP	√	√												√		
	ACF.1.1 Initialization SFP														√		
	ACF.1.2 Initialization SFP	√	√												√		
	ACF.1.3 Initialization SFP														√		
	ACF.1.4 Initialization SFP	√	√												√		
	ACF.1.1 SVD Transfer SFP														√		
	ACF.1.2 SVD Transfer SFP	√	√												√		
	ACF.1.3 SVD Transfer SFP														√		
	ACF.1.4 SVD Transfer SFP														√		
	ACF.1.1 Personalization SFP														√		
	ACF.1.2 Personalization SFP	√	√												√		
	ACF.1.3 Personalization SFP														√		
	ACF.1.4 Personalization SFP														√		
	ACF.1.1 Sign. Creation SFP														√		
	ACF.1.2 Sign. Creation SFP	√	√												√		√
	ACF.1.3 Sign. Creation SFP														√		
	ACF.1.4 Sign. Creation SFP	√	√												√		√
	ETC.1.1 SVD Transfer	√															√
	ETC.1.2 SVD Transfer	√															√
	ITC.1.1. DTBS	√															√
	ITC.1.2. DTBS	√															√
	ITC.1.3. DTBS	√															√
	RIP.1.1									√							
	SDI.2.1. Persistent								√				√	√			√
	SDI.2.2. Persistent								√				√	√			√
	SDI.2.1. DTBS					√										√	√
	SDI.2.2. DTBS					√										√	√
	UIT.1.1 SVD Transfer					√										√	√
	UIT.1.2 SVD Transfer					√										√	√
	UIT.1.1 TOE DTBS					√										√	√
	UIT.1.2 TOE DTBS					√										√	√

Table 8: Functional requirements to TOE security functions mapping

		I & A		KEY AND CRYPTO				STORED DATA PROTECTION				TST, FAIL, LIFE CYCLE, AC, SM, HW					
		SF.AUTH	SF.RAD	SF.KEY_GEN	SF.HASH	SF.MAC	SF.SIGN	SF.OBS_A	SF.INT_A	SF.DATA_ERASE	SF.TRANSACTION	SF.TEST	SF.EXCEPTION	SF.LIFE_CYCLE	SF.AC	SF.SM	SF.HARDWARE
FIA	AFL.1.1	√	√														
	AFL.1.2	√	√														
	ATD.1.1														√		
	UAU.1.1	√															
	UAU.1.2	√															
	UID.1.1	√															
	UID.1.2	√															
FMT	MOF.1.1														√		
	MSA.1.1 Administrator														√		
	MSA.1.1 Signatory														√		
	MSA.2.1														√		
	MSA.3.1														√		
	MSA.3.2														√		
	MTD.1.1	√	√												√		
	SMF.1.1	√													√		
	SMR.1.1														√		
	SMR.1.2														√		
FPT	AMT.1.1											√					
	EMSEC.1.1							√									√
	EMSEC.1.2							√									√
	FLS.1.1										√	√	√	√			√
	PHP.1.1								√			√	√	√			√
	PHP.1.2								√			√	√	√			√
	PHP.3.1											√	√	√			√
	TST.1.1											√					
	TST.1.2								√								√
	TST.1.3								√								√
FTP	ITC.1.1 SVD Transfer	√				√										√	√
	ITC.1.2 SVD Transfer	√				√										√	√
	ITC.1.3 SVD Transfer	√				√										√	√
	ITC.1.1 DTBS Import	√				√										√	√
	ITC.1.2 DTBS Import	√				√										√	√
	ITC.1.3 DTBS Import	√				√										√	√
	TRP.1.1 TOE	√				√										√	√
	TRP.1.2 TOE	√				√										√	√
	TRP.1.3 TOE	√				√										√	√

Table 9: Functional requirements to TOE security functions mapping (continued)

15.4. TOE Strength of Function claim

The TSF SF.AUTH, SF.SM, SF.HASH and SF.HARDWARE have a SOF claim “high”. All the other TSF have no SOF claim statement.

15.5. PP claims Rationale

[281] The chapter 5 lists all of the SFRs included in this security target; this list includes all of the SFRs identified in the [SSCD PP] [6]. All of the operations applied to the SFRs are in accordance with the requirements of the [SSCD PP] [6].

15.6. Functional Requirements Dependencies

[282] This Security Target fully complies with [SSCD PP] [6] § 6.4. To reflect the additional TOE security functional requirement **FMT_SMF.1** the following additional dependencies are defined and completely fulfilled:

FMT_MOF.1: FMT_SMF.1 Specification of Management Functions

FMT_MSA.1: FMT_SMF.1 Specification of Management Functions

FMT_MTD.1: FMT_SMF.1 Specification of Management Functions