STMicroelectronics

J-SIGN Security Target Public Version

Common Criteria for IT security evaluation

J-SIGN_Security_Target_Lite Rev. A
April 2015

life.augmented

BLANK

J-SIGN SecurityTarget
Public Version

Common Criteria for IT Evaluation

1. INTRODUCTION

1.1 Document Reference

Document identification: **J-Sign Security Target - Public Version**
Revision: **A**
Registration: J-SIGN_Security_Target _Lite_A

1.2 Security Target Reference

Document identification: J-SIGN Security Target
Revision: **G**
Registration: J-SIGN_Security_Target_G

1.3 TOE Reference

TOE Name and Version: J-SIGN V1.8.4

2. PURPOSE

This document presents the Security Target lite of J-SIGN a smartcard application implementing a SSCD type 3 and CIE/CNS application (Italian identity and service citizen card see [CIE] [CNS]) designed as a Java card 3.0.4 applet integrated on STMicroelectronics J-SAFE java card platform designed on the STMicroelectronics ST23 SB23YR80B ICC (ST23YR80 Security Integrated Circuit with dedicated software and embedded cryptographic library).

This document is a sanitized version of the Security Target used for the evaluation. It is classified as public information.

INDEX

List of tables

List of figures

3. REFERENCE DOCUMENTS

[ST23_DS]	ST23YR80 Data Sheet – Rev.2 June 2010
[JSIGN_ST]	J-SIGN Security Target – Rev-G 9-Feb-2015
[GAZETTE_FNAE]	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)
[DIRECTIVE_93]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 3. July 2009. CCMB-2009-07-001.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 3. July 2009. CCMB-2009-07-002.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 3. July 2009. CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 3. July 2009. CEM-2009-07-004.
[ALGO_EC]	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. V.2.1 Oct. 19th 2001
[SSCD_PP]	CWA 14169 - Annex C Protection Profile-Secure Signature - Creation Device Type 3, version: 1.05, EAL4+, March 2002 (BSI-PP-0006-2002 EAL 4+).
[PP_9806]	Protection Profile PP9806 -Smartcard - Integrated Circuit, version: 2.0, EAL4+, September 1998.
[CWA_14355]	CWA 14355- Guidelines for the implementation of Secure Signature - Creation Devices version 0.91, Dec 17, 2001.

[ISO_7816_3] ISO/IEC 7816 Part 3 Signal and transmission protocols Second Edition 1997

[ISO_7816_4] ISO/IEC 7816 Part 4 Interindustry commands for interchange Edition 2005

[ISO_7816_5] ISO/IEC 7816 Part 5 Numbering System and registration procedure for application identifiers First Edition 1994

[ISO_7816_8] ISO/IEC 7816 Part 8 Security related interindustry commands Edition 1998

[ISO_7816_9] ISO/IEC 7816 Part 9 Additional interindustry commands and security attributes First Edition 2001

[ISO_14443_2] SO/IEC 14443-2 Identification Cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal – 2001-07-1

[ISO_14443_3] ISO/IEC 14443-3 Identification cards – Contactless integrated circuit(s) card – Proximity cards – Part 3: Initialization and anticollision First edition 2001-02-01

[ISO_14443_4] ISO/IEC 14443-4 Identification Card – Contactless integrated circuit card – Proximity card – part 4 – Transmission Protocol – 1/02/2001

[ISO_14888_3] ISO/IEC 14888-3 Information technology - Security techniques - Digital signatures with appendix - Part 3 : Certificate-based mechanisms 15-12-1999

[ISO_9797] ISO/IEC 9797-1 Information technology - Security techniques – Message Authentication Codes (MACs) - Part 1 : Mechanisms using a block cipher - First Edition 15-12-1999

[FIPS_PUB113] FIPS 113: Computer Data Authentication (FIPS PUB 113), NIST, 30 May 1985

[BSI_AIS31] 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

[FIPS_PUB180_1] FIPS 180-1: Secure Hash Standard (FIPS PUB 180-1), NIST, 17 April 1995

[FIPS_PUB180_2] FIPS 180-2: Secure Hash Standard 1 August 2002

[PKCS1_v1_5] PKCS #1 v1.5: RSA Encryption Standard – RSA Laboratories – 1 Nov 1993

[RFC3447] NWG Request For Comments 3447 – February 2003

[FIPS_PUB_186-3] FIPS PUB 186-3: Digital Signature Standard – June 2009

[FIPS_PUB46] FIPS PUB 46-3: Data Encryption Standard – 5 Oct 1999

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

[JSAFE_ST] J-Safe on SB23YR80B Security Target – Revision: G, January 2015

[PP_JC_Closed] Java Card System – Closed Configuration Protection Profile, Version 2.6, August 25th 2010

[STlite_SB23] SA23YR48B / SB23YR48B / SA23YR80B / SB23YR80B SECURITY TARGET - PUBLIC VERSION, Rev. 2.01, November 2009

[MntRep_SB23] Secured microcontrollers SA23YR48/80B and SB23YR48/80B, including the cryptographic libraries NesLib v2.0 or v3.0, in SA or SB configurations – Maintenance Report ANSSI-2010/02-M01, 19th March 2010

[CNS] CNS – Carta Nazionale dei Servizi – Functional Specification V1.1.6 – 02/04/2011

[CIE] CIE – Carta di Identità Elettronica – Functional Specification V2.1 – 26/07/2011

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

4. DEFINITIONS

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	STMicroelectronics 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 SA.
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.
Personal Identification Number (PIN)	Value transmitted from the smartcard reader to J-SIGN 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 J-SIGN 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 0
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 J-SIGN this is synonym of PIN.

ACRONYMS	DEFINITION
AC	Access Conditions
BSO	Base Security Object
CC	Common Criteria
CIE	Carta d'Identità Elettronica (Electronic Identity Card for Italian citizen)
CGA	Certificate Generation Application
CNS	Carta Nazionale Servizi (National Services Card for Italian citizen)
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 0
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
SSCD (the TOE)	Secure Signature Creation Device
SSCD PP	Protection Profile 0
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

5. J-SIGN SECURITY TARGET

5.1 Conventions

The document follows the rules and conventions laid out in “Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model Version 3.1, Annex B “Specification of Security Targets” [CC1].
This Security target lite (ST) is compliant to Protection Profile - Secure Signature Creation Device Type 3, version: 1.05, 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 the document [ALGO_EC].

5.2 ST and TOE Reference

(1) This Security target lite provides a complete and consistent statement of the security enforcing functions and mechanisms of J-SIGN (hereafter referred to as the TOE, i.e. the Target of Evaluation).

(2) The Security target lite details the TOE security requirements and the countermeasures proposed to address the perceived threats to the assets protected by the TOE.

Here are the labelling and descriptive information necessary to control and identify the ST and the TOE to which it refers.

ST Reference	
Title:	J-SIGN - Security Target Lite
Assurance Level:	EAL 4 augmented with AVA_VAN.5.
Company:	ST Microelectronics srl
CC Version:	3.1 [CC1][CC2][CC3]
PP Conformance:	SSCD Protection Profile Type 3 [SSCD_PP].
Version:	Rev-A 02-April-2015
General Status:	final release
Related ST:	[JSAFE_ST] [STlite_SB23] [JSAFE_ST]

TOE reference	J-SIGN V1.8.4

5.3 TOE Overview

(3) J-SIGN is the composition of a javacard applet with a java card platform J-SAFE.

(4) J-SIGN is a smartcard application implementing a type 3 Secure Signature-Creation Device as described in [SSCD_PP] and CIE/CNS application (Italian identity and service citizen card see [CIE] [CNS]) designed as a Java Card 3.0.4 applet integrated on STMicroelectronics J-SAFE V2.11.0 java card platform designed on the STMicroelectronics ST23 SB23YR80B ICC product (from now on also referenced as J-SAFE).

(5) Main J-SIGN functionalities cover the 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
- ♦ 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) J-SIGN is a Java applet integrated on STMicroelectronics J-SAFE java card 3.0.4 platform designed on the STMicroelectronics secure microcontroller: SB23YR80B ICC.

(7) J-SAFE provides the following main features:

- Communication protocols:
  - o T=0
  - o T=1
  - o T=CL (contact-less)

- Cryptographic algorithms and services:
  - o DES / 3-DES
  - o AES (up to 256 bits)
  - o RSA with key generation (up to 2048 bits)
  - o SHA-1, SHA-224, SHA-256, SHA-512
  - o EC over GF(p) in the range between 160 and 521 bits
  - o Secure random number generation

J-SAFE is based on Java card 3.0.4 Classic Edition and GlobalPlatform 2.1.1 providing the related API.

J-SAFE platform also includes a set of proprietary API providing optimized services for handling integrity of application-specific sensitive data. The proprietary functionalities are Secure Storage API (integrity-protected arrays), Secure comparison of byte arrays, Generation of random primes and multi transaction.

J-SAFE platform also includes an Operating System component which provides memory management functions, I/O functions that are compliant with ISO standards, transaction facilities and secure (native) implementation of cryptographic functions

J-SAFE java card platform is under evaluation/certification with French scheme and the security target is [JSAFE_ST]

(8) The STMicroelectronics secure microcontroller: SB23YR80B ICC is a hardware platform offering 390Kb 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, EC, DES, TripleDES, AES). The hardware includes a public key cryptographic processor NESCRYPT able to handle operands up to 4096 bits, and a DES accelerator, both designed to speed up cryptographic calculations. The hardware also includes a true random number generator (TRNG) compliant to P2 class of [BSI_AIS31]. 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
The SB23YR80B Secured Microcontroller with Cryptographic Library has been certified by ANSSI (cert. report ANSSI-CC-2010/02) with assurance level EAL6+: its associated Security Target Lite is [STlite_SB23] and the applicable Maintenance Report is [MntRep_SB23].

6. TOE DESCRIPTION

(9) This section of the ST describes the TOE and its security requirements. The scope and boundaries of the TOE are described in general terms both at physical (hardware and/or software components/modules) and at logical level (IT and security features offered by the TOE).

6.1 Product type

(10) The Target Of Evaluation (TOE) is a composite-TOE which is the Secure Signature Creation Device (SSCD type3) with the J-SAFE platform defined by:

- The SSCD type 3 with CIE/CNS Application J-SIGN
- The J-SAFE Java card 3.0.4 platform with the components:
  - o Card Manager (This component and its interface is permanently disabled before TOE delivery. The Card Manager is out of scope of current evaluation)
  - o GP API (This interface is permanently disabled before TOE delivery and it is out of scope of current evaluation)
  - o Javacard 3.0.4 API
  - o Proprietary API
  - o Operating System
  - o The Secured Microcontroller with Cryptographic Library STMicroelectronics ST23 SB23YR80B ICC
- User and Administrator guidance

6.2 TOE functionalities

(11) J-SIGN 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):

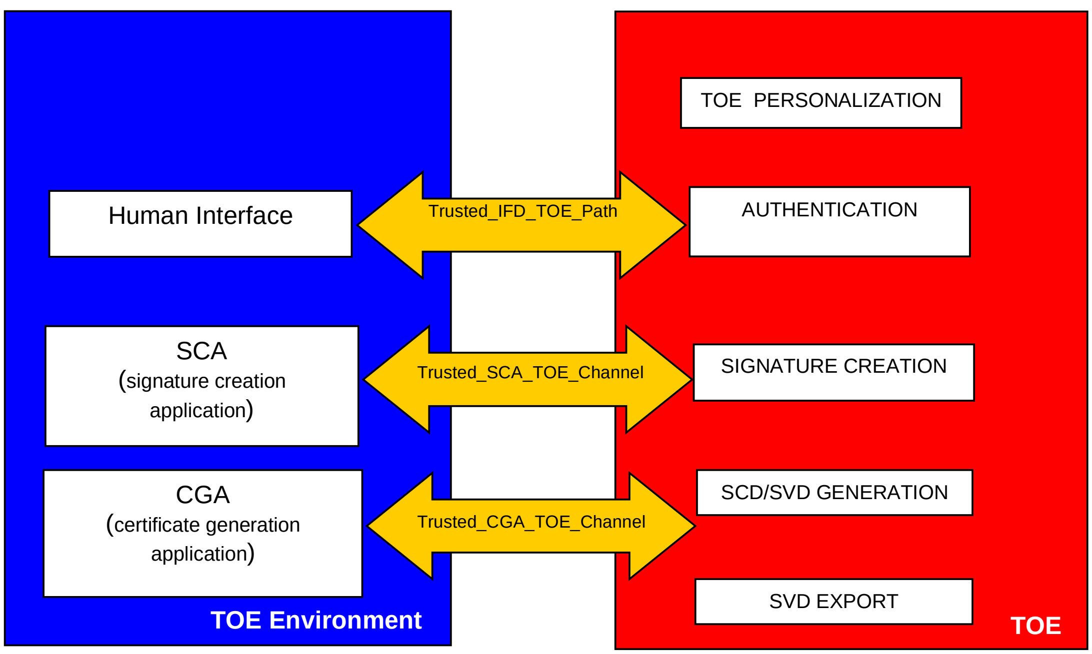


Figure 1: TOE environment and boundaries

(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 TOE User and Administrator Guidance. During TOE personalization, the administrator is responsible for J-SIGN File System creation and configuration via a Personalization application. See 6.3 for more details.

(14) After personalization, the TOE is ready to be:

- Securely used for signature under exclusive 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 and/or import its own signature keys (the SCD/SVD pair); in case of RSA key pair generation, the TOE only generates RSA keys in CRT format. When a RSA key is imported in the TOE and used for signature operation, the RSA key shall be in CRT format with the public exponent otherwise the TOE couldn't work properly. An authorized Administrator uses the CGA to initiate SCD/SVD generation and to ask the SSCD to export the SVD for the 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 CRT and EC cryptographic algorithms and parameters agreed as suitable according to [ALGO_EC][PKCS1_v1_5][RFC3447].

(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 Signatory and/or the Administrator can change his Reference Authentication Data (RAD) stored in the TOE

(20) The Administrator can unblock the Signatory's Reference Authentication Data, when needed

(21) 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]).

(22) 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 [ALGO_EC].

(23) As depicted in the figure 2, J-SIGN SSCD type 3 application is structured as a javacard applet, in which Software functionalities are implemented as APDU commands compliant with ISO/IEC 7816-part 4 and 8 (see [ISO_7816_4][ISO_7816_8])

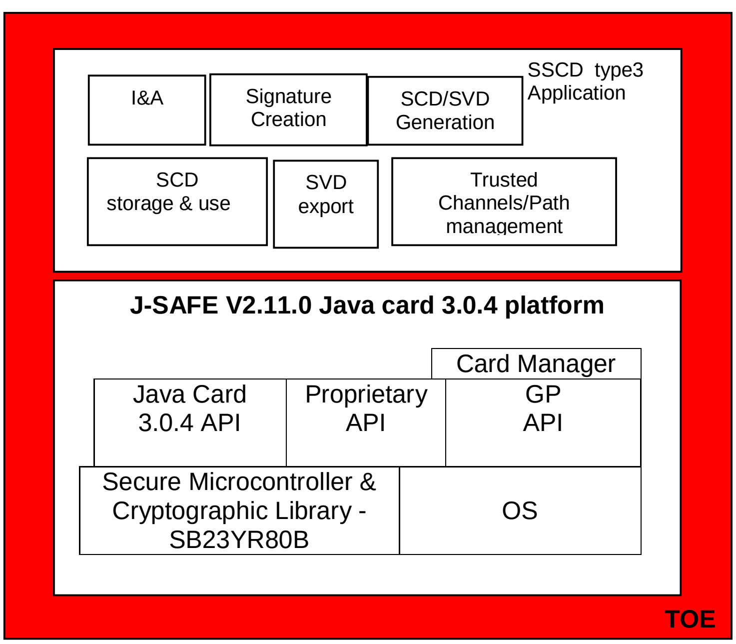


Figure 2: TOE components

6.3 TOE life cycle

(24) The typical TOE lifecycle is shown in Figure 3. Basically, it consists of a design and development phase and an operational phase. The Figure 3 also shows the correspondence between the TOE states and the states as reported in [SSCD PP].

(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.

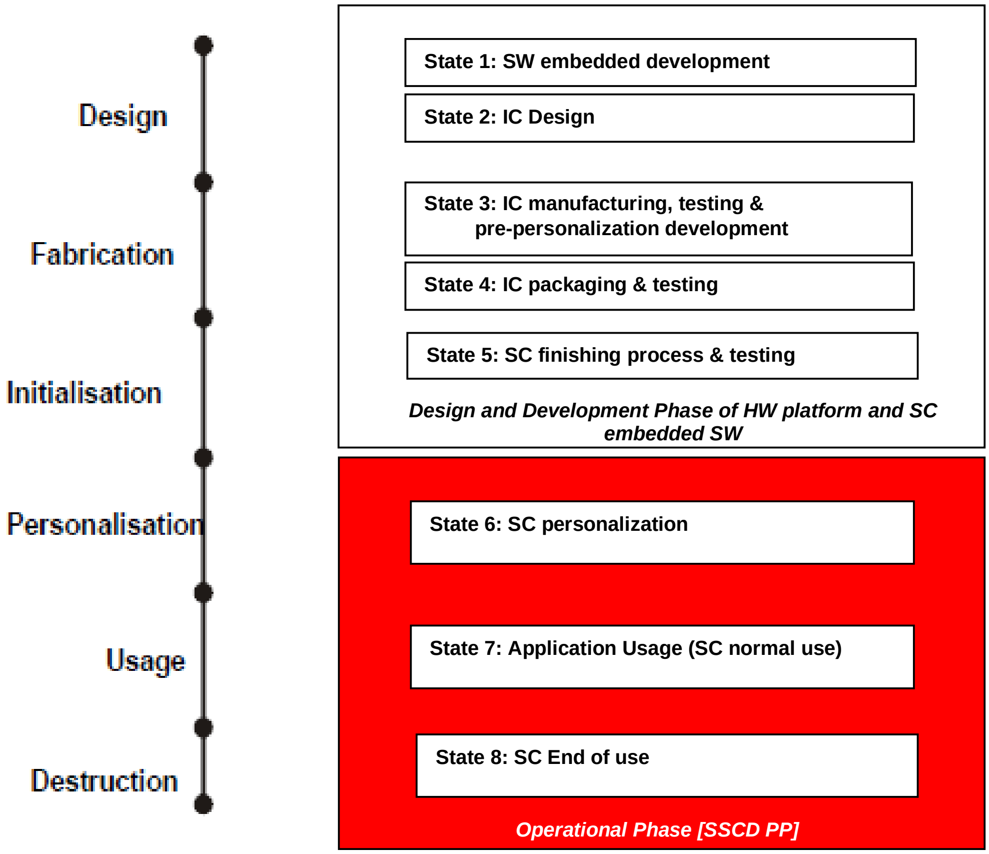


Figure 3: TOE life cycle

(26) The TOE implements a mechanism in order to recognize its operational phase.

(27) The TOE states 1 **“SW embedded development”** and 2 **“IC Design”** correspond to the **“Design”** state in [SSCD PP].

(28) The TOE is delivered from chip manufacturer (ST Microelectronics Rousset) to card manufacturer (ST Microelectronics Marcianise) after the completion of the state 4 **“IC Packaging and & Testing“** which with the state 3 **“IC Manufacturing, testing and pre-personalization development“** are part of the **“Fabrication”** state in [SSCD PP].

(29) 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.

(30) The state 5 **“SC finishing process & Testing”** is managed by card manufacturer. This state corresponds to the **“Initialization”** state in [SSCD PP]. In this state the TOE J-SIGN applet is installed and configured, eventually patches and/or code extensions are loaded in memory and finally a typical structure of the TOE file system can be loaded in the TOE memory according to TOE Administration Guidance. At completion of finishing process step, the TOE operational phase can be entered.

(31) The TOE operational phase starts after J-SIGN applet Java card 3.0.4 platform J-SAFE and its HW platform SB23YR80B have been successfully designed, developed, manufactured, tested and initialized.

(32) The TOE is in *SC personalization* state at the beginning of TOE Operational phase.

(33) 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. This state corresponds to the **“Personalization”** state in [SSCD PP].

(34) Moreover, in the state 6 **“SC personalization“** the TOE administrator is in particular responsible for:

- Changing the default administrator 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 certificate generation 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

(35) After completion of **“SC personalization“** state, the administrator put the TOE in state 7 **“SC Normal use”**, where the TOE can be used either by the Signatory or the Administrator.

(36) 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

This state corresponds to the **“Usage”** state in [SSCD PP].

(37) 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

(38) When a failure occurs in state 7 **“SC Normal use”**, the TOE manages the fault and, according to the severity of the fault, entering 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 SSCD application is no more available;

- In all other cases in which the failure is recovered, the TOE remains in the state 7 **"SC Normal use"**.

(39) The state 8 **"SC end of use"** of the TOE corresponds to the **"Destruction"** state in [SSCD PP].

6.4 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 gives 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.

6.5 TOE Environment

6.5.1 Development and Production Environment

(40) The TOE described in this ST is developed in the following environments:

STATE	DESCRIPTION	RESPONSIBLE	ENVIRONMENT
1	Embedded Software (OS and application) Development	Card Manufacturer	STMicroelectronics Marcianise (CE) Italy
2	IC Design	Chip Manufacturer	STMicroelectronics Rousset, France STMicroelectronics Singapore STMicroelectronics Zaventem
3	IC manufacturing and testing	Chip Manufacturer	STMicroelectronics Rousset, France
4	IC Packaging and testing	Chip Manufacturer	STMicroelectronics or other qualified packaging manufacturer
5	SC finishing process & testing	Card Manufacturer	STMicroelectronics Marcianise (CE) Italy
6	SC personalization	TOE Administrator	STMicroelectronics Marcianise (CE) Italy or other qualified personalization center or Certification authority.

6.6 CC conformance claim

This ST is conformant with Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model Version 3.1 [CC1].

This ST is conformant with Common Criteria for Information Technology Security Evaluation – Part 2: Security Functional Components Version 3.1 [CC2] with extension "FPT_EMSEC.1" made in the SSCD Protection Profile [SSCD_PP].

This ST is conformant with Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Components Version 3.1 [CC3] package EAL with augmentation AVA_VAN.5.

This ST is strict conformant to the SSCD Protection Profile [SSCD_PP] with the addition of FMT_SMF.1.

The TOE assurance level claim is EAL 4 augmented with AVA_VAN.5.

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

The TOE is conformant with Common Criteria Version 3.1 part 2 and part 3 [CC2][CC3].

7. TOE SECURITY ENVIRONMENT

(41) Following paragraphs describe the security aspects of the environment in which the TOE is intended to be used.

7.1 Assets

(42) With regard to J-SIGN implementation, assets that need to be protected by the TOE are here defined according to [SSCD_PP]. 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 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.
SCF	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.
ES	Electronic signature	Not forgery (Integrity).

7.2 Subjects

(43) In [SSCD_PP] 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.

7.3 Threat agents

(44) In [SSCD_PP] 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**.

7.4 Assumptions

ASSUMPTION	DEFINITION
A.CGA	*Trustworthy certification-generation application* The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.
A.SCA	*Trustworthy signature-creation application* The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

7.5 Organizational Security Policies

(45) As defined in [SSCD_PP] and with the addition of **P.PERSONALIZATION, P.MANAGEMENT and P.VAD,** are here reported for clarity.

OSP	DEFINITION
P.CSP_QCert	*Qualified certificate* The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information
P.QSign	*Qualified electronic signatures* The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate (according to directive Annex 1) and is created by the TOE.
P.Sigy_SSCD	*TOE as secure signature-creation device* The TOE implements the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once
P.PERSONALIZATION	*TOE Personalization* The 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 the 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.

P.MANAGEMENT	*TOE Management* 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.
P.VAD	*TOE VAD* The information needed for the positive identification and authentication by the TOE of the final user are delivered to the TOE final users in a secure manner.

7.6 Threats to Security

(46) Threats are here reported for clarity as they are defined in [SSCD_PP].

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.

8. SECURITY OBJECTIVES

8.1 Security objectives for the TOE

(47) Following table summarizes which are the security objectives for the TOE, as they are defined in [SSCD_PP].

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. **NOTE**: no specific limits are definable at this stage but it is reasonable assume as "specified limit" for a physical signal (Icc, VDC, Clock, EM field) an operating range within which the TOE works properly without data leakage. These physical signals are managed directly in the Secured Microcontroller SB23YR80B ICC and by J-SAFE java card platform [ST23_DS],[STlite_SB23],[MntRep_SB23],[JSAFE_ST]
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. **NOTE**: The Secured Microcontroller SB23YR80B ICC provides physical tampering detection to protect internal non-volatile memory [ST23_DS],[STlite_SB23],[MntRep_SB23].
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.

8.2 Security objectives for the environment

As defined in [SSCD_PP] and here reported for clarity

OE.CGA_QCert	*Generation of qualified certificates* The CGA generates qualified certificates which include inter alia a) the name of the signatory controlling the TOE, b) the SVD matching the SCD implemented in the TOE under sole control of the signatory c) the advanced signature of the CSP
OE.SVD_Auth_CGA	*CGA verifies the authenticity of the SVD* The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate
OE.HI_VAD	*Protection of the VAD* If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.
OE.SCA_Data_Intend	*Data intended to be signed* The SCA a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE, b) sends the DTBS-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE c) attaches the signature produced by the TOE to the data or provides it separately

8.3 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

9. IT SECURITY REQUIREMENTS

(48) Here are defined the security functional and assurance requirements that the TOE and the supporting environment for its evaluation need to satisfy in order to meet the security objectives for the TOE.

9.1 TOE Security Functional Requirement

(49) 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 protection profile [SSCD_PP].

(50) The table below lists each TOE Security Functional Requirement (SFR) included in this Security target lite 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]..

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_SMF.1.1 [1]	Specification of Management Functions	×			
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

(51) This paragraph fully restates TOE security functional requirements (see [SSCD_PP]) for clarity: operations completed in this ST are shown in ***bold italics***.

[1] This SFR is an addition to the protection profile [SSCD_PP].

(52)	**Cryptographic support (FCS)**	
(53)	**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 ***RSAGEN1*** and specified cryptographic key sizes ***of 1024 and 2048 bits*** that meet the following: [ALGO_EC] par. 4.5.2.2. Moreover the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***ECGEN1*** and specified cryptographic key sizes of ***160,192,224,256,384 and 512 bits*** that meet the following: [ALGO_EC] par. 4.5.4.2.
(54)	**Cryptographic key destruction (FCS_CKM.4)**	
	FCS_CKM.4.1[2]	The TSF shall destroy cryptographic keys in case of regeneration of a new SCD in accordance with a specified cryptographic key destruction method ***irreversible deletion from the memory of the stored key value*** that meets the following standard ***none***.
(55)	**Cryptographic operation (FCS_COP.1)**	
	FCS_COP.1.1/CORRESP RSA	The TSF shall perform SCD/SVD correspondence verification in accordance with a specified cryptographic algorithm ***RSA CRT*** and cryptographic key sizes of ***1024 and 2048 bits*** that meet the following: ***RSA CRT*** ([ALGO_EC] par. 4.5.2.1).
	FCS_COP.1.1/CORRESP ECC	The TSF shall perform SCD/SVD correspondence verification in accordance with a specified cryptographic algorithm ***ECDSA-Fp*** and cryptographic key sizes of ***160,192,224,256,384 and 521 bits*** that meet the following: ***ECDSA-Fp*** ([ALGO_EC] par. 4.5.4.1).
	FCS_COP.1.1/SIGNING RSA	The TSF shall perform digital signature-generation in accordance with a specified cryptographic 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*** [PKCS1_v1_5] *and* ***Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 - February 2003*** [RFC3447]**.**
	FCS_COP.1.1/SIGNING ECC	The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm ***ECDSA-Fp*** and specified cryptographic key sizes ***160,192,224,256,384 and 521 bits*** that meet the following: ***ECDSA-Fp*** ([ALGO_EC] par. 4.5.4.1).

[2] 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.

(56)	USER DATA PROTECTION (FDP)	
(57)	**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.
(58)	**Security attribute based access control (FDP_ACF.1)[3]**	
	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.
	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.

[3] 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.1.2/ 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".
(59)	**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.

(60)	**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 TOE.
	FDP_ITC.1.2/DTBS	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
	FDP_ITC.1.3/DTBS[4]	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: DTBS-representation shall be sent by an authorized SCA.
(61)	**Subset residual information protection (FDP_RIP.1)**	

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

	FDP_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.
(62)	**Stored data integrity monitoring and action (FDP_SDI.2)**[5]	
	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.
(63)	**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.

(64)	IDENTIFICATION AND AUTHENTICATION (FIA)	
(65)	**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.
(66)	**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.
(67)	**Timing of authentication (FIA_UAU.1)**	

[5] 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".

	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[6] 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.
(68)	**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.

(69)	**SECURITY MANAGEMENT (FMT)**	
(70)	**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.
(71)	**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.
(72)	**Secure security attributes (FMT_MSA.2)**	
	FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.
(73)	**Static attribute initialization (FMT_MSA.3)**	
	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.
(74)	**Management of TSF data (FMT_MTD.1)**	
	FMT_MTD.1.1	The TSF shall restrict the ability to modify the RAD to Signatory.
(75)	**Specification of Management Functions (FMT_SMF.1)**	

[6] 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_SMF.1.1[7]	The TSF shall be capable of performing the following security management functions: 1. Creation and modification of RAD, 2. Enabling the signature-creation function, 3.Modification of the security attribute SCD/SVD management, SCD operational, 4. Change the default value of the security attribute SCD Identifier,
(76)	**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.

(77)	PROTECTION OF THE TSF (FPT)	
(78)	**Abstract machine testing (FPT_AMT.1)**	
	FPT_AMT.1.1	The TSF shall run a suite of tests *during* ***initial start-up*** and ***periodically during normal operation*** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.
(79)	**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[8]	The TOE shall ensure ***all users*** are unable to use the following interface ***external contacts/contactless*** to gain access to RAD and SCD.
(80)	**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: ***1. power shortage*** ***2. over voltage*** ***3. over and under clock frequency*** 4. ***IC integrity problems***.
(81)	**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.
(82)	**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 SFRs are always enforced
(83)	**TSF Testing (FPT_TST.1)**	

[7] This SFR is an addition to the protection profile [SSCD_PP].

[8] 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.

	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.

(84)	TRUSTED PATH/CHANNELS (FTP)	
(85)	**Inter-TSF trusted channel (FTP_ITC.1)**	
	FTP_ITC.1.1/SVD Transfer	The TSF shall provide a communication channel between itself and another 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 another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
	FTP_ITC.1.2/DTBS Import	The TSF shall permit 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.
(86)	**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***.

9.2 TOE Security Assurance Requirements

(87) TOE assurance requirements are those stated in Table 2.

The assurance requirements of this evaluation are EAL4 augmented by AVA_VAN.5.
The assurance requirements ensure, among others, the security of the TOE during its development and production. We present here the assurance requirements included in the EAL of the ST.

These requirements are covered by this document.

The EAL claimed in this ST (EAL4+ augmentation AVA_VAN.5) is a subset of the EAL claimed in the ST for the platform (EAL5+ Augmentations: ALC_DVS.2 and AVA_VAN.5) [JSAFE_ST].

ASSURANCE CLASS	ASSURANCE COMPONENTS

ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures These SARs ensure proper installation and configuration: the TOE will be properly configured and the TSFs are configured to process as expected
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification ADV_IMP.1 Implementation representation of the TSF ADV_TDS.3 Basic modular design
ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample. The purpose of these SARs is to ensure whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis EAL4 requires for the vulnerability assessment the assurance component AVA_VAN.3. Its aim is to determine whether the TOE, in its intended environment, has vulnerabilities exploitable by attackers with attack potential of enhanced-basic. In order to provide the necessary level of protection, EAL4 is augmented with the component AVA_VAN.5, which requires that the TOE is resistant against attackers processing high attack potential.

Table 2: Assurance Requirements - EAL 4 extended with AVA_VAN.5

9.3 IT Environment Security requirements [9]

[9] The CCv3.1 norm doesn't require to list the SFRs for IT Environment. In the evaluation of the document this chapter can be skipped through.

(88) Following table lists each IT Environment Security Functional Requirement (SFR) included in this Security target lite 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].

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_TRP.1.2/SCA	Trusted Path		×		
FTP_TRP.1.3/SCA	Trusted Path	×	×		

Table 3: Operation performed on ENVIRONMENT SFRs

(89) Following paragraph fully restates security requirements for the IT environment presented in [SSCD_PP].

(90) Numbering of SFRs in this ST is the same proposed in [SSCD_PP]: operations completed in this ST are shown in ***bold italics***.

(91)	CERTIFICATION GENERATION APPLICATION (CGA)	
(92)	**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, DES and Triple DES with 2 or 3 key.***
(93)	**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***.
(94)	**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.
(95)	**Inter-TSF trusted channel (FTP_ITC.1)**	
	FTP_ITC.1.1/ SVD import	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
	FTP_ITC.1.2/ 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.

(96)	SIGNATURE CREATION APPLICATION (SCA)	
(97)	**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*** **[FIPS_PUB180_1][FIPS_PUB180_2]**.

(98)	**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.
(99)	**Inter-TSF trusted channel (FTP_ITC.1)**	
	FTP_ITC.1.1/ SCA DTBS	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
	FTP_ITC.1.2/ 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.
(100)	**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 local user*** 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.***

9.3.1 Non-IT Environment Security requirements

(101) **R.Administrator_Guide** *Application of Administrator Guidance*

The implementation of the requirements of the Directive [DIRECTIVE_93], ANNEX II “Requirements for certification-service-providers issuing qualified certificates”, literal (e), stipulates employees of the CSP or other relevant entities to follow the administrator guidance provided for the TOE. Appropriate supervision of the CSP or other relevant entities shall ensure the ongoing compliance.

(102) **R.Sigy_Guide** *Application of User Guidance*

The SCP implementation of the requirements of the Directive [DIRECTIVE_93], ANNEX II “Requirements for certification-service-providers issuing qualified certificates”, literal (k), stipulates the signatory to follow the user guidance provided for the TOE.

(103) **R.Sigy_Name** *Signatory’s name in the Qualified Certificate*

The CSP shall verify the identity of the person to which a qualified certificate is issued according to the Directive [DIRECTIVE_93], ANNEX II “Requirements for certification-service-providers issuing qualified certificates”, literal (d). The CSP shall verify that this person holds the SSCD which implements the SCD corresponding to the SVD to be included in the qualified certificate.

10. TOE SUMMARY SPECIFICATION

(104) This section contains a high-level specification of each TOE Security Function (TSF) that contributes to satisfaction of the Security Functional Requirements of chapter 9.

(105) 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.

(106) Following table lists the SFRs not mentioned in the [SSCD_PP] but included in this Security target lite.

FMT_SMF.1

(107) The Table 23 shows that all the SFRs are satisfied by at least one TSF and that every TSF is used to satisfy at least one SFR.

10.1 TOE Security Functions

(108) This part lists the TOE Security Functions. In the following TOE platform is intended the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B with embedded library. The TOE Security Functions 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.SIGN	Key Generation Hash computation Signature functions
Secure Messaging	SF.SM	Secure Messaging
Stored Data Protection	SF.OBS_A SF.INT_A SF.DATA_ERASE SF.DATA_UPDATE	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 PLATFORM	SF.PLATFORM	TOE Cryptographic support, TRNG and physical protection

Table 4: List of TOE security functions

10.1.1 Identification and authentication

SF.AUTH
(109) 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 TOE platform which is compliant with [BSI_AIS31]. The internal authenticate requires a challenge generated by the IFD. Both internal and external authentications use Triple DES with 2 or 3 keys, AES or RSA CRT with 512-bit, 768-bit, and 1024-bit key length. An authentication failure counter related to the authentication key is decreased after each unsuccessful authentication, when the counter decrease to zero then 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 [NETLINK]). The crypto algorithm support and random generation is provided by the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B embedded library functionalities included in the TSF SF.PLATFORM.

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
(110) This function controls all operations related to the Reference Authentication Data (RAD) management. It includes the verification, unblock, and change of the RAD. 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. 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. 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. The support for the functionalities related to RAD objects is provided by the J-SAFE Java card 3.0.4 platform

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		

10.1.2 Access Control

SF.AC			
(111) 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**	

10.1.3 Key Management and Cryptography

SF.KEY_GEN
(112) The TSF SF.KEY_GEN implements the following main functions: • SCD/SVD CRT format generation for RSA • SCD/SVD for ECC • SCD/SVD correspondence • SCD/SVD storing This function generates the SCD/SVD pair according to the RSA algorithm (see [ALGO_EC][PKCS1_v1_5][RFC3447]), using a length of 512, 768, 1024 or 2048 bits. The SCD is generated and stored in the TOE in the format: 1. 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. The SVD for RSA algorithm is generated and stored in the TOE in the format **(n, e)** where **n** is the RSA modulus and **e** the RSA public exponent. This function generates the SCD/SVD pair for the ECC algorithm (see [ALGO_EC]), using a key length of sizes of 160,192,224,256,384 and 521 bits. The function checks the SCD/SVD correspondence. The RSA and EC key generation and SCD/SVD correspondence support is provided by the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B embedded library functionalities included in the TSF SF.PLATFORM.

MAPPED TOE SFRs		
FCS		
CKM.1.1		
COP.1.1 correspondence		

SF.HASH		
(113) This function generates a hashing of data, using the algorithm SHA-1 or SHA-256 (see [FIPS_PUB180_1][FIPS_PUB180_2]). 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-1 and SHA-256 algorithm support is provided by the J-SAFE Java card 3.0.4platform and the Integrated Circuit SB23YR80B embedded library functionalities included in the TSF SF.PLATFORM.		
MAPPED TOE SFRs		
FCS		
COP.1.1 signing		

SF.SIGN		
(114) The function signs imported data (DTBS/R), using a RSA with private key length of 1024 or 2048 bits in conformance with the algorithm RSA. The private key is stored in the TOE in CRT format then the Chinese Remainder Theorem method is applied to perform the RSA signature algorithm. The signature is computed applying the scheme RSA PKCS#1 1.5 Block Type 01 and RSASSA-PSS (see [ALGO_EC][PKCS1_v1_5][RFC3447]). The function signs imported data (DTBS/R), using ECC with private key length of 160,192,224,256,384 and 521 bits in conformance with the algorithm ECDSA-Fp (see [ALGO_EC][FIPS_PUB_186-3]). The function is protected against the SPA/DPA/DFA attack The signature algorithm support is provided by the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B embedded library functionalities included in the TSF SF.PLATFORM.		
MAPPED TOE SFRs		
FCS		
COP.1.1 signing		

10.1.4 Secure Messaging

SF.SM	
(115)	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 TOE by ensuring two basic security functions: data confidentiality and data authentication. The confidentiality is obtained by the encipherment of the transmitted message. This operation uses the Triple DES algorithm with 2 or 3 Keys (see [FIPS_PUB46]). The command authentication uses a cryptogram based on MAC. In case of an unsuccessful authentication the command is refused. This operation uses a DES or Triple DES with 2 or 3 keys as defined in the standards [ISO_9797][FIPS_PUB113] to generate and verifie a MAC. 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 function is protected against the SPA/DPA/DFA attack The crypto algorithm support is provided by the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B embedded library functionalities included in the TSF SF.PLATFORM.

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**	

10.1.5 Stored Data Protection

SF.OBS_A	
(116)	This function addresses the TOE emanation security functional requirements. This function provides mechanism to avoid information leakage and data disclosure. 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 [ST23_DS][STlite_SB23][JSAFE_ST]. This function is mostly realized by SB23YR80B Integrated Circuit design and implementation of the TSFs in the J-SAFE Java card 3.0.4 platform. The basic mechanisms required to prevent data disclosure and leakage are provided by the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B embedded library and Hardware functionalities included in the TSF SF.PLATFORM.

MAPPED TOE SFRs		
FPT		
EMSEC.1.1.		
EMSEC.1.2		

SF.INT_A		
(117) This function addresses the TOE physical and 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 and on the severity, 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 die integrity sensors. The device is protected by active shield. If an attempt is made to access the physical layers protected by the shield, and the shield is damaged, the die integrity detector resets the product, as well as destroys the first two EEPROM pages. After the detection of such die integrity attack the TOE enter the “end of use” state. The TSF code integrity is supported by SF.INT_A through the implementation of some check commands. The sensitive data integrity is supported by the TSF and the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B. The Integrated Circuit SB23YR80B through the EEPROM ECC mechanism detects and reports integrity failures. The TSF manages the data integrity failure condition. The basic mechanisms required to assure TOE die and sensitive data integrity are provided by the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B embedded library and Hardware functionalities included in the TSF SF.PLATFORM.		
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		
(118) This function is responsible to erase the data. It includes mainly two types of operations: - Erasing of security related data buffers before starting a new working session. This allows the TOE to start new working sessions from a well defined and clean condition. Security status reached in previously working session is not still valid in following new working session. - Erasing of data buffer indented to contain sensitive data before allocation and after de-allocation. When a new couple of SCD/SVD is generated, the old one is definitely destroyed. Sensitive data are maintained in volatile TOE memory only for the time necessary for their usage. The basic mechanisms required to assure TOE security status and sensitive data erasing are provided by the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B embedded library and Hardware functionalities included in the TSF SF.PLATFORM.		
MAPPED TOE SFRs		
FCS	**FDP**	
CKM.4.1	**RIP.1.1**	

SF.DATA_UPDATE		
(119) 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. The basic mechanisms required to assure TOE data atomic transactions are provided by the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B embedded library and Hardware functionalities included in the TSF SF.PLATFORM.		
MAPPED TOE SFRs		
FPT		
FLS.1.1		

10.1.6 Test

SF.TEST		
(120) This function ensures the tests of TOE functionalities. It includes the test of Integrated Circuit SB23YR80B hardware components and its environmental operating conditions such as temperature, voltage and clock frequency. Depending on the typology and on the operation to be performed, the test is executed at power-up or before/after sensitive operation e.g. digital signature or cryptographic computation. Upon detection of an anomaly and depending on anomaly severity the TOE may end the working session entering a state becoming irresponsive or, in case of major severity, may change its life cycle state entering the "end of use" state. The basic mechanisms required to assure TOE test functionalities are provided by the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B embedded library and Hardware functionalities included in the TSF SF.PLATFORM.		
MAPPED TOE SFRs		
FPT	**FPT**	**FPT**
FLS.1.1	**PHP.1.2**	**TST.1.1**
PHP.1.1	**PHP.3.1**	**AMT.1.1**

10.1.7 Failure

SF.EXCEPTION		
(121) This function addresses the TOE exception management. The reasons of these exceptions are: range of operating conditions, integrity errors, life cycle and TOE internal audit failure. Upon detection of exception and depending on exception severity the TOE may end the working session entering a state were the TOE becomes irresponsive or, in case of major severity, may change its life cycle state entering the "end of use" state. The basic mechanisms required to assure TOE suitable exception management are provided by the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B embedded library and Hardware functionalities included in the TSF SF.PLATFORM.		
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**

10.1.8 TOE Life Cycle

SF.LIFE_CYCLE		
(122) This function manages the TOE life cycle, as described in chapter 6.3 TOE life cycle. The TOE life cycle states are: Pre-Personalization, Perso-A, Normal Use and End of Use. It ensures the detection of the current state and the switching to the next state. Commands are allowed or denied as well as some functionality are available or not depending on the state entered by the TOE. 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**

10.1.9 TOE PLATFORM

SF.PLATFORM
(123) The TSF manages all functionalities provided by the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B with embedded library and Hardware functionalities Some TOE TSFs have the own functionalities based on the functionalities made available from the security functions provided by J-SAFE Java card 3.0.4 platform [JSAFE_ST]. This includes : **SF.SecureManagement** for support of functionalities such as: • Memory cleaning upon: allocation of class instances, arrays, and APDU buffer, and de-allocation of array object, any transient object, any reference to an object instance created during an aborted transaction. • Unobservability: operations on secret keys and PIN codes are not observable by other subjects by observation of variations in power consumption or timing analysis. • Preservation of a secure state when the following types of failures occur: loss of power or card tearing, EEPROM memory wear-out, failed checksum verification on sensitive data. • Monitor events related to TOE security and to preserve a TOE secure state, auditable events are: card tearing, power failure, abnormal environmental operating conditions (frequency, voltage, and temperature), physical tampering and EEPROM consistency/integrity check failure. **SF.CryptoKey** for support of functionalities such as: • key generation • key destruction • integrity and the unobservability of the keys. **SF.CryptoOp** for functionalities of encryption/decryption and signature/verification with the support of the following algorithms: • DES ECB and CBC • Triple DES ECB and CBC with 16, 24 bytes of key • AES ECB and CBC with 128, 256 bits of key • RSA CRT with key length 512, 768, 1024 and 2048 bits • EC over GF(p) with key length up to 521 bits • Deterministic Random Number Generation according to ANSI X9.31, seeded with random numbers from the physical RNG of the hardware. **SF.Transaction** for support of functionalities concerning “persistent memory” changes in order to: • assures the coherence of the data if a failure occurs during their update • support of Java Card transactional mechanism **SF.ObjectDeletion**: de-allocation of memory resources of objects no longer accessible. The security functionality also guarantees that, once the method has been invoked, information content of unreachable objects cannot be retrieved anymore **SF.SmartCardPlatform**: hardware Security Functionalities: HW initialisation, logical integrity, Memory Firewall, Physical tampering protection, Security violation administrator, Unobservability, Symmetric/Asymmetric Key Cryptography and Unpredictable Number Generation Support

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

10.2 Assurance Measures

(124) Appropriate assurance measures have been and are being employed to meet the assurance requirements for the Common Criteria EAL4 evaluation level augmented with AVA_VAN.5 components.

11. STATEMENT OF COMPATIBILITY CONCERNING COMPOSITE SECURITY TARGET

(125) This is a Statement of Compatibility between this Composite ST and the ST of J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B with embedded library and Hardware functionalities from now on referred to as Platform ST [JSAFE_ST]. The following mappings regarding SFRs, threats, assumptions, organizational security policies and objectives demonstrate the compatibility between the Composite Security Target and the Platform ST [JSAFE_ST].

(126) The following table lists the Platform Security Functionalities and classifies the Platform SF as relevant or not relevant for the Composite TOE

Platform Security Functionality	Relevant
SF.Firewall: FIREWALL access control SFP and JCVM information flow control SFP	**N** [10]
SF.SecureManagement: Memory cleaning, secure state preservation, secure usage of sensitive data, management of security attributes	**Y**
SF.CryptoKey: key distribution, access, destruction, generation integrity and unobservability	**Y**
SF.CryptoOp: cryptographic support to perform encryption/decryption, signature generation, verification	**Y**
SF.Transaction: atomic updates of persistemt memory	**Y**
SF.PIN: all the operation related to PIN objects, verification and try counter management	**N** [11]
SF.ObjectDeletion: de-allocation of memory resources of objects no longer accessible. The security functionality also guarantees that, once the method has been invoked, information content of unreachable objects cannot be retrieved anymore.	**Y**
SF.SmartCardPlatform: hardware Security Functionalities: hardware secure initialization, Memory segmentation protection, Physical tampering protection, Information leakage protection, Cryptography Support, Random Number Generation	**Y**

Table 5 - Platform Security Functionality relevance for the composite TOE

(127) **SF.Firewall** and **SF.PIN** are considered not relevant to the composite TOE because these functionalities available in J-SAFE platform are not used by the composite TOE

(128) The composite security functionalities that are proper to composite TOE are: **SF.RAD, SF.AC and SF.LIFE_CYCLE**

(129) The Table 6 is the mapping of composite TOE SARs with Platform SARs

[10] **SF.Firewall**, is considered not relevant for the composite TOE because only the javacard applet implementing the TOE is installed and default select in the final TOE. The javacard platform J-SAFE has the card manager disabled.

[11] **SF.PIN** is considered not relevant for the composite TOE because these functionalities available in J-SAFE platform are not used by the composite TOE. All the functionalities related to PIN management are implemented directly into the javacard applet J-SIGN.

Composite TOE SAR	Platform SAR
ASE	
ASE_CCL.1 Conformance claims	ASE_CCL.1
ASE_ECD.1 Extended components definition	ASE_ECD.1
ASE_INT.1 ST introduction	ASE_INT.1
ASE_OBJ.2 Security objectives	ASE_OBJ.2
ASE_REQ.2 Derived security requirements	ASE_REQ.2
ASE_SPD.1 Security problem definition	ASE_SPD.1
ASE_TSS.1 TOE summary specification	ASE_TSS.1
ALC	
ALC_CMC.4 Production support, acceptance procedures and automation	ALC_CMC.4
ALC_CMS.4 Problem tracking CM coverage	ALC_CMS.5 - Development tools CM coverage
ALC_DEL.1 Delivery procedures	ALC_DEL.1
ALC_DVS.1 Identification of security measures	ALC_DVS.2 - Sufficiency of security measures
ALC_LCD.1 Developer defined life-cycle model	ALC_LCD.1
ALC_TAT.1 Well-defined development tools	ALC_TAT.2 - Compliance with implementation standards
AGD	
AGD_PRE.1 Preparative procedures	AGD_PRE.1
AGD_OPE.1 Operational user guidance	AGD_OPE.1
ADV	
ADV_ARC.1 Security architecture description	ADV_ARC.1
ADV_FSP.4 Complete functional specification	ADV_FSP.5 - Complete semi-formal functional specification with additional error information
ADV_IMP.1 Implementation representation of the TSF	ADV_IMP.1
ADV_TDS.3 Basic modular design	ADV_TDS.4 - Semiformal modular design
ATE	
ATE_COV.2 Analysis of coverage	ATE_COV.2
ATE_DPT.1 Testing: basic design	ATE_DPT.3 - Testing: modular design
ATE_FUN.1 Functional testing	ATE_FUN.1
ATE_IND.2 Independent testing – sample.	ATE_IND.2
AVA	
AVA_VAN.5 Advanced methodical vulnerability analysis	AVA_VAN.5

Table 6 - Platform SARs Vs Composite TOE SARs

(130) The table below shows the mapping between the Platform SFRs and the Composite ST SFRs. Only the relevant platform SFRs are listed.

Platform SFRs	Composite TOE SFRs
Firewall Policy	
fdp_rip.1.1/OBJECTS Subset residual information protection	**FDP_RIP.1.1**
Application Programming Interface	
fcs_ckm.1.1/RSA Cryptographic key generation	**FCS_CKM.1.1**
fcs_ckm.1.1/EC Cryptographic key generation	**FCS_CKM.1.1**
fcs_ckm.4.1 Cryptographic key destruction	**FCS_CKM.4.1**
fcs_cop.1.1/DES-TDES_Cipher Cryptographic operation	**FTP_ITC.1.1, FTP_TRP.1.1, FDP_UIT.1.1, FDP_UIT.1.2**
fcs_cop.1.1/DES_MAC Cryptographic operation	**FTP_ITC.1.1, FTP_TRP.1.1, FDP_UIT.1.1, FDP_UIT.1.2, FIA_UID.1.1, FIA_UAU.1.1**
fcs_cop.1.1/AES_Cipher Cryptographic operation **fcs_cop.1.1/AES_MAC** Cryptographic operation	**FIA_UID.1.1, FIA_UAU.1.1**
fcs_cop.1.1/RSA_Cipher Cryptographic operation **fcs_cop.1.1/RSA_Signature** Cryptographic operation	**FCS_COP.1.1/CORRESP, FCS_COP.1.1/SIGNING, FIA_UID.1.1, FIA_UAU.1.1**
fcs_cop.1.1/EC_Signature Cryptographic operation	**FCS_COP.1.1/CORRESP, FCS_COP.1.1/SIGNING**
fcs_cop.1.1/SHA Cryptographic operation	**FCS_COP.1.1/SIGNING**
fdp_rip.1.1/ABORT Subset residual information protection	**FDP_RIP.1.1**
fdp_rip.1.1/APDU Subset residual information protection	**FDP_RIP.1.1**
fdp_rip.1.1/bArray Subset residual information protection	**FDP_RIP.1.1**
fdp_rip.1.1/KEYS Subset residual information protection	**FDP_RIP.1.1**
fdp_rip.1.1/TRANSIENT Subset residual information protection	**FDP_RIP.1.1**
fdp_rip.1.1/OBJECTS	**FDP_RIP.1.1**
fdp_rip.1.1/ODEL	**FDP_RIP.1.1**
Card Security Management	
fdp_sdi.2.1 Stored data integrity monitoring and action	**FDP_SDI.2.1, FDP_SDI.2.1**
IC Hardware	
fpt_fls.1.1/SCP Failure with preservation of secure state	**FPT_FLS.1.1**
fpt_php.3.1 Resistance to physical attack	**FPT_PHP.1.1, FPT_PHP.1.2, FPT_PHP.3.1**
fcs_rng.1.1 **fcs_rng.1.2**	**FTP_ITC.1.1, FTP_TRP.1.1, FCS_CKM.1.1, FCS_COP.1.1/SIGNING**
Additional Security Functional Requirements	
fpt_tst.1.1 TSF testing	**FPT_TST.1.1, FPT_AMT.1.1**
fpt_emsec.1.1 **fpt_emsec.1.2**	**FPT_EMSEC.1.1** **FPT_EMSEC.1.2**

Table 7 - Platform SFRs VS Composite TOE SFRs

Proper Composite TOE SFRs
FDP_ACC.1/SVD TRANSFER SFP
FDP_ACC.1/INITIALISATION SFP
FDP_ACC.1/PERSONALISATION SFP
FDP_ACC.1/SIGNATURE-CREATION SFP
FDP_ACF.1/INITIALISATION SFP
FDP_ACF.1/SVD TRANSFER SFP

FDP_ACF.1/PERSONALISATION SFP
FDP_ACF.1/SIGNATURE-CREATION SFP
FDP_ETC.1/SVD TRANSFER
FDP_ITC.1/DTBS
FIA_AFL.1
FIA_ATD.1
FMT_MOF.1
FMT_MSA.1/ADMINISTRATOR
FMT_MSA.1/SIGNATORY
FMT_MSA.2
FMT_MSA.3
FMT_MTD.1
FMT_SMR.1

Table 8 – Proper composite TOE SFRs

(131) There is no conflict between security objectives of the Composite ST and the Platform ST. A mapping between security objectives of the Composite ST and the Platform ST is reported in Table 9.

Platform Objectives	**Composite TOE** Objectives
O.SCP.IC O.ALARM	**OT.Tamper_ID, OT.Tamper_Resistance**
O.SIDE_CHANNEL	**OT.EMSEC_Design**
O.CIPHER O.KEY-MNGT	**OT.SCD_SVD_Corresp OT.SCD_Unique**
O.KEY-MNGT O.SIDE_CHANNEL	**OT.SCD_Secrecy**
O.REALLOCATION O.OBJ-DEL	**OT.Lifecycle_Security**
	Proper composite TOE Objectives **OT.Sig_Secure** **OT.Init** **OT.SVD_Auth_TOE** **OT.DTBS_Integrity_TOE** **OT.Sigy_SigF**

Table 9 – Platform Objectives Vs Composite TOE Objectives

(132) **OT.Tamper_ID, OT.Tamper_Resistance** concerning tamper detection and resistance can be mapped on the platform security objectives O.ALARM and O.CSP.IC; see [JSAFE_ST] for platform objective definition.

(133) **OT.EMSEC_Design** concerning physical emanations security can be mapped on the platform security objectives O.SIDE_CHANNEL; see [JSAFE_ST] for platform objective definition.

(134) **OT.SCD_SVD_Corresp OT.SCD_Unique** concerning SVD/SCD correspondence and SCD unicity can be mapped on the platform security objectives O.CIPHER and O.KEY-MNGT; see [JSAFE_ST] for platform objective definition.

(135) **OT.SCD_Secrecy** concerning SCD secrecy can be mapped on the platform security objectives O.SIDE_CHANNEL and O.KEY-MNGT; see [JSAFE_ST] for platform objective definition.

(136) **OT.Lifecycle_Security** life cycle security can be mapped on the platform security objectives O.REALLOCATION and O.OBJ-DEL; see [JSAFE_ST] for platform objective definition.

Platform SFRs	Platform Objective
fpt_fls.1.1/SCP **fpt_php.3.1**	O.SCP.IC
fpt_emsec.1.1 **fpt_emsec.1.2**	O.SIDE_CHANNEL
fcs_ckm.1.1/RSA **fcs_ckm.1.1/EC** **fcs_ckm.4.1** **fcs_cop.1.1/DES-TDES_Cipher** **fcs_cop.1.1/DES_MAC** **fcs_cop.1.1/AES_Cipher** **fcs_cop.1.1/AES_MAC** **fcs_cop.1.1/RSA_Cipher** **fcs_cop.1.1/RSA_Signature** **fcs_cop.1.1/EC_Signature** **fcs_cop.1.1/SHA** **fcs_rng.1.1** **fcs_rng.1.2**	O.CIPHER
fdp_rip.1.1/OBJECTS **fdp_rip.1.1/ABORT** **fdp_rip.1.1/APDU** **fdp_rip.1.1/bArray** **fdp_rip.1.1/KEYS** **fdp_rip.1.1/TRANSIENT** **fdp_rip.1.1/ODEL** **fdp_sdi.2.1**	O.KEY-MNGT
fdp_rip.1.1/ODEL	O.OBJ-DEL
fpt_fls.1/SCP	O.ALARM
fdp_rip.1.1/OBJECTS **fdp_rip.1.1/ABORT** **fdp_rip.1.1/APDU** **fdp_rip.1.1/bArray** **fdp_rip.1.1/KEYS** **fdp_rip.1.1/TRANSIENT** **fdp_rip.1.1/ODEL**	O.REALLOCATION

Table 10 – Relevant Platform SFRs Vs Platform Objectives

(137) There is no conflict between threats of the Composite ST and the Platform ST. A mapping between threats of the Composite ST and the Platform ST is reported in the Table 11.

Platform Threats	Composite TOE Threats
T.PHYSICAL	**T.Hack_Phys**
T.INTEG-APPLI-DATA	**T.Sig_Forgery, T.SVD_Forgery T.DTBS_Forgery**

T.EXE-CODE.1 T.EXE-CODE.2 T.NATIVE T.INTEG-APPLI-CODE T.INTEG-APPLI-DATA	**T.SigF_Misuse**

Table 11 – Platform Threats VS Composite TOE Threats

(138) **T.Hack_Phys** Physical attacks through the TOE interfaces can be mapped to the platform threat T.PHYSICAL; see [JSAFE_ST] for platform threats definition

(139) **T.Sig_Forgery, T.SVD_Forgery T.DTBS_Forgery** all concerning the forgery of sensitive data can be mapped to the platform threat T.INTEG-APPLI-DATA; see [JSAFE_ST] for platform threats definition

(140) **T.SigF_Misuse** Misuse of the signature-creation function of the can be mapped to the platform threats T.EXE-CODE.1, T.EXE-CODE.2, T.NATIVE, T.INTEG-APPLI-CODE and T.INTEG-APPLI-DATA; see [JSAFE_ST] for platform threats definition

Platform Threats	Platform Objectives
T.PHYSICAL	**O.SCP.IC, O.SCP.SUPPORT, O.ALARM,O.SIDE_CHANNEL**
T.INTEG-APPLI-CODE	**O.NATIVE, OE.CARD_MANAGEMENT OE.VERIFICATION**
T.INTEG-APPLI-DATA	**O.SID , O.FIREWALL, O.GLOBAL_ARRAYS_INTEG O.OPERATE, O.REALLOCATION, O.SCP.RECOVERY O.SCP.SUPPORT, O.ALARM, O.CIPHER O.KEY-MNGT, O.PIN-MNGT, O.TRANSACTION OE.CARD_MANAGEMENT, OE.VERIFICATION**
T.EXE-CODE.1	**O.FIREWALL, OE.VERIFICATION**
T.EXE-CODE.2	**OE.VERIFICATION**
T.NATIVE	**O.NATIVE, OE.VERIFICATION, O.OPERATE**
	Proper composite TOE Threats **T.SCD_Derive T.SCD_Divulg T.Sig_Repud**

Table 12 – Relevant Platform Threats Vs Platform Objectives

(141) There is no conflict between organizational security policies of the Composite ST and the organizational security policies of the Platform ST. A mapping between organizational security policies of the Composite ST and the Platform ST is reported in Table 13.

Platform OSP	**Composite TOE OSP**
OSP.CARD_ADMINISTRATION_DISABLED OSP.VERIFICATION OSP.ROLES	Not directly mapped on proper composite TOE OSP but considered **relevant** as they are not in conflict and they enhance the global security of composite TOE. No evidence of contradictions respect to the composite TOE threats.
OSP.MANAGEMENT_OF_SECRETS	**P.PERSONALIZATION, P.VAD**
	Proper composite TOE OSP **P.MANAGEMENT** **P.CSP_QCert** **P.QSign** **P.Sigy_SSCD**

Table 13 – Platform OSPs VS Composite TOE OSPs

Platform OSP	**Platform** Objectives
OSP.CARD_ADMINISTRATION_DISABLED	OE.CARD_MANAGEMENT
OSP.VERIFICATION	OE.VERIFICATION
OSP.ROLES	O.ROLES
OSP.MANAGEMENT_OF_SECRETS	OE.MANAGEMENT_OF_SECRETS

Table 14 – Platform OSPs Vs Platform objectives

(142) There is no conflict between assumptions of the Composite ST and the Platform ST.

Platform Assumptions	**Composite ST Assumptions**
A.VERIFICATION A.NO-DELETION A.NO-INSTALL	Not directly mapped on proper composite TOE assumptions but considered **relevant** as they are not in conflict and they enhance the global security of composite TOE. The assumptions defined for the Platform J-SAFE, **A.VERIFICATION**, **A.NO-DELETION** and **A.NO-INSTALL** are related to bytecode verification and to the no-deletion or no-installation of packages/applets after TOE issuance; these assumptions are not in conflict and compatible with the proper composite TOE assumptions **A.CGA** and **A.SCA** all concerning the trustworthy of external applications which interact with the composite TOE for certificate and signature processing
	Proper composite TOE assumptions **A.CGA** **A.SCA**

Table 15 – Platform Assumptions VS Composite TOE Assumptions

(143) There is no conflict between security objectives for the environment of the Composite ST and the security objectives for the environment of the Platform ST.

Platform Objectives for the Environment	Composite TOE Objectives for the Environment
OE.NO-DELETION OE.NO-INSTALL OE.VERIFICATION OE.CARD_MANAGEMENT	Not directly mapped on proper composite TOE objective for environment but considered **relevant** as they are not in conflict and they enhance the global security of composite TOE.
OE.MANAGEMENT_OF_SECRETS	**OE.Op_Phase, OE.HI_VAD**
	Proper composite TOE Objective for environment **OE.CGA_QCert** **OE.SVD_Auth_CGA** **OE.SCA_Data_Intend**

Table 16 – Platform OEs Vs Composite TOE OEs

(144) **OE.Op_Phase** *TOE operational phase security* concerning the security of sensitive data can be mapped to the platform objective for the environment OE.MANAGEMENT_OF_SECRETS; see [JSAFE_ST] for platform OE definition

(145) **OE.HI_VAD** *Protection of the VAD* concerning the protection of VAD by a TOE external device can be mapped to the platform objective for the environment OE.MANAGEMENT_OF_SECRETS; see [JSAFE_ST] for platform OE definition

Platform Objectives for the Environment	Platform Assumptions
OE.VERIFICATION	**A.VERIFICATION**
OE.NO-DELETION , OE.CARD_MANAGEMENT	**A.NO-DELETION**
OE.NO-INSTALL, OE.CARD_MANAGEMENT	**A.NO-INSTALL**
OE.MANAGEMENT_OF_SECRETS	OSP.MANAGEMENT_OF_SECRETS

Table 17 – Platform OEs Vs Platform assumptions

12. SSCD PP CLAIMS

(146) J-SIGN conforms to the requirements in [SSCD_PP].

12.1 PP reference

(147) The ST is in compliance with the [SSCD_PP] 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

12.2 PP tailoring

(148) Tables in chapter 9 identifies each SFR for this Security target lite and the tailoring operations performed relative [SSCD_PP]. 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].

12.3 PP additions

(149) This Security target lite includes one additional TOE security functional requirement **FMT_SMF.1** in 9.

(150) This Security target lite includes one additional security objective for the non-IT environment **OE.Op_Phase** in 8.3.

(151) 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] has been split in $\textbf{RAD}_\textbf{A}$ and $\textbf{RAD}_\textbf{S}$, which have the same security need.

(152) **P.PERSONALIZATION** states that the TOE personalization must be performed in the observance of proper physical and procedural measures.

(153) **P.MANAGEMENT** 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.

(154) **P.VAD** covers the procedural measures needed for the secure distribution of PIN codes to related TOE users.

13. RATIONALE

13.1 Security Objectives Rationale

(155) The security objectives for the TOE are listed in 8.1 and they map exactly the security objectives for the TOE in [SSCD_PP] § 4.1 as required by the claim of strict conformance to [SSCD_PP].

13.1.1 Security Objectives Coverage

(156) As for [SSCD_PP] § 6.2.1.

Threats - Assumptions – Policies Vs 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																√	
P.CSP_QCert					√								√				
P.QSign											√	√	√			√	
P.Sigy_SSCD			√						√		√						
P.PERSONALIZATION																	√
P.MANAGEMENT																	√
P.VAD																	√

Table 18: Threats, Assumptions and Policy Vs Security objective mapping

13.1.2 Threats and Security Objectives Sufficiency

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

(158) **T.SCD_Divulg** (Storing,copying, and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [1], recital (18). This threat is countered by OT.SCD_Secrecy which assures the secrecy of the SCD used for signature generation.

(159) **T.SCD_Derive** (Derive the signature-creation data) deals with attacks on the SCD via public known data produced by the TOE. This threat is countered by OT.SCD_Unique that provides cryptographic secure generation of the SCD/SVD-pair. OT.Sig_Secure ensures cryptographic secure electronic signatures.

(160) **T.DTBS_Forgery** (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which than does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by verifying the integrity of the DTBS-representation. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.SCA_Data_Indent.

.

(161) **T.SigF_Misuse** (Misuse of the signature-creation function of the TOE) addresses the threat of misuse of the TOE signature-creation function to create SDO by others than the signatory to create SDO for data the signatory has not decided to sign, as required by the Directive [1], Annex III, paragraph 1, literal (c). This threat is addressed by the OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OE.SCA_Data_Intend (Data intended to be signed), OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity), and OE.HI_VAD (Protection of the VAD) as follows: OT.Sigy_SigF ensures that the TOE provides the signature-generation function for the legitimate signatory only. OE.SCA_Data_Intend ensures that the SCA sends the DTBS-representation only for data the signatory intends to sign. The combination of OT.DTBS_Integrity_TOE and OE.SCA_Data_Intend counters the misuse of the signature generation function by means of manipulation of the channel between the SCA and the TOE. If the SCA provides the human interface for the user authentication, OE.HI_VAD provides confidentiality and integrity of the VAD as needed by the authentication method employed.

(162) **T.Sig_Forgery** (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. This threat is in general addressed by OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_Secrecy (Secrecy of the signature-creation data),, OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance) and OT.Lifecycle_Security (Lifecycle security), as follows: OT.Sig_Secure ensures by means of robust encryption techniques that the signed data and the electronic signature are securely linked together. OE.SCA_Data_Intend provides that the methods used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation is appropriate for the cryptographic methods employed to generate the electronic signature. The combination of OE.CGA_QCert, OT.SCD_SVD_Corresp, OT.SVD_Auth_TOE, and OE.SVD_Auth_CGA provides the integrity and authenticity of the SVD that is used by the signature verification process. OT.Sig_Secure, OT.SCD_Secrecy, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

(163) **T.Sig_Repud** (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGA_QCert (Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signaturecreation data), , OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed) and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity). OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. OE.CGA_QCert and OT.SCD_SVD_Corresp ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OT.SCD_Unique provides that the signatory’s SCD can practically occur just once. OT.Sig_Secure, OT.SCD_Transfer, OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD. OT.Sigy_SigF provides that only the signatory may use the TOE for signature generation. OT.Sig_Secure ensures by means of robust cryptographic techniques that valid electronic signatures

may only be generated by employing the SCD corresponding to the SVD that is used for signature verification and only for the signed data. OE.SCA_Data_Intend and OT.DTBS_Integrity_TOE ensure that the TOE generates electronic signatures only for DTBS-representations which the signatory has decided to sign as DTBS.

(164) **T.SVD_Forgery** (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.SVD_Auth_TOE which ensures that the TOE sends the SVD in a verifiable form to the CGA, as well as by E.SVD_Auth_CGA which provides verification of SVD authenticity by the CGA.

13.1.3 Policies and Security Objective Sufficiency

(165) **P.CSP_QCert** (CSP generates qualified certificates) establishes the qualified certificate for the signatory and provides that the SVD matches the SCD that is implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by the TOE by OT.SCD_SVD_Corresp concerning the correspondence between the SVD and the SCD, in the TOE IT environment, by OE.CGA_QCert for generation of qualified certificates by the CGA, respectively.

(166) **P.QSign** (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with qualified electronic signatures, as defined by the Directive [1], article 5, paragraph 1. Directive [1], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The requirement of qualified electronic signatures being based on qualified certificates is addressed by OE.CGA_QCert. OE.SCA_Data_Intend provides that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. OT.Sig_Secure and OT.Sigy_SigF address the generation of advanced signatures by the TOE.

(167) **P.Sigy_SSCD** (TOE as secure signature-creation device) establishes the TOE as secure signature-creation device of the signatory with practically unique SCD. This is addressed by OT.Sigy_SigF ensuring that the SCD is under sole control of the signatory and OT.SCD_Unique ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. OT.Init provides that generation of the SCD/SVD pair is restricted to authorised users.

(168) **P.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.

(169) **P.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.

(170) **P.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.

13.1.4 Assumptions and Security Objective Sufficiency

(171) **A.SCA** (Trustworthy signature-creation application) establishes the trustworthiness of the SCA according to the generation of DTBS-representation. This is addressed by OE.SCA_Data_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS-representation of the data that has been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE

(172) **A.CGA** (Trustworthy certification-generation application) establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert (Generation of qualified certificates) which ensures the generation of qualified certificates and by OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) which ensures the verification of the integrity of the received SVD and the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

13.2 Security Requirements Rationale

(173) The security functional requirements with assignment, selection and refinement operations for the TOE are listed in 9.1 and they map exactly the functional requirements for the TOE in [SSCD_PP] § 5.1 as required by the claim of strict conformance to [SSCD_PP].

13.2.1 Security Requirements coverage

(174) The Table 19 is the mapping of TOE security functional requirements to the TOE security objectives

TOE SFR vs 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
FCS_CKM.1				x	x				x			
FCS_CKM.4		x		x								
FCS_COP.1/CORRESP					x							
FCS_COP.1/SIGNING												x
FDP_ACC.1/SVD TRANSFER SFP						x						
FDP_ACC.1/INITIALISATION SFP			x	x								
FDP_ACC.1/PERSONALISATION SFP											x	
FDP_ACC.1/SIGNATURE-CREATION SFP										x	x	
FDP_ACF.1/INITIALISATION SFP			x	x								
FDP_ACF.1/SVD TRANSFER SFP						x						
FDP_ACF.1/PERSONALISATION SFP											x	
FDP_ACF.1/SIGNATURE-CREATION SFP										x	x	
FDP_ETC.1/SVD TRANSFER						x						
FDP_ITC.1/DTBS										x		
FDP_RIP.1				x							x	
FDP_SDI.2/Persistent				x	x						x	x
FDP_SDI.2/DTBS										x		
FDP_UIT.1/SVD TRANSFER						x						
FDP_UIT.1/TOE DTBS										x		
FIA_AFL.1			x								x	
FIA_ATD.1			x								x	
FIA_UAU.1			x								x	
FIA_UID.1			x								x	
FMT_MOF.1				x							x	
FMT_MSA.1/ADMINISTRATOR			x	x								
FMT_MSA.1/SIGNATORY											x	
FMT_MSA.2											x	
FMT_MSA.3/			x	x							x	
FMT_MTD.1											x	
FMT_SMR.1				x							x	
FPT_AMT.1		x		x								x
FPT_EMSEC.1	x											
FPT_FLS.1				x								
FPT_PHP.1							x					
FPT_PHP.3								x				
FPT_TST.1		x										x
FTP_ITC.1/SVD TRANSFER						x						
FTP_ITC.1/DTBS IMPORT										x		
FTP_TRP.1/TOE											x	

Table 19: TOE Security functional requirements vs TOE Security Objectives

Environment Security Requirement vs 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

Table 20: Environment Security Requirement vs Environment Security objectives

(175) This Security target lite includes one additional TOE security functional requirement **FMT_SMF.1** in 9. This Security target lite fully complies with [SSCD_PP] § 6.3.1 with the following line added to the table 6.2 in [SSCD_PP] § 6.3.1.

TOE Security Functional Requirement vs TOE Security objectives	OT.EMSEC_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			√	√							√	

Table 21: TOE Security Functional Requirement vs TOE Security objectives

13.2.2 TOE Security Requirements sufficiency

(176) **OT.EMSEC_Design (Provide physical emanations security)** covers that no intelligible information is emanated. This is provided by FPT_EMSEC.1.1.

(177) **OT.Init (SCD/SVD generation)** addresses that generation of a SCD/SVD pair requires proper user authentication. FIA_ATD.1 define RAD as the corresponding user attribute. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorized functions. The attributes of the authenticated user are provided by FMT_MSA.1/ADMINISTRATOR, FMT_MSA.3 for static attribute initialization. Access control is provided by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1.**security).** The

management specification for Identification and Authentication and access control is provided by **FMT_SMF.1**

(178) **OT.Lifecycle_Security (Lifecycle security)** is provided by the security assurance requirements ALC_DVS.1, ALC_LCD.1, ALC_TAT.1,ADO_DEL.2, and ADO_IGS.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functions FPT_TST.1 and FPT_AMT.1 provide failure detection throughout the lifecycle. FCS_CKM.4 provides secure destruction of the SCD.

(179) **OT.SCD_Secrecy (Secrecy of signature-creation data)** counters that, with reference to recital (18) of the Directive, storage or copying of SCD causes a threat to the legal validity of electronic signatures. OT.SCD_Secrecy is provided by the security functions specified by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP that ensure that only authorized user can initialize the TOE and create or load the SCD. The authentication and access management functions specified by FMT_MOF.1, FMT_MSA.1, FMT_MSA.3 corresponding to the actual TOE (i.e., FMT_MSA.1/ADMINISTRATOR, FMT_MSA.3), and FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_AMT.1 and FPT_FLS.1 test the working conditions of the TOE and guarantee a secure state when integrity is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS is differential fault analysis (DFA). The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation, AVA_SOF HIGH by requesting strength of function high for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient. The management specification for Identification and Authentication and access control is provided by **FMT_SMF.1**

(180) **OT.SCD_SVD_Corresp (Correspondence between SVD and SCD)** addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Cryptographic correspondence is provided by FCS_COP.1/CORRESP

(181) **OT.SCD_Unique (Uniqueness of the signature-creation data)** implements the requirement of practically unique SCD as laid down in the Directive [1], Annex III, article 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

(182) **OT.DTBS_Integrity_TOE (Verification of DTBS-representation integrity)** covers that integrity of the DTBS-representation to be signed is to be verified, as well as the DTBS-representation is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms of FDP_ITC.1/DTBS, FTP_ITC.1/DTBS IMPORT, and by FDP_UIT.1/TOE DTBS. The verification that the DTBS-representation has not been altered by the TOE is done by integrity functions specified by FDP_SDI.2/DTBS. The access control requirements of FDP_ACC.1/SIGNATURE CREATION SFP and FDP_ACF.1/SIGNATURE CREATION SFP keeps unauthorized parties off from altering the DTBS-representation.

(183) **OT.Sigy_SigF (Signature generation function for the legitimate signatory only)** is provided by FIA_UAU.1 and FIA_UID.1 that ensure that no signature generation function can be invoked before the signatory is identified and authenticated. The security functions specified by FDP_ACC.1/PERSONALISATION SFP, FDP_ACC.1/SIGNATURE-CREATION SFP, FDP_ACF.1/PERSONALISATION SFP, FDP_ACF.1/SIGNATURE-CREATION SFP, FMT_MTD.1 and FMT_SMR.1 ensure that the signature process is restricted to the signatory. The security functions specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, and FMT_MSA.3 ensure that the access to the signature generation functions remain under the sole control of the signatory, as well

as FMT_MSA.1/SIGNATORY provides that the control of corresponding security attributes is under signatory's control. The security functions specified by FDP_SDI.2 and FPT_TRP.1/TOE ensure the integrity of stored data both during communication and while stored. The security functions specified by FDP_RIP.1 and FIA_AFL.1 provide protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The assurance measures specified by AVA_MSU.3 by requesting analysis of misuse of the TOE implementation, AVA_SOF.1 by requesting high strength level for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient. The management specification for Identification and Authentication and access control is provided by **FMT_SMF.1**

(184) **OT.Sig_Secure (Cryptographic security of the electronic signature)** is provided by the cryptographic algorithms specified by FCS_COP.1/SIGNING which ensures the cryptographic robustness of the signature algorithms. The security functions specified by FPT_AMT.1 and FPT_TST.1 ensure that the security functions are performing correctly. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE**.**

(185) **OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD)** is provided by a trusted channel guaranteeing SVD origin and integrity by means of FTP_ITC.1/SVD TRANSFER and FDP_UIT.1/SVD TRANSFER. The cryptographic algorithms specified by FDP_ACC.1/SVD TRANSFER SFP, FDP_ACF.1/SVD TRANSFER SFP and FDP_ETC.1/SVD TRANSFER ensure that only authorised user can export the SVD to the CGA.

(186) **OT.Tamper_ID (Tamper detection)** is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

(187) **OT.Tamper_Resistance (Tamper resistance)** is provided by FPT_PHP.3 to resist physical attacks.

13.2.3 TOE Environment Security Requirements Sufficiency

(188) **OE.CGA_QCert (Generation of qualified certificates)** addresses the requirement of qualified certificates. The functions specified by FCS_CKM.2/CGA provide the cryptographic key distribution method. The functions specified by FCS_CKM.3/CGA ensure that the CGA imports the SVD using a secure channel and a secure key access method.

(189) **OE.HI_VAD (Protection of the VAD)** covers confidentiality and integrity of the VAD which is provided by the trusted path FTP_TRP.1/SCA

(190) **OE.SCA_Data_Intend (Data intended to be signed)** is provided by the functions specified by FTP_ITC.1/SCA DTBS and FDP_UIT.1/SCA DTBS that ensure that the DTBS can be checked by the TOE, and FCS_COP.1/SCA HASH that provides that the hashing function corresponds to the approved algorithms.

.

(191) **OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD)** is provided by FTP_ITC.1/SVD.IMPORT which assures identification of the sender and by FDP_UIT.1/ SVD IMPORT which guarantees it's integrity

.

(192) **OE.OP_Phase** adresses 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

13.2.4 Rationale for extensions

(193) The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. 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. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations.

.

(194) The additional family **FMT_SMF** (Specification of Management Functions) of the Class FMT (Security Management) is defined here to describe the IT security functional requirements of the TOE.
The TOE shall be capable of performing the following management functions:

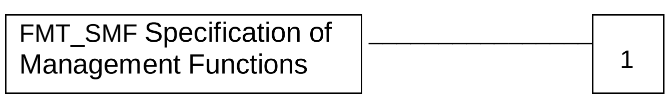
(1) Creation and modification of RAD,
(2) Enabling the signature-creation function,
(3) Modification of the security attribute SCD/SVD management, SCD operational,
(4) Change the default value of the security attribute SCD Identifier,

13.2.5 FMT_SMF Specification of Management Functions

Family Behaviour

This family allows the specification of the management functions to be provided by the TOE. Management functions provide TSFI that allow administrators to define the parameters that control the operation of security-related aspects of the TOE, such as data protection attributes, TOE protection attributes, audit attributes, and identification and authentication attributes. Management functions also include those functions performed by an operator to ensure continued operation of the TOE, such as backup and recovery. This family works in conjunction with the other components in the FMT: Security management class: the component in this family calls out the management functions, and other families in FMT: Security management restrict the ability to use these management functions.

Component levelling



FMT_SMF.1 Specification of Management Functions requires that the TSF provide specific management functions.

Management: FMT_SMF.1

There are no management activities foreseen.

Audit: FMT_SMF.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: Use of the management functions.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF].

13.3 Functional Requirements Dependencies

(195) This Security target lite fully complies with [SSCD_PP] § 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

The table below resumes all the SFR dependencies.

REQUIREMENT	DEPENDENCY
FCS_CKM.1	FCS_COP.1/SIGNING, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2
FCS_COP.1/ CORRESP RSA FCS_COP.1/ CORRESP ECC	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/ SIGNING RSA FCS_COP.1/ SIGNING ECC	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1/ Initialisation SFP	FDP_ACF.1/Initialisation SFP
FDP_ACC.1/ Personalisation SFP	FDP_ACF.1/Personalisation SFP
FDP_ACC.1/ Signature-Creation SFP	FDP_ACF.1/Signature Creation SFP
FDP_ACC.1/ SVD Transfer SFP	FDP_ACF.1/SVD Transfer SFP
FDP_ACF.1/ Initialisation SFP	FDP_ACC.1/Initialisation SFP, FMT_MSA.3
FDP_ACF.1/ Personalisation SFP	FDP_ACC.1/Personalisation SFP, FMT_MSA.3
FDP_ACF.1/ Signature-Creation SFP	FDP_ACC.1/Signature-Creation SFP, FMT_MSA.3
FDP_ACF.1/ SVD Transfer SFP	FDP_ACC.1/SVD Transfer SFP, FMT_MSA.3
FDP_ETC.1/ SVD Transfer SFP	FDP_ACC.1/ SVD Transfer SFP
FDP_ITC.1/DTBS	FDP_ACC.1/ Signature-Creation SFP, FMT_MSA.3
FDP_UIT.1/ SVD Transfer	FTP_ITC.1/SVD Transfer, FDP_ACC.1/SVD Transfer SFP
FDP_UIT.1/ TOE DTBS	FDP_ACC.1/Signature_Creation SFP, FTP_ITC.1/DTBS Import

FIA_AFL.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Administrator	FDP_ACC.1/Initialisation SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	FDP_ACC.1/ Signature_Creation SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	FDP_ACC.1/Personalisation SFP, FMT_SMR.1 FMT_MSA.1/Administrator, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1/Administrator, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1
FMT_SMR.1	FIA_UID.1
FPT_PHP.1	FMT_MOF.1
FPT_TST.1	FPT_AMT.1
FDP_RIP.1 FDP_SDI.2/Persistent FDP_SDI.2/DTBS FIA_ATD.1 FIA_UID.1 FPT_AMT.1 FPT_FLS.1 FPT_PHP.3 FTP_ITC.1/SVD TRANSFER FTP_ITC.1/DTBS IMPORT FTP_TRP.1/TOE FPT_EMSEC.1 FMT_SMF.1	No dependency

13.3.1 Assurance Requirements Suitability

(196) According to [SSCD_PP], the target assurance level is EAL4 augmented by AVA_VAN.5 assurance component.

(197) The TOE includes the J-SAFE Java card 3.0.4 platform and the Integrated Circuit SB23YR80B with embedded library and Hardware functionalities. J-SAFE Java card 3.0.4 platform is evaluated against the protection profile [PP_JC_Closed] with assurance level EAL5 augmented by **ALC_DVS.2** and **AVA_VAN.5**.assurance components [JSAFE_ST]. The SB23YR80B Secured Microcontroller with Cryptographic Library has been certified by ANSSI (cert. report ANSSI-CC-2010/02) with assurance level EAL6+: its associated Security Target Lite is [STlite_SB23] and the applicable Maintenance Report is [MntRep_SB23].

13.4 TOE Summary Specification Rationale

(198) 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.

(199) 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:

- the combination of specified TOE IT security functions work together so as to satisfy the TOE security functional requirements;
- the claim is justified that the stated assurance measures are compliant with the assurance requirements.

13.4.1 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**	(200) **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 CRT representation for the RSA algorithms and 160,192,224,256,384 and 521 bits for ECC algorithms (201) **SF.PLATFORM** contributes to FCS_CKM.1.1 satisfaction. The function acts as a support mechanism in the SCD/SVD key pair generation.
	CKM.4.1	(202) **SF.DATA_ERASE** grants the FCS_CKM.4.1 satisfaction specifying that the TOE correctly erase the data before/after allocation/deallocation of sensitive data. Once the data are erased from memory they are not more retrievable. (203) **SF.PLATFORM** contributes to FCS_CKM.4.1 satisfaction. The function acts as a support mechanism in clearing and/or erasing of data buffers before/after allocation/deallocation for sensitive data.
	COP.1.1/CORRESP	(204) **SF.KEY_GEN** grants the FCS_COP.1.1/CORRESP satisfaction specifying that the TOE moreover to correctly produce RSA and ECC SCD/SVD key pair of length 1024 or 2048 bit for RSA and 160,192,224,256,384 and 521 bits for ECC, performs a check to verify the SCD/SVD correspondence. (205) **SF.PLATFORM** contributes to FCS_COP.1.1/CORRESP satisfaction. The function acts as a support mechanism in the SCD/SVD key pair correspondence check.
	COP.1.1/SIGNING	(206) **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 CRT algorithms and key of length 160,192,224,256,384 and 521 bit and the ECC algorithms. (207) **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. (208) **SF.PLATFORM** contributes to FCS_COP.1.1/SIGNING satisfaction. The function acts as a support mechanism in the digital signature generation processing.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
FDP	**ACC.1.1 SVD Transfer SFP**	(209) **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. (210) **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 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. (211) **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. (212) **SF.PLATFORM** contributes to FDP_ACC.1.1 SVD Transfer SFP satisfaction. The function acts as a support mechanism for functionalities related to RAD objects.
	ACC.1.1 Initialization SFP	(213) **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. (214) **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 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. (215) **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. (216) **SF.PLATFORM** contributes to FDP_ACC.1.1 Initialization SFP satisfaction. The function acts as a support mechanism for functionalities related to RAD objects.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	ACC.1.1 Personalization SFP	(217) **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 RADS. This function compares the security status required to process the command and allows or denies the RADS creation. (218) **SF.AUTH** grants the FDP_ACC.1.1 Personalization SFP satisfaction. This function addresses the "Administrator" authentication by the TOE allowing or denying the RADS creation. The "Administrator" authentication is based on PIN mechanism. The 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. (219) **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 RADA stored in the TOE. The function is executed in a secure manner. (220) **SF.PLATFORM** contributes to FDP_ACC.1.1 Personalization SFP satisfaction. The function acts as a support mechanism for functionalities related to RAD objects.
	ACC.1.1 Signature Creation SFP	(221) **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 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. (222) **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. (223) **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. (224) **SF.PLATFORM** contributes to FDP_ACC.1.1 Signature Creation SFP satisfaction. The function acts as a support mechanism for functionalities related to RAD objects.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	ACF.1.1 Initialization SFP	(225) **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	(226) **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. (227) **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 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. (228) **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. (229) **SF.PLATFORM** contributes to FDP_ACF.1.2 Initialization SFP satisfaction. The function acts as a support mechanism for functionalities related to RAD objects.
	ACF.1.3 Initialization SFP	(230) **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.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	ACF.1.4 Initialization SFP	(231) **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. (232) **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 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. (233) **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. (234) **SF.PLATFORM** contributes to FDP_ACF.1.4 Initialization SFP satisfaction. The function acts as a support mechanism for functionalities related to RAD objects.
	ACF.1.1 SVD Transfer SFP	(235) **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.
	ACF.1.2 SVD Transfer SFP	(236) **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. (237) **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 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. (238) **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. (239) **SF.PLATFORM** contributes to FDP_ACF.1.2 SVD Transfer SFP satisfaction. The function acts as a support mechanism for functionalities related to RAD objects.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	ACF.1.3 SVD Transfer SFP **ACF.1.4 SVD Transfer SFP**	(240) **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	(241) **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	(242) **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. (243) **SF.AUTH** grants the FDP_ACF.1.2 Personalization SFP satisfaction. This function addresses the "Administrator" authentication by the TOE allowing or denying the RADS creation. The "Administrator" authentication is based on PIN mechanism. The 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. (244) **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. (245) **SF.PLATFORM** contributes to FDP_ACF.1.2 Personalization SFP satisfaction. The function acts as a support mechanism for functionalities related to RAD objects.
	ACF.1.3 Personalization SFP **ACF.1.4 Personalization SFP**	(246) **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 RADS. 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	(247) **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	(248) **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 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. (249) **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. (250) **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 RAD_S stored in the TOE. The function is executed in a secure manner. (251) **SF.PLATFORM** contributes to FDP_ACF.1.2 Signature Creation SFP satisfaction. The function acts as a support mechanism in the SCA authentication and for functionalities related to RAD objects.
	ACF.1.3 Signature Creation SFP	(252) **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.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	ACF.1.4 Signature Creation SFP	(253) **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 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. (254) **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. (255) **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 RAD_S stored in the TOE. The function is executed in a secure manner. (256) **SF.PLATFORM** contributes to FDP_ACF.1.4 Signature Creation SFP satisfaction. The function acts as a support mechanism in the SCA authentication processing and for functionalities related to RAD objects.
	ETC.1.1 SVD Transfer	(257) **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 TSC. (258) **SF.PLATFORM** 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	(259) **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 TSC. (260) **SF.PLATFORM** contributes to FDP_ETC.1.2 SVD Transfer satisfaction. The function acts as a support mechanism in the CGA authentication processing.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	ITC.1.1. DTBS	(261) **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. (262) **SF.PLATFORM** contributes to FDP_ITC.1.1. DTBS satisfaction. The function acts as a support mechanism in the SCA authentication processing.
	ITC.1.2. DTBS	(263) **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. (264) **SF.PLATFORM** contributes to FDP_ITC.1.2. DTBS satisfaction. The function acts as a support mechanism in the SCA authentication processing.
	ITC.1.3. DTBS	(265) **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. (266) **SF.PLATFORM** contributes to FDP_ITC.1.3. DTBS satisfaction. The function acts as a support mechanism in the SCA authentication processing.
	RIP.1.1	(267) **SF.DATA_ERASE** grants the FDP_RIP.1.1 satisfaction making unavailable any residual information related to the SCD/RAD/VAD.This function erase residual sensitive data before starting a new working session and before allocation and after deallocation of working data buffer indeed to contain sensitive data. (268) **SF.PLATFORM** contributes to FDP_RIP.1.1 satisfaction. The function acts as basic mechanisms required to assure residual sensitive data erasing and working data buffer clearing.
	SDI.2.1. Persistent	(269) **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. (270) **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. (271) **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. (272) **SF.PLATFORM** 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.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	SDI.2.2. Persistent	(273) **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. (274) **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. (275) **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. (276) **SF.PLATFORM** 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	(277) **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 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. (278) **SF.PLATFORM** contributes to FDP_SDI.2.1 DTBS satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.
	SDI.2.2. DTBS	(279) **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 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. (280) **SF.PLATFORM** contributes to FDP_SDI.2.2 DTBS satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	UIT.1.1 SVD Transfer	(281) **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 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. (282) **SF.PLATFORM** contributes to FDP_UIT.1.1 SVD Transfer satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.
	UIT.1.2 SVD Transfer	(283) **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 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. (284) **SF.PLATFORM** contributes to FDP_UIT.1.2 SVD Transfer satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.
	UIT.1.1 TOE DTBS	(285) **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 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. (286) **SF.PLATFORM** contributes to FDP_UIT.1.1 TOE DTBS satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.
	UIT.1.2 TOE DTBS	(287) **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 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. (288) **SF.PLATFORM** contributes to FDP_UIT.1.2 TOE DTBS satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
FIA	**AFL.1.1**	(289) **SF.AUTH** grants the FIA_AFL.1.1 satisfaction. This function addresses the user authentication. The user authentication is based on PIN mechanism. The 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. (290) **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. (291) **SF.PLATFORM** contributes to FIA_AFL.1.1 satisfaction. The function acts as a support mechanism for functionalities related to RAD objects.
	AFL.1.2	(292) **SF.AUTH** grants the FIA_AFL.1.2 satisfaction. This function addresses the user authentication. The user authentication is based on PIN mechanism. The 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. (293) **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. (294) **SF.PLATFORM** contributes to FIA_AFL.1.2 satisfaction. The function acts as a support mechanism for functionalities related to RAD objects.
	ATD.1.1	(295) **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	(296) **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 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.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	UAU.1.2	(297) **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 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	(298) **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 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	(299) **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 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.**	(300) **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.
	MSA.1.1 Administrator	(301) **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	(302) **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.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	MSA.2.1	(303) **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	(304) **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	(305) **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	(306) **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 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. (307) **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. (308) **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 RAD_S stored in the TOE. The function is executed in a secure manner. (309) **SF.PLATFORM** contributes to FMT_MTD.1.1 satisfaction. The function acts as a support mechanism for functionalities related to RAD objects.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	SMF.1.1	(310) **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. (311) **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	(312) **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	(313) **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**	(314) **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	(315) **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. (316) **SF.PLATFORM** contributes to FPT_EMESEC.1.1 satisfaction. The function acts as support mechanism preventing sensitive data to be disclose.
	EMSEC.1.2	(317) **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. (318) **SF.PLATFORM** contributes to FPT_EMESEC.1.2 satisfaction. The function acts as support mechanism preventing sensitive data to be disclose.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	FLS.1.1	(319) **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. (320) **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. (321) **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. (322) **SF.DATA_UPDATE** contributes to FPT_FLS.1.1 satisfaction. The function acts as a support mechanism. The function addresses the atomicity of the TOE transactions. (323) **SF.PLATFORM** 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	(324) **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. (325) **SF.INT_A** contributes to FPT_PHP.1.1 satisfaction. This function addresses the TOE data integrity. (326) **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. (327) **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. (328) **SF.PLATFORM** 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	(329) **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. (330) **SF.INT_A** contributes to FPT_PHP.1.2 satisfaction. This function addresses the TOE data integrity. (331) **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. (332) **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. (333) **SF.PLATFORM** 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	(334) **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. (335) **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. (336) **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. (337) **SF.PLATFORM** 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	(338) **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	(339) **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. (340) **SF.PLATFORM** 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
	TST.1.3	(341) **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. (342) **SF.PLATFORM** contributes to FPT_TST.1.2 satisfaction. The function acts as a support mechanism in the detection of TOE data integrity failures.
	ITC.1.1 SVD Transfer	(343) **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. (344) **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 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. (345) **SF.PLATFORM** contributes to FTP_ITC.1.1 SVD Transfer satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.
FTP	**ITC.1.2 SVD Transfer**	(346) **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. (347) **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 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. (348) **SF.PLATFORM** contributes to FTP_ITC.1.2 SVD Transfer satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	ITC.1.3 SVD Transfer	(349) **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. (350) **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 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. (351) **SF.PLATFORM** contributes to FTP_ITC.1.3 SVD Transfer satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.
	ITC.1.1 DTBS Import	(352) **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. (353) **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 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. (354) **SF.PLATFORM** contributes to FTP_ITC.1.1 DTBS Import satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	ITC.1.2 DTBS Import	(355) **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. (356) **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 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. (357) **SF.PLATFORM** contributes to FTP_ITC.1.2 DTBS Import satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.
	ITC.1.3 DTBS Import	(358) **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. (359) **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 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. (360) **SF.PLATFORM** contributes to FTP_ITC.1.3 DTBS Import satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE
	TRP.1.1 TOE	(361) **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. (362) **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 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. (363) **SF.PLATFORM** contributes to FTP_TRP.1.1 TOE satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.
	TRP.1.2 TOE	(364) **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. (365) **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 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. (366) **SF.PLATFORM** contributes to FTP_TRP.1.2 TOE satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.

FAMILY	SFRS	TOE SECURITY FUNCTIONS RATIONALE
	TRP.1.3 TOE	(367) **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. (368) **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 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. (369) **SF.PLATFORM** contributes to FTP_TRP.1.3 TOE satisfaction. The function acts as support mechanism during the usage of symmetric crypto algorithms.

Table 22: Functional requirements and TOE security function rational

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

Table 23: Functional requirements to TOE security functions mapping

	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.SIGN	SF.OBS_A	SF.INT_A	SF.DATA_ERASE	SF.DATA_UPDATE	SF.TEST	SF.EXCEPTION	SF.LIFE_CYCLE	SF.AC	SF.SM	SF.PLATFORM
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							√								√
	ITC.1.1 SVD Transfer	√													√	√
FTP	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 24: Functional requirements to TOE security functions mapping (continued)

13.5 PP claims Rationale

(370) The [SSCD_PP] §5 lists all of the SFRs included in this security target lite; this list includes all of the SFRs identified in the [SSCD_PP]. All of the operations applied to the SFRs are in accordance with the requirements of the [SSCD_PP].

14. QUALITY REQUIREMENTS

8.1 Revision History

Version	**Subject**
A	Initial Release

Table 25 - Revision History

15. ENVIRONMENTAL/ECOLOGICAL REQUIREMENTS

STMicroelectronics recommends viewing documents on the screen rather than printing to limit paper consumption.