STMicroelectronics

JSIGN4 Security Target Lite

Common Criteria for IT security evaluation

Rev. E
17-February-2022

INDEX

List of tables

List of figures

1. INTRODUCTION

1.1 Document Reference

Document identification: **JSIGN4 Security Target Lite**
Revision: **E**
Registration: **JSIGN4_SecurityTarget_Lite**

1.2 Security Target Reference

Document identification: **JSIGN4 Security Target**
Revision: **F**
Registration: **JSIGN4_Security_Target**

1.3 TOE Reference

- TOE Name and Version: **JSIGN4 V1.0.4**

2. SCOPE

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

TITLE: JSIGN4 - Security Target lite

3. PURPOSE

This document presents the Security Target Lite of JSIGN4 a smartcard application implementing a Secure Signature Creation Device (SSCD) with key generation and thrusted channel with Certificate Generation Application (CGA) and Signature Creation Application (SCA) and the application Italian National Service Card (see [CNS]) designed as a Java card applet integrated on STMicroelectronics Java Card platform designed for the STMicroelectronics ST31P450 ICC B04 (ST31P450 Security Integrated Circuit with dedicated software and embedded cryptographic library).

4. SCOPE

Due to the confidential nature of the contents, this document is intended for the sole use of Software Design Center (SDC) of STMicroelectronics srl - Marcianise (CE), the third-party laboratory and the certification body selected for the Common Criteria evaluation of the product.

5. REFERENCE DOCUMENTS

[ST31_DS] ST31P450 Data Sheet – Rev.2. January 2020

[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.

[REGEU_910/2014] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

[DECESE_650/2016] Commission Implementing Decision (EU) 2016/650 of 25 April 2016

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1 Revision 5. April 2017.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004.

[ETSI-ESI-Suites] ETSI Technical Specification – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites – ETSI TS 119 312 V1.3.1 (02-2019)

[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

[EN 419211-2] EN 419211-2 — Protection profiles for secure signature creation device — Part 2: Device with key generation - 2013

[EN 419211-4] EN 419211-4 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application - 2013

[EN 419211-5] EN 419211-5 — Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application - 2013

[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
[ISO_10116]	ISO/IEC 10116, Information technology - Security Techniques --Modes of operation of an n-bit block cipher, ISO, 2006
[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_PUB113]	FIPS 113: Computer Data Authentication (FIPS PUB 113), NIST, 30 May 1985
[FIPS_PUB180_1]	FIPS 180-1: Secure Hash Standard 17 April 1995
[FIPS_PUB180_2]	FIPS 180-2: Secure Hash Standard (SHS) 1 August 2002
[FIPS_PUB180_4]	FIPS 180-4: Secure Hash Standard (SHS) 5 August 2015
[PKCS1_v1_5]	PKCS #1 v1.5: RSA Encryption Standard – RSA Laboratories – 1 Nov 1993
[PKCS1_v2_2]	PKCS #1 v2.2: RSA Encryption Standard – RSA Laboratories – 27 October 2012
[RFC8017]	RSA Cryptography Specification Version 2.2 – November 2016
[FIPS_PUB_186-4]	FIPS PUB 186-4: Digital Signature Standard (DSS) – July 2013
[ANSI X9.62]	ANSI X9.62, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standard for Financial Services,2005
[SP800-67]	NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology
[FIPS_PUB197]	FIPS PUB 197: Advanced Encryption Standard – 26 November 2001
[SP800-38A]	NIST, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Special Publication 800-38A 2001 Edition
[STLite_ST31P450]	ST31P450 B04 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFIRE EV1 and MIFARE PLUS X Security Target for composition, Rev B04.1, August 2021.

[CNS]	CNS – Carta Nazionale dei Servizi – Functional Specification V1.1.6 – 02/04/2011
[NETLINK]	Requirements for Interoperability – Ref. NK/2/ZI/A/3/2.2.1 – Ver.2.2.1 – 24 Nov 2000

6. 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_93] and repealed by [REGEU_910/2014][DECESE_650/2016]) 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_93] repealed by [REGEU_910/2014][DECESE_650/2016])
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
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. Repealed by: • REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 • DECISIONE DI ESECUZIONE (UE) 2016/650 DELLA COMMISSIONE del 25 aprile 2016

Local User	User using the trusted path provided between the SCA in the TOE environment and the TOE.
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 JSIGN4 and used for signatory's authentication.
Qualified certificate	Means a certificate which meets the requirements defined in the [DIRECTIVE_93] repealed by [REGEU_910/2014][DECESE_650/2016] and is provided by a CSP who fulfils the requirements defined in the [DIRECTIVE_93] repealed by [REGEU_910/2014][DECESE_650/2016]
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 defined in the [DIRECTIVE_93] repealed by [REGEU_910/2014][DECESE_650/2016]
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.
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.
Signature Verification Data (SVD)	Means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.
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.
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 JSIGN4 this is synonym of PIN.

ACRONYMS	DEFINITION
AC	Access Conditions
BSO	Base Security Object
CC	Common Criteria
CGA	Certificate Generation Application
CNS	Carta Nazionale Servizi (National Services Card for Italian citizen)
CRT	Chinese Remainder Theorem
CSP	Certification Service Provider
DES	Data Encryption Standard
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
JCS	Java Card System
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
TDES	Triple Data Encryption Standard
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

7. JSIGN4 SECURITY TARGET LITE

7.1 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, Revision 5 Annex B “Specification of Security Targets” [CC1].
This Security Target (ST) is compliant to:

- Protection profiles for secure signature creation device — Part 2 - Device with key generation, [EN 419211-2],
- Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application [EN 419211-4]
- Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application [EN 419211-5]

Admissible algorithms and parameters for algorithms for secure signature-creation devices referred hereafter are derived from the document [ETSI-ESI-Suites].

7.2 ST and TOE Reference

(1) This Security Target provides a complete and consistent statement of the security enforcing functions and mechanisms of JSIGN4 (hereafter referred to as the TOE, i.e. the Target of Evaluation).
(2) The Security Target 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 lite and the TOE to which it refers.

ST Reference	
Title:	JSIGN4 - Security Target Lite
Assurance Level:	EAL 4 augmented with AVA_VAN.5
Company:	ST Microelectronics srl
CC Version:	3.1 Revision 5 [CC1][CC2][CC3]
PP Conformance:	Protection profiles for secure signature creation device — Part 2 - Device with key generation, [EN 419211-2] Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application [EN 419211-4] Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application [EN 419211-5]
Version:	Rev.E 17-February-2022
General Status:	Final
Related ST:	[STLite_ST31P450]

7.3 TOE Overview

(3) The TOE is the composition of an SW application with the secure IC STMicroelectronics ST31P450.

(4) The TOE is a smartcard SW application implementing a Secure Signature-Creation Device with key generation as described in [EN 419211-2], [EN 419211-4], [EN 419211-5] and CIE/CNS application (Italian identity and service citizen card see [CNS]) designed as a Java card applet integrated on STMicroelectronics Java Card platform designed for the STMicroelectronics ST31P450 ICC B04 (ST31P450 Security Integrated Circuit with dedicated software and embedded cryptographic library).

(5) Main TOE 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 CGA/SCA

(6) The TOE provides the following main features:

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

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

The TOE also includes an OS platform SW layer (JCS and Kernel) which provide optimized services for handling integrity of application-specific sensitive data, memory management functions, I/O functions that are compliant with ISO standards, atomic data transaction facilities, secure implementation of cryptographic functions and other proprietary functionalities. The proprietary functionalities provided from the OS platform include the secure data storage (integrity-protected arrays), secure data comparison of arrays, generation of random primes and multi data atomic transaction. Moreover, the OS platform tests and manages all the HW peripheral integrated in the ST31P450 ICC B04 .

(7) The STMicroelectronics secure microcontroller: ST31P450 ICC B04 is a hardware platform offering 450Kbytes of flash memory, 12Kbytes RAM and cryptographic support, especially designed for secure application based on high performance Public and Secret key algorithms (i.e. RSA, EC, TDES, AES). The hardware includes a public key cryptographic processor NESCRYPT able to handle operands up to 4096 bits, an AES and TDES accelerator (EDES+), 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 [ST31_DS].

The ST31P450 B04 Secured Microcontroller with Cryptographic Library has been certified by ANSSI (cert. report ANSSI-CC-2020/05 and maintenance report ANSSI-CC-2020/05-M01) with assurance level EAL5+: its associated Security Target Lite is [STLite_ST31P450].

8. TOE DESCRIPTION

(8) 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).

8.1 Product type

(9) The Target Of Evaluation (TOE) is a composite TOE which is the Secure Signature Creation Device (SSCD) with key generation and the secure IC STMicroelectronics ST31P450 B04:

(10) The TOE interacts with the external environment through the physical contact interfaces ISO/IEC-7816-3 and/or through the physical contactless interfaces ISO/IEC-14443 type B. The TOE provides the communication protocols T=0, T=1 and T=CL (contact-less).

8.2 TOE Reference

(11) JSIGN4 V1.0.4

8.3 TOE Delivery

- The Secure Signature Creation Device (SSCD) with key generation and with Application JSIGN4 on the Secured Microcontroller STMicroelectronics ST31P450 B04 with Cryptographic Library
- User and Administrator guidance delivered in paper and (.pdf) format.
    - JSIGN4 - Operational User Guidance Rev.B 27-September-2021
    - JSIGN4 - Preparative Procedures Rev.C 05-November-2021

The TOE will be delivered in two format:

- smartcard ID-1/Plug-in
- QFN32 or DFN8 plastic packages

8.4 TOE functionalities

(12) The TOE as multifunctional smartcard product is intended to provide all capabilities required for devices involved in creating qualified electronic signatures (see next figure to identify main TOE functional components and interfaces with TOE environment and TOE boundaries):

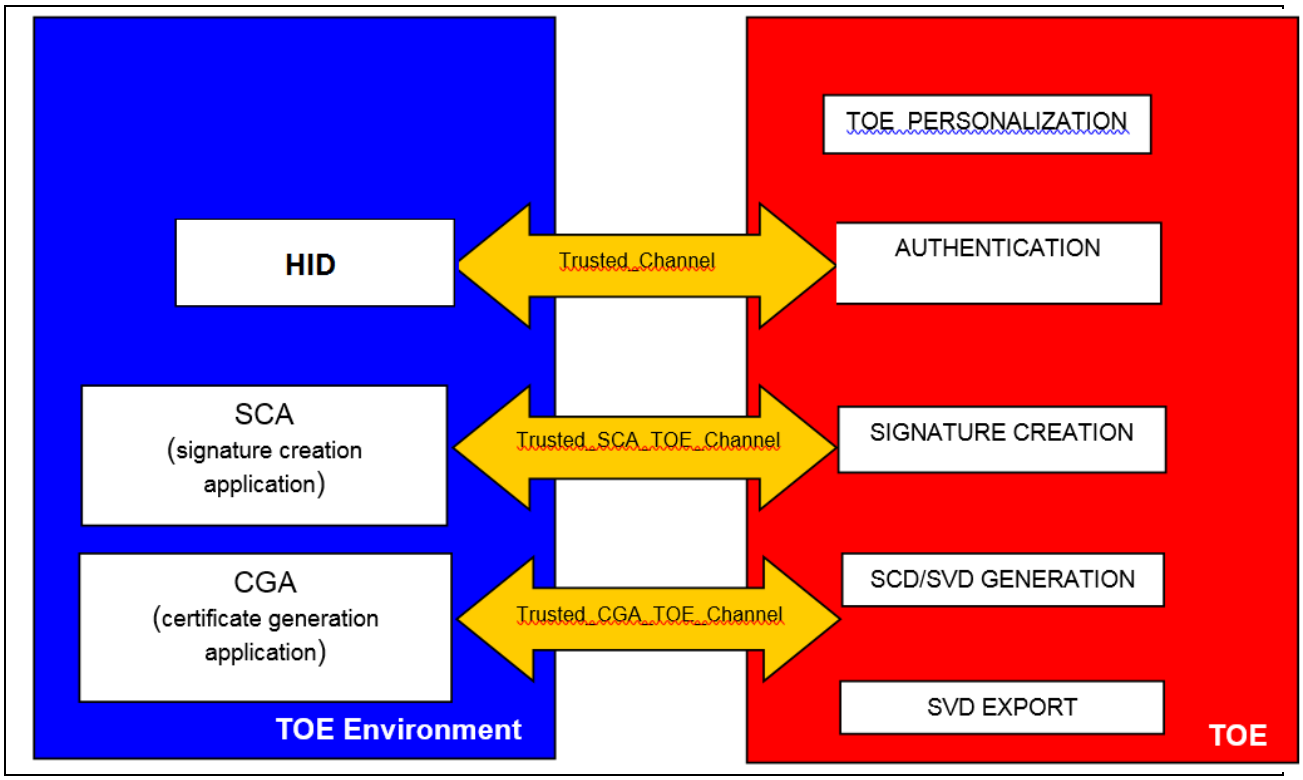


Figure 1: TOE environment and boundaries

(13) The CGA, the SCA are part of the immediate environment of the TOE.

(14) 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 File System creation and configuration via a Personalization application. See 8.5 for more details.

(15) 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.

(16) The TOE is able to generate internally its own signature keys (the SCD/SVD pair); in case of RSA key pair generation, the TOE only generates RSA keys in CRT format. Only internally generated key pair (the SCD/SVD pair) should be used for signature generation. 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.

(17) 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 (see [EN 419211-4]).

(18) The Administrator can generate and store in the TOE the signatory Reference Authentication Data (RAD)

(19) The Signatory can change/unblock his RAD stored in the TOE

(20) The signatory must be authenticated before signatures creation is allowed, for this reason the signatory sends his authentication data (VAD Verification Authentication Data e.g. a PIN) to the TOE using a trusted path between the interfaces device used and the TOE. The TOE compares the received VAD against the stored RAD if there is a match then the signatory is successful authenticated.

(21) The data to be signed (DTBS) or their representation (DTBS/R) 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 [EN 419211-5])

(22) The TOE is able to perform the signature operation using the RSA CRT and EC cryptographic algorithms and parameters agreed as suitable according to [PKCS1_v2_2][RFC8017][ANSI X9.62][FIPS_PUB_186-4].

(23) The TOE is able to perform crypto operations based on TDES, AES. The TOE support SHA-1, and SHA-256 for digest computation. The TOE also support a RNG.

(24) The TOE, when requested by the SCA, is able to generate data to be signed representation (DTBS/R) using a hash function agreed as suitable according to [ETSI-ESI-Suites]

(25) As depicted in the figure 2, JSIGN4 the Secure Signature Creation Device (SSCD) with key generation application is structured as a SW application in which functionalities are implemented as APDU commands compliant to ISO/IEC 7816 part 4 and 8 (see [ISO_7816_4][ISO_7816_8])

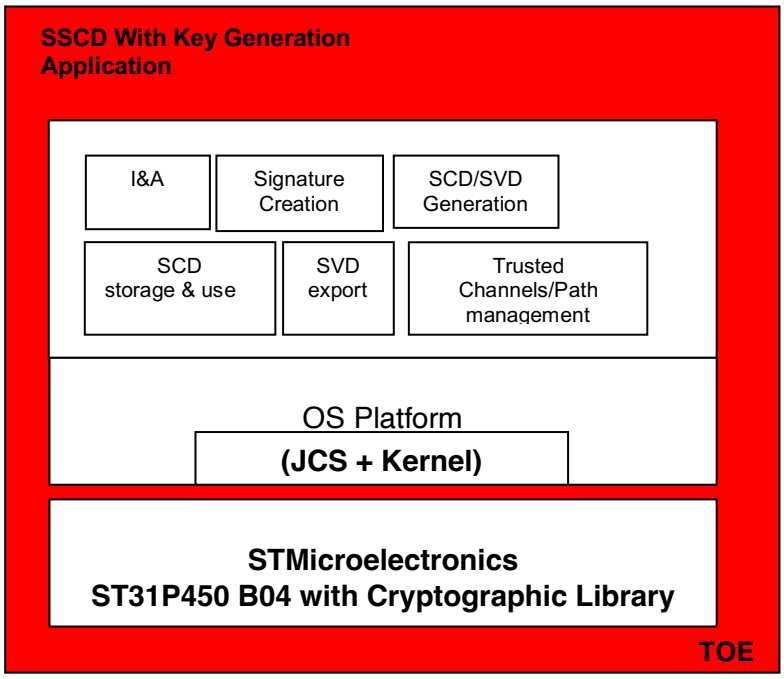


Figure 2: TOE components

8.5 TOE life cycle

(26) The typical TOE lifecycle is shown in Figure 3. Basically, it consists of a development phase and an usage phase. The Figure 3 also shows the correspondence between the TOE states and the states as reported in [EN 419211-2].

(27) TOE lifecycle states within the scope of the evaluation are those covered by [EN 419211-2], which refers to the usage phase. This phase represents installation, generation, start-up and operation in the CC terminology.

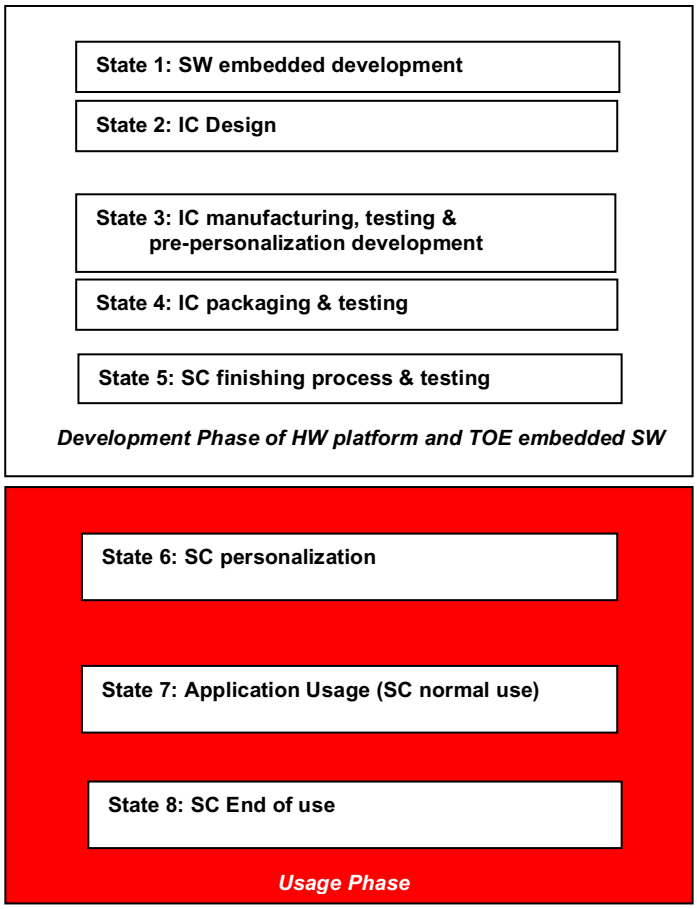


Figure 3: TOE life cycle

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

(29) The TOE states "**1-SW embedded development"** and **"2-IC Design"** correspond to the **"SSCD Development"** state in [EN 419211-2].

(30) The TOE is delivered from chip manufacturer (STMicroelectronics Rousset) to card manufacturer (STMicroelectronics Marcianise) after the completion of the states "3-**IC Manufacturing, testing and pre-personalization development"** and "4-**IC Packaging and & Testing"** which are part of the **"SSCD Production"** state in [EN 419211-2].

(31) The TOE is delivered to the card manufacturer (STMicroelectronics Marcianise) with a secret Reference Authentication Data (RAD) called Manufacturer Transport Secure Code (MTSC) to be used for card manufacturer identification and authentication.

(32) The state "**5-SC finishing process & Testing"** is managed by card manufacturer. This state corresponds to the **"SSCD Production"** state in [EN 419211-2]. In this state the TOE SSCD application with key generation is configured, eventually patches and/or code extensions are loaded in flash memory and finally a typical structure of the TOE file system can be loaded in the TOE memory according to TOE Guidance. At the end of these operations the flash memory

loader is locked (no more available) then the OS platform is configured (ATR, and other parameters) and finally locked, these steps are irreversible. At completion of finishing process step, the TOE operational phase can be entered. The hardware platform IC ST31P450 B04 has 450Kbytes of flash memory available.

(33) The TOE operational phase starts after TOE SSCD application with key generation and its HW platform ST31P450 B04 have been successfully designed, developed, manufactured, tested and initialized.

(34) The TOE is in **"6-SC personalization"** state at the beginning of TOE Operational phase.

(35) The TOE can be delivered to a "SSCD Provisioning Service Center". The card manufacturer (STMicroelectronics Marcianise) can also be act as a "SSCD Provisioning Service Center".

(36) 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 trusted channel (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 **"SSCD preparation"** state in [EN 419211-2].

(37) Moreover, in the state **"6-SC personalization"** the TOE administrator is in particular responsible for:

- Changing the default administrator Reference Authentication Data (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 Signatory 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. The import procedure is performed by the TOE administrator in a secured environment using the TOE available commands to create and import cryptographic keys.

(38) After completion of **"6-SC personalization"** state, the administrator change the TOE in state **"7-Application Usage (SC normal use)",** where the TOE can be used either by the Signatory or Administrator. The TOE can be delivered to the Signatory.

(39) In state **"7-Application Usage (SC normal use)"** the TOE allows the Signatory to:

- Change/Unblock the RAD_S 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
- Use the SCD stored in the TOE for signing DTBS and DTBS/R

This state corresponds to the **"SSCD operational use"** state in [EN 419211-2]

(40) When a failure occurs in state **"7-Application Usage (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 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 with key generation is no more available

- In all other cases in which the failure is recovered, the TOE remains in the state **"7-Application Usage (SC normal use)"**

(41) The state **"8-SC end of use"** of the TOE corresponds to the **"Destruction of SCD"** state in [EN 419211-2].

8.6 User and Administrator guidance

The user and administrator guidance (JSIGN4 - Operational User Guidance Rev.B and JSIGN4 - Preparative Procedures Rev.C) are TOE manuals 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.

8.7 TOE Environment

8.7.1 Development and Production Environment

(42) 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 site covered by ST31P450 ICC B04 certificate ANSSI-CC-2020/05 ANSSI-CC-2020/05-M01
5	SC finishing process & testing	Card Manufacturer	STMicroelectronics Marcianise (CE) Italy
6	SC personalization	TOE Administrator	STMicroelectronics Marcianise (CE) Italy or other qualified SSCD Provisioning Service Center or Certification authority.

9. PROTECTION PROFILE CLAIMS

9.1 CC conformance claim

(43) This ST is conformant with Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model Version 3.1 Revision 5 [CC1].

(44) This ST is conformant with Common Criteria for Information Technology Security Evaluation – Part 2: Security Functional Components Version 3.1 Revision 5 [CC2] with extension “FPT_EMSEC.1” made in the SSCD Protection Profile [EN 419211-2] and “FIA_API.1” made in the SSCD Protection Profile [EN 419211-4].

(45) This ST is conformant with Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Components Version 3.1 Revision 5 [CC3] package EAL 4 with augmentation AVA_VAN.5.

(46) This ST is strict conformant to the SSCD with key generation Protection Profiles [EN 419211-2], [EN 419211-4] and [EN 419211-5]

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

(48) The TOE meets the SSCD with key generation Protection Profiles [EN 419211-2], [EN 419211-4] and [EN 419211-5].

(49) The TOE is conformant with Common Criteria Version 3.1 part 2 and part 3 Revision 5 [CC2][CC3].

(50) The PART 2 extended with FPT_EMS.1 and FIA_API.1.

(51) The PART 3 conformant EAL4 augmented by AVA_VAN.5.

9.2 PP reference

(52) This ST is strict conformant to the SSCD with key generation Protection Profiles [EN 419211-2], [EN 419211-4] and [EN 419211-5]

9.3 PP tailoring

(53) Tables in chapter 13 identifies each SFR for this ST and the tailoring operations performed relative Protection Profiles [EN 419211-2], [EN 419211-4] and [EN 419211-5]. The tailoring is identified underlined within the text of each SFR. All of the tailoring operations performed are in conformance with the assignment and selections in [EN 419211-2], [EN 419211-4] and [EN 419211-5]

(54) This ST replaces the references to [DIRECTIVE_93] done in Protection Profiles [EN 419211-2], [EN 419211-4] and [EN 419211-5] with the references to [REGEU_910/2014][DECESE_650/2016]).

(55) In this ST the EAL4 assurance level is augmented with AVA_VAN.5.

10. SECURITY PROBLEM DEFINITION

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

10.1 Assets

(57) With regard to JSIGN4 implementation, assets that need to be protected by the TOE are here defined according to protection profiles [EN 419211-2], [EN 419211-4] and [EN 419211-5]. The following table summarizes them:

ASSET ACRONYM	ASSET DESCRIPTION	SECURITY NEED
SCD	Private key used to perform an electronic signature operation.	The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.
SVD	Public key linked to the SCD and used to perform electronic signature verification.	The integrity of the SVD when it is exported must be maintained.
DTBS and DTBS/R	Set of data, or its representation, which is intended to be signed.	Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.

10.2 Subjects

(58) In [EN 419211-2], [EN 419211-4] and [EN 419211-5] are defined subjects that can operate with the TOE.

SUBJECTS	DEFINITION
User	End user of the TOE who can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy
Administrator	User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator
Signatory	User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory

10.3 Threat agents

(59) In [EN 419211-2], [EN 419211-4] and [EN 419211-5] are defined malicious subjects that aim to attack the TOE.

THREAT AGENT	DEFINITION
Attacker	Human or process acting on their behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the electronic signature. The attacker has got a high attack potential and knows no secret

10.4 Threats to Security

(60) Threats are here reported for clarity as they are defined in [EN 419211-2], [EN 419211-4] and [EN 419211-5].

T.TYPE	THREAT
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 obtain 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 exported outside the TOE, which is a threat against the secrecy of the SCD.
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 is directed against SCD, SVD and DTBS.
T.SVD_Forgery	*Forgery of the signature-verification data* An attacker forges the SVD presented by the CSP to the CGA. This result in loss of SVD integrity in the certificate of the signatory.
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.
T.DTBS_Forgery	*Forgery of the DTBS/R* An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign.
T.Sig_Forgery	*Forgery of the electronic signature* An attacker forges a signed data object, maybe using an 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.

10.5 Organizational Security Policies

(61) As defined in [EN 419211-2], [EN 419211-4] and [EN 419211-5].

OSP	DEFINITION
P.CSP_QCert	*Qualified certificate* The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. [DIRECTIVE_93] and repealed by [REGEU_910/2014][DECESE_650/2016]) for the SVD generated by the SSCD. The certificates contain at least 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 as SSCD 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 an advanced electronic signature (cf. [DIRECTIVE_93] and repealed by [REGEU_910/2014][DECESE_650/2016]), which is a qualified electronic signature if it is based on a valid qualified certificate (cf. [DIRECTIVE_93] and repealed by [REGEU_910/2014][DECESE_650/2016]). The DTBS are

	presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.
P.Sigy_SSCD	*TOE as secure signature creation device* The TOE meets the requirements for an SSCD defined in [DIRECTIVE_93] and repealed by [REGEU_910/2014][DECESE_650/2016]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once
P.Sig_Non-Repud	*Non-repudiation of signatures* The lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate

10.6 Assumptions

(62) As defined in [EN 419211-2], [EN 419211-4] and [EN 419211-5]

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

11. SECURITY OBJECTIVES

11.1 Security objectives for the TOE

(63) Following table summarizes the security objectives for the TOE, as they are defined in [EN 419211-2] and add OT.TOE_SSCD_Auth (Authentication proof as SSCD), OT.TOE_TC_SVD_Exp (Trusted channel for SVD), OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import) and OT.TOE_TC_DTBS_Imp (Trusted channel for DTBS) as defined in [EN 419211-4] and [EN 419211-5].

OT.TYPE	TOE OBJECTIVE
OT.Lifecycle_Security	*Lifecycle security* The TOE shall detect flaws during the initialization, personalization and operational usage. The TOE shall securely destroy the SCD on demand of signatory **Application Note**: The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

OT.SCD/SVD_Auth_Gen	*Authorized SCD/SVD generation* The TOE shall provide security features to ensure that authorized users only may invoke the generation of the SCD and the SVD
OT.SCD_Unique	*Uniqueness of the signature creation data* The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation shall practically occur only once and shall not be reconstructable from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible.
OT.SCD_SVD_Corresp	*Correspondence between SVD and SCD* The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD
OT.SCD_Secrecy	*Secrecy of the signature creation data* The secrecy of the SCD (used for signature generation) shall be reasonably assured against attacks with a high attack potential. **Application note:** The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and secure destruction
OT.Sig_Secure	*Cryptographic security of the electronic signature* The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential
OT.Sigy_SigF	*Signature creation function for the legitimate signatory only* The TOE shall provide the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential
OT.DTBS_Integrity_TOE	*DTBS/R integrity inside the TOE* The TOE must not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation
OT.EMSEC_Design	*Provide physical emanations security* The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits
OT.Tamper_ID	*Tamper detection* The TOE shall provide system features that detect physical tampering of its components, and uses those features to limit security breaches
OT.Tamper_Resistance	*Tamper resistance* The TOE shall prevent or resist physical tampering with specified system devices and components
OT.TOE_SSCD_Auth	*Authentication proof as SSCD* The TOE shall hold unique identity and authentication data as SSCD and provide security mechanisms to identify and to authenticate itself as SSCD.

OT.TOE_TC_SVD_Exp	*TOE trusted channel for SVD export* The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the *TOE*.
OT.TOE_TC_VAD_Imp	*Trusted channel of TOE for VAD import* The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed. **Application note:** This security objective for the TOE is partly covering OE.HID_VAD from the core PP [EN 419211-2]. While OE.HID_VAD in the core PP [EN 419211-2] requires only the operational environment to protect VAD, the PP [EN 419211-5] requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore the PP [EN 419211-5] re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as *described* by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.
OT.TOE_TC_DTBS_Imp	*Trusted channel of TOE for DTBS import* The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE must not generate electronic signatures with the SCD for altered DTBS. **Application note:** This security objective for the TOE is partly covering OE.DTBS_Protect from the core PP [EN 419211-2]. While OE.DTBS_Protect in the core PP [EN 419211-2] requires only the operational environment to protect DTBS, the PP [EN 419211-5] requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore the PP [EN 419211-5] re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

11.2 Security objectives for the operational environment

(64) Following table summarizes the security objectives for the operational environment as defined in [EN 419211-2], [EN 419211-4] and [EN 419211-5]. As defined in [EN 419211-2] the security objective OE.Dev_Prov_Service replaces OE.SSCD_Prov_Service; in order to address the extended security functionality of the TOE and methods of use two security objectives are added OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp. As stated in [EN 419211-5], in order to address the new security functionality provided by the TOE, the security objectives OE.HI_VAD and OE.DTBS_Protect are redefined and changed in OE.HID_TC_VAD_Exp and OE.SCA_TC_DTBS_Exp respectively.

OE.SVD_Auth	*Authenticity of the SVD* The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence

	between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.
OE.CGA_QCert	*Generation of qualified certificates* The CGA shall generate qualified certificate that include (amongst others) a) the name of the signatory controlling the TOE, b) the SVD matching the SCD stored in the TOE and being under sole control of the signatory c) the advanced signature of the CSP The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a SSCD
OE.DTBS_Intend	*SCA sends data intended to be signed* The signatory shall use a trustworthy SCA that: • generates the DTBS/R 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, • sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE, • attaches the signature produced by the TOE to the data or provides it separately. **Application note**: The SCA should be able to support advanced electronic signatures. Currently, there exist three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CAdES, XAdES and PAdES. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.
OE.Signatory	*Security obligation of the signatory* The signatory shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The signatory shall keep their VAD confidential.
OE.Dev_Prov_Service	*Authentic SSCD provided by SSCD Provisioning Service* The SSCD Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, personalises the TOE for the legitimate user as signatory, links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the signatory. Note: This objective replaces OE.SSCD_Prov_Service from the core PP, which is possible as it does not imply any additional requirements for the operational environment when compared to OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_Service).
OE.CGA_SSCD_Auth	*Pre-initialisation of the TOE for SSCD authentication* The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSCD, successfully proved this identity as SSCD to the CGA, and whether this identity is linked to the legitimate holder of the device as applicant for the certificate.
OE.CGA_TC_SVD_Imp	*CGA trusted channel for SVD import* The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the SSCD.

OE.HID_TC_VAD_Exp	*Trusted channel of HID for VAD export* The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.
OE.SCA_TC_DTBS_Exp	*Trusted channel of SCA for DTBS export* The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

11.3 Security Objectives Rationale

11.3.1 Security Objectives backtracking

(65) The following table shows how the security objectives for the TOE and the security objectives for the operational environment cover the threats, organizational security policies and assumptions.

Threats - Assumptions – Policies Vs Security Objectives	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OE.SVD_Auth	OE.CGA_QCert	OE.DTBS_Intend	OE.Signatory	OE.Dev_Prov_Service	OE.CGA_SSCD_Auth	OE.CGA_TC_SVD_Imp	OE.HID_TC_VAD_Exp	OE.SCA_TC_DTBS_Exp
T.SCD_Divulg					x																			
T.SCD_Derive		x				x																		
T.Hack_Phys					x				x	x	x													
T.SVD_Forgery				x									x			x						x		
T.SigF_Misuse	x						x	x						x	x			x	x				x	x
T.DTBS_Forgery								x							x			x						x
T.Sig_Forgery			x			x											x							
P.CSP_QCert	x			x								x					x				x			
P.QSign						x	x										x	x						
P.Sigy_SSCD	x	x	x		x	x	x	x	x		x	x	x							x	x	x		
P.Sig_Non-Repud	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
A.CGA																x	x							
A.SCA																		x						

Table 1: Mapping of security problem definition to security objectives - Threats, Assumptions and Policy Vs Security objective

11.3.2 Security Objectives Sufficiency

(66) **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 [DIRECTIVE_93] (repealed by [REGEU_910/2014][DECESE_650/2016]). This threat is countered by OT.SCD_Secrecy, which assures the secrecy of the SCD used for signature creation.

(67) **T.SCD_Derive (***Derive the signature creation data***)** deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD.

T.SCD/SVD_Auth_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographically secure electronic signatures

(68) **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. OT.EMSEC_Design counters physical attacks through the TOE interfaces and observation of TOE emanations. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tampering attacks.

(69) **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.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA and verification of the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP. Additionally, T.SVD_Forgery is addressed by OT.TOE_TC_SVD_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA_TC_SVD_Imp, which provides verification of SVD authenticity by the CGA.

(70) **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 an electronic signature on data for which the signatory has not expressed the intent to sign, as required in [DIRECTIVE_93] (repealed by [REGEU_910/2014][DECESE_650/2016]). OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. OT.Sigy_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign. The combination of OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission form the SCA to the TOE. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) requires the HID to protect the confidentiality and the integrity of the VAD as needed by the authentication method employed. The HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD). OE.Signatory (Security obligation of the signatory) ensures that the signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD. OE.Signatory (Security obligation of the signatory) ensures also that the signatory keeps their VAD confidential.

(71) **T.DTBS_Forgery** *(Forgery of the DTBS/R)* addresses the threat arising from modifications of the DTBS/R sent to the TOE for signing which than does not correspond to the DTBS/R corresponding to the DTBS the signatory intends to sign. The threat T.DTBS_Forgery is addressed by the security objectives OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS), which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE. The TOE counters internally this threat by the means of OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensuring the integrity of the DTBS/R inside the TOE. The TOE IT environment also addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE.

(72) **T.Sig_Forgery (***Forgery of the electronic signature***)** deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique and OE.CGA_QCert address this threat in general. OT.Sig_Secure (*Cryptographic security of the electronic signature*) ensures by means of

robust cryptographic techniques that the signed data and the electronic signature are securely linked together. OT.SCD_Unique and ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

11.3.3 Enforcement of OSPs by security objectives

(73) **P.CSP_QCert** (*CSP generates qualified certificates*) provides that the TOE and the SCA may be employed to sign data with (qualified) electronic signatures, as defined by [DIRECTIVE_93] (repealed by [REGEU_910/2014][DECESE_650/2016]) refers to SSCDs to ensure the functionality of advanced signatures. The OE.CGA_QCert addresses the requirement of qualified (or advanced) electronic signatures as being based on qualified (or non-qualified) certificates. According to OT.TOE_SSCD_Auth the copies of the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD to prove this identity as SSCD to the CGA. The OE.CGA_SSCD_Auth ensures that the SP checks the proof of the device presented of the applicant that it is a SSCD. The OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE to the CGA corresponds to the SCD stored in the TOE and used by the signatory. The OT.Lifecycle_Security ensures that the TOE detects flaws during the initialisation, personalisation and operational usage.

(74) **P.QSign** (*Qualified electronic signatures*) provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

(75) **P.Sigy_SSCD** (*TOE as secure signature creation device*) requires the TOE to meet [DIRECTIVE_93] (repealed by [REGEU_910/2014][DECESE_650/2016]) is ensured by OT.SCD_Unique requiring that the SCD used for signature creation can practically occurs only once. The OT.SCD_Secrecy OT.Sig_Secure and OT.EMSEC_Design and OT.Tamper_Resistance address the secrecy of the SCD (cf. [DIRECTIVE_93] repealed by [REGEU_910/2014][DECESE_650/2016]). OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in [DIRECTIVE_93] (repealed by [REGEU_910/2014][DECESE_650/2016]) by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE. OT.Sigy_SigF meets the requirement in [DIRECTIVE_93] (repealed by [REGEU_910/2014][DECESE_650/2016]) by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others. OT.DTBS_Integrity_TOE meets the requirements in [DIRECTIVE_93] (repealed by [REGEU_910/2014][DECESE_650/2016]) as the TOE must not alter the DTBS/R. The usage of SCD under sole control of the signatory is ensured by OT.Lifecycle_Security, OT.SCD/SVD_Gen and OT.Sigy_SigF. OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised TOE from an SSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD. In the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA_SSCD_Auth and the received SVD is sent by this SSCD as required by OE.CGA_TC_SVD_Imp. Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

(76) **P.Sig_Non-Repud** *(Non-repudiation of signatures)* deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures generated with the TOE.

OE.Dev_Prov_Service (Authentic SSCD provided by SSCD Provisioning Service) ensures that the signatory uses an authentic TOE, initialised and personalised for the signatory.

OE.CGA_QCert (Generation of qualified certificates) ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory.

OE.SVD_Auth (Authenticity of the SVD) and OE.CGA_QCert (Generation of qualified certificates) require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) ensures that the SVD exported by the TOE corresponds to the SCD that is stored in the TOE.

OT.SCD_Unique (Uniqueness of the signature creation data) provides that the signatory's SCD can practically occur just once.

OE.Signatory (Security obligation of the signatory) ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD).

The TOE security feature addressed by the security objectives OT.TOE_SSCD_Auth (Authentication proof as SSCD) and OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export) supported by OE.Dev_Prov_Service (Authentic SSCD provided by SSCD Provisioning Service) enables the verification whether the device presented by the applicant is a SSCD as required by OE.CGA_SSCD_Auth (Pre-initialisation of the TOE for SSCD authentication) and the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA_TC_SVD_Imp (CGA trusted channel for SVD import).

OT.Sigy_SigF (Signature creation function for the legitimate signatory only) provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory (Security obligation of the signatory) ensures that the signatory keeps their VAD confidential.

The confidentiality of VAD is protected during the transmission between the HI device and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD).

OE.DTBS_Intend (SCA sends data intended to be signed), OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE), OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) and OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS.

The robust cryptographic techniques required by OT.Sig_Secure (Cryptographic security of the electronic signature) ensure that only this SCD may generate a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification.

The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

11.3.4 Upkeep of assumptions by security objectives

(77) **A.SCA** *(Trustworthy signature creation application)* establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by OE.DTBS_Intend *(Data intended to be signed*) which ensures that the SCA generates the DTBS/R of the data that have 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.

(78) **A.CGA** *(Trustworthy certificate 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 (Authenticity of the SVD), which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

12. EXTENDED COMPONENTS DEFINITION

(79) The additional family FPT_EMS (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, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.
To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

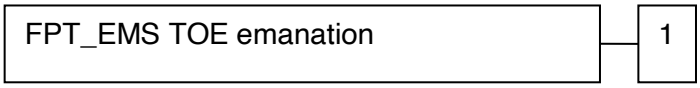
12.1 FPT_EMS TOE Emanation

The family "TOE Emanation (FPT_EMS)" is specified as follows.

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1
There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions identified that shall be auditable if FAU_GEN (Security audit data generation) is included in a PP or ST using FPT_EMS.1.

FPT_EMS.1 TOE Emanation

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

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

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

12.2 FIA_API Authentication Proof of Identity

The family “Authentication Proof of Identity (FIA_API)” is specified as follows.

Family behaviour:

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component leveling:

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

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

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

13. SECURITY REQUIREMENTS

(80) 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.

13.1 Security Functional Requirement

(81) 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 [EN 419211-2], [EN 419211-4] and [EN 419211-5].

(82) Common Criteria allow several operations to be performed on functional requirements; refinement, selection, assignment, and iteration. Operations completed in this ST are shown in underline.

(83) This paragraph fully restates TOE security functional requirements ([EN 419211-2], [EN 419211-4] and [EN 419211-5])

13.2 Cryptographic support (FCS)

(84)	**FCS_CKM.1 - Cryptographic key generation**	
	Hierarchical to: No other components. Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	
	FCS_CKM.1.1/RSA	The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm RSAGEN1[1] and specified cryptographic key sizes of 2048 bits[2] that meet the following: [ALGO_EC] par. 4.5.2.2[3].
	FCS_CKM.1.1/ECC	The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm ECGEN1[4] and specified cryptographic key sizes of 160,192,224,256,384, 512 and 521 bits[5] that meet the following: [ALGO_EC] par. 4.5.4.2[6].
(85)	**FCS_CKM.4 - Cryptographic key destruction**	
	Hierarchical to: No other components. Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	
	FCS_CKM.4.1	The TSF shall destroy cryptographic keys in case of regeneration of a new SCD in accordance with a specified cryptographic key destruction method irreversible deletion from the memory of the stored key value overwriting by zero bytes [7] that meets the following standard none[8].
(86)	**FCS_COP.1 - Cryptographic operation**	

[1] [assignment*: cryptographic algorithm*]
[2] [assignment*: cryptographic key sizes*]
[3] [assignment: *list of standards]*
[4] [assignment*: cryptographic algorithm*]
[5] [assignment*: cryptographic key sizes*]
[6] [assignment: *list of standards]*
[7] [assignment*: cryptographic key destruction method*]
[8] [assignment: *list of standards]*

	Hierarchical to: No other components. Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	
	FCS_COP.1.1/RSA	The TSF shall perform digital signature creation[9] in accordance with a specified cryptographic algorithm RSA[10] and cryptographic key sizes 2048[11] bits that meet the following: Public-Key Cryptography Standards (PKCS#1) : RSA Cryptography Specifications Version 2.2 - [PKCS1_v2_2][RFC8017].[12]
	FCS_COP.1.1/ECC	The TSF shall perform digital signature creation[13] in accordance with a specified cryptographic algorithm ECDSA[14] and cryptographic key sizes 160,192,224,256,384, 512 and 521 bits[15] that meet the following: [FIPS_PUB_186-4] [ANSI X9.62][16].
	FCS_COP.1.1/TDES	The TSF shall perform data encryption/decryption[17] in accordance with a specified cryptographic algorithm TDES ECB and TDES CBC[18] and cryptographic key sizes 112 and 168 bits[19] that meet the following: ISO/IEC 10116, Information technology - Security Techniques-Modes of operation of an n-bit block cipher and NIST, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Special Publication 800-38A 2001 Edition[20].
	FCS_COP.1.1/TDES MAC	The TSF shall perform MAC calculation[21] in accordance with a specified cryptographic algorithm TDES[22] and cryptographic key sizes 112 bits[23] that meet the following: ISO/IEC 9797-1[24].
	FCS_COP.1.1/AES MAC	The TSF shall perform MAC calculation[25] in accordance with a specified cryptographic algorithm AES[26] and cryptographic key sizes 128,192,256 bits[27] that meet the following: ISO/IEC 9797-1[28].

13.3 User Data Protection (FDP)

The security attributes and related status for the subjects and objects are:

SUBJECT OR OBJECT THE SECURITY ATTRIBUTE IS ASSOCIATED WITH	SECURITY ATTRIBUTE TYPE	VALUE OF SECURITY ATTRIBUTE
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD management	Authorized, not Authorized
SCD	SCD operational	No, yes
SCD	SCD identifier	Arbitrary value
SVD	Security attribute not defined	Security attribute not defined

[9] [assignment: *list of cryptographic operations*]
[10] [assignment*: cryptographic algorithm*]
[11] [assignment*: cryptographic key sizes*]
[12] [assignment: *list of standards]*
[13] [assignment: *list of cryptographic operations*]
[14] [assignment*: cryptographic algorithm*]
[15] [assignment*: cryptographic key sizes*]
[16] [assignment: *list of standards*]
[17] [assignment: *list of cryptographic operations*]
[18] [assignment*: cryptographic algorithm*]
[19] [assignment*: cryptographic key sizes*]
[20] [assignment: *list of standards*]
[21] [assignment: *list of cryptographic operations*]
[22] [assignment*: cryptographic algorithm*]
[23] [assignment*: cryptographic key sizes*]
[24] [assignment: *list of standards*]
[25] [assignment: *list of cryptographic operations*]
[26] [assignment*: cryptographic algorithm*]
[27] [assignment*: cryptographic key sizes*]
[28] [assignment: *list of standards*]

(87)	**FDP_ACC.1/SCD/SVD_Generation - Subset access control**	
	Hierarchical to: No other components. Dependencies: FDP_ACF.1 Security attribute based access control	
	FDP_ACC.1.1/ SCD/SVD_Generation	The TSF shall enforce the SCD/SVD Generation SFP [29] on 1. subjects: S.User, 2. objects: SCD, SVD, 3. operations: generation of SCD/SVD pair[30]
(88)	**FDP_ACF.1/SCD/SVD_Generation - Security attribute based access control**	
	Hierarchical to: No other components. Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	
	FDP_ACF.1.1/SCD/SVD_Generation	The TSF shall enforce the SCD/SVD Generation SFP[31] to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management"[32].
	FDP_ACF.1.2/SCD/SVD_Generation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute "SCD/SVD Management" set to "authorized" is allowed to generate SCD/SVD pair[33]
	FDP_ACF.1.3/SCD/SVD_Generation	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[34].
	FDP_ACF.1.4/SCD/SVD_Generation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute "SCD/SVD management" set to "not authorized" is not allowed to generate SCD/SVD pair[35].
	FDP_ACC.1/SVD_Transfer - Subset access control	
	Hierarchical to: No other components. Dependencies: FDP_ACF.1 Security attribute based access control	
	FDP_ACC.1.1/ SVD_Transfer	The TSF shall enforce the SVD Transfer SFP[36] on 1. subjects: S.User, 2. objects: SVD 3. operations: export[37].
	FDP_ACF.1/SVD_Transfer - Security attribute based access control	
	Hierarchical to: No other components. Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	

[29] [assignment: *access control SFP*]
[30] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[31] [assignment: *access control SFP*]
[32] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[33] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[34] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[35] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[36] [assignment: *access control SFP*]
[37] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

	FDP_ACF.1.1/SVD_Transfer	The TSF shall enforce the SVD Transfer SFP[38] to objects based on the following: 1. the S.User is associated with the security attribute Role, 2. the SVD [39].
	FDP_ACF.1.2/SVD_Transfer	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Admin and R.Sigy[40] is allowed to export SVD[41].
	FDP_ACF.1.3/SVD_Transfer	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[42].
	FDP_ACF.1.4/SVD_Transfer	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[43].
	FDP_ACC.1/Signature_Creation - Subset access control	
	Hierarchical to: No other components. Dependencies: FDP_ACF.1 Security attribute based access control	
	FDP_ACC.1.1/Signature_creation	The TSF shall enforce the Signature Creation SFP[44] on 1. subjects: S.User, 2. objects: DTBS/R, SCD, 3. operations: signature creation[45].
(89)	**FDP_ACF.1/Signature creation - Security attribute based access control**	
	Hierarchical to: No other components. Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	
	FDP_ACF.1.1/Signature_Creation	The TSF shall enforce the Signature Creation SFP[46] to objects based on the following: 1. the user S.User is associated with the security attribute “Role” and 2. the SCD with the security attribute “SCD Operational” [47].
	FDP_ACF.1.2/Signature_Creation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Sigy is allowed to create electronic signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “yes” [48]

[38] [assignment: *access control SFP*]

[39] assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

[40] [selection: *R.Admin,R.Sigy*]

[41] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[42] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

[43] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

[44] [assignment: *access control SFP*]

[45] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

[46] [assignment: *access control SFP*]

[47] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

[48] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

	FDP_ACF.1.3/Signature_Creation	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[49]
	FDP_ACF.1.4/Signature_Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no" [50]

(90)	**FDP_RIP.1 - Subset residual information protection**	
	Hierarchical to: No other components. Dependencies: No dependencies.	
	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[51] the following objects: SCD[52]. NOTE: The following data persistently stored by the TOE shall have the user data attribute "integrity checked persistent stored data": 1. SCD 2. SVD (if persistently stored by the TOE). The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data":
(91)	**FDP_SDI.2/Persistent - Stored data integrity monitoring and action**	
	Hierarchical to: FDP_SDI.1 Stored data integrity monitoring. Dependencies: No dependencies	
	FDP_SDI.2.1/Persistent	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[53] on all objects, based on the following attributes: integrity checked stored data[54]
	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 S.Sigy about integrity error[55]
(92)	**FDP_SDI.2/DTBS - Stored data integrity monitoring and action**	
	Hierarchical to: FDP_SDI.1 Stored data integrity monitoring. Dependencies: No dependencies	
	FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[56] on all objects, based on the following attributes: integrity checked stored DTBS[57]
	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 S.Sigy about integrity error[58]

[49] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[50] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[51] [selection: *allocation of the resource to, deallocation of the resource from*]
[52] [assignment: *list of objects*]
[53] [assignment: *integrity errors*]
[54] [assignment: *user data attributes*]
[55] [assignment: *action to be taken*]
[56] [assignment: *integrity errors*]
[57] [assignment: *user data attributes*]
[58] [assignment: *action to be taken*]

(93)	**FDP_UIT.1/DTBS - Data exchange integrity**	
	Hierarchical to: No other components. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	
	FDP_UIT.1.1/DTBS	The TSF shall enforce the Signature Creation SFP[59] to receive[60]user data in a manner protected from modification and insertion[61] errors.
	FDP_UIT.1.2/DTBS	The TSF shall be able to determine on receipt of user data, whether modification and insertion[62] has occurred
(94)	**FDP_DAU.2/SVD - Data Authentication with Identity of Guarantor**	
	Hierarchical to: FDP_DAU.1 Basic Data Authentication Dependencies: FIA_UID.1 Timing of identification	
	FDP_DAU.2.1/SVD	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of SVD[63]
	FDP_DAU.2.2/SVD	The TSF shall provide CGA[64] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence

13.4 Identification and Authentication (FIA)

(95)	**FIA_UID.1 - Timing of identification**	
	Hierarchical to: No other components. Dependencies: No dependencies.	
	FIA_UID.1.1	The TSF shall allow 1. Self-test according to FPT_TST.1, 2. none[65] 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.
(96)	**FIA_UAU.1 - Timing of authentication**	
	Hierarchical to: No other components. Dependencies: FIA_UID.1 Timing of identification.	
	FIA_UAU.1.1	The TSF shall allow 1. Self-test according to FPT_TST.1, 2. Identification of the user by means of TSF required by FIA_UID.1. 3. establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD 4. establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD[66] on behalf of the user to be performed before the user is authenticated.

[59] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[60] [selection: *transmit, receive*]
[61] [selection: *modification, deletion, insertion, replay*]
[62] [selection: *modification, deletion, insertion, replay*]
[63] [assignment: *list of objects or information types*]
[64] [assignment: *list of subjects*]
[65] [assignment: *list of TSF-mediated actions*]
[66] [assignment: *list of TSF-mediated actions*]

	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
(97)	**FIA_AFL.1 - Authentication failure handling**	
	Hierarchical to: No other components. Dependencies: FIA_UAU.1 Timing of authentication	
	FIA_AFL.1.1	The TSF shall detect when 3[67] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[68]
	FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met[69], the TSF shall block RAD[70]
(98)	**FIA_API.1 - Authentication Proof of Identity**	
	Hierarchical to: No other components. Dependencies: No dependencies	
	FIA_API.1.1	The TSF shall provide an Internal authentication command[71] to prove the identity of the SSCD[72]

13.5 Security Management (FMT)

(99)	**FMT_SMR.1 - Security roles**	
	Hierarchical to: No other components. Dependencies: FIA_UID.1 Timing of identification.	
	FMT_SMR.1.1	The TSF shall maintain the roles R.Admin and R.Sigy[73].
	FMT_SMR.1.2	The TSF shall be able to associate users with roles.
(100)	**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 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[74],
(101)	**FMT_MOF.1 - Management of security functions behaviour**	
	Hierarchical to: No other components. Dependencies: FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions.	

[67] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[68] [assignment: *list of authentication events*]
[69] [selection: *met, surpassed*]
[70] [assignment: *list of actions*]
[71] [assignment: authentication mechanism]
[72] [assignment: authorized user or rule]
[73] [assignment: *the authorized identified roles*]
[74] [assignment: *list of security management functions to be provided by the TSF*]

	FMT_MOF.1.1	The TSF shall restrict the ability to enable[75] the signature creation function[76] to R.Sigy[77].
(102)	**FMT_MSA.1/Admin - Management of security attributes**	
	Hierarchical to: No other components. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	
	FMT_MSA.1.1/Admin	The TSF shall enforce the SCD/SVD Generation SFP[78] to restrict the ability to modify[79] the security attributes SCD/SVD management[80] to R.Admin[81]
(103)	**FMT_MSA.1/Signatory - Management of security attributes**	
	Hierarchical to: No other components. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	
	FMT_MSA.1.1/Signatory	The TSF shall enforce the Signature Creation SFP[82] to restrict the ability to modify[83] the security attributes SCD operational[84] to R.Sigy[85]
(104)	**FMT_MSA.2 - Secure security attributes**	
	Hierarchical to: No other components. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	
	FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for SCD/SVD Management and SCD operational[86]
(105)	**FMT_MSA.3 - Static attribute initialization**	
	Hierarchical to: No other components. Dependencies: FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	
	FMT_MSA.3.1	The TSF shall enforce the SCD/SVD Generation SFP, SVD Transfer SFP and Signature Creation SFP[87] to provide restrictive [88] default values for security attributes that are used to enforce the SFP.
	FMT_MSA.3.2	The TSF shall allow the R.Admin[89] to specify alternative initial values to override the default values when an object or information is created.

75 [selection: *determine the behavior of, disable, enable, modify the behavior of*]
76 [assignment: *list of functions*]
77 [assignment: *the authorized identified roles*]
78 [assignment: *access control SFP(s), information flow control SFP(s)*]
79 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
80 [assignment: *list of security attributes*]
81 [assignment: *the authorized identified roles*]
82 [assignment: *access control SFP(s), information flow control SFP(s)*]
83 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
84 [assignment: *list of security attributes*]
85 [assignment: *the authorized identified roles*]
86 [selection: *list of security attributes*]
87 [assignment: *access control SFP, information flow control SFP*]
88 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
89 [assignment: *the authorized identified roles*]

(106)	**FMT_MSA.4 - Security attribute value inheritance**	
	Hierarchical to: No other components. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	
	FMT_MSA.4.1	The TSF shall use the following rules to set the value of security attributes: 1. If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation. 2. If S.Sigy successfully generates an SCD/SVD pair the security attribute "SCD operational of the SCD" shall be set to "yes" as a single operation. [90]
(107)	**FMT_MTD.1/Admin - Management of TSF data**	
	Hierarchical to: No other components. Dependencies: FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	
	FMT_MTD.1.1/Admin	The TSF shall restrict the ability to create[91] the RAD[92] to R.Admin[93]
(108)	**FMT_MTD.1/Signatory - Management of TSF data**	
	Hierarchical to: No other components. Dependencies: FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	
	FMT_MTD.1.1/Signatory	The TSF shall restrict the ability to modify and unblock[94] the RAD[95] to R.Sigy[96].

13.6 Protection of the TSF (FPT)

(109)	**FPT_EMS.1 - TOE Emanation**	
	Hierarchical to: No other components. Dependencies: No dependencies.	
	FPT_EMS.1.1	The TOE should not emit Side Channel Current and Electromagnetic emanation[97] in excess of limits exploitable by State of the Art attacks[98] enabling access to RAD[99] and SCD[100]
	FPT_EMS.1.2	The TOE shall ensure all users[101] are unable to use the following interface external contacts/contactless[102] to gain access to RAD[103] and SCD[104].

90 [assignment: *rules for setting the values of security attributes*]
91 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
92 [assignment: *list of TSF data*]
93 [assignment: *the authorized identified roles*]
94 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
95 [assignment: *list of TSF data*]
96 [assignment: *the authorized identified roles*]
97 [assignment: types of emissions]
98 [assignment: specified limits]
99 [assignment*: list of types of TSF data*]
100 [assignment*: list of types of user data*]
101 [assignment: type of users]
102 [assignment: type of connection]
103 [assignment*: list of types of TSF data*]
104 [assignment*: list of types of user data*]

(110)	**FPT_FLS.1 - Failure with preservation of secure state**	
	Hierarchical to: No other components. Dependencies: No dependencies.	
	FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. self-test according to FPT_TST fails, 2. power shortage, over voltage, over and under clock frequency, IC integrity problems. [105]
(111)	**FPT_PHP.1 - Passive detection of physical attack**	
	Hierarchical to: No other components. Dependencies: No dependencies.	
	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.
(112)	**FPT_PHP.3 - Resistance to physical attack**	
	Hierarchical to: No other components. Dependencies: No dependencies.	
	FPT_PHP.3.1	The TSF shall resist operating changes by the environment[106], to the clock, voltage supply and shield layers[107] by responding automatically such that the SFRs are always enforced
(113)	**FPT_TST.1 - TSF Testing**	
	Hierarchical to: No other components. Dependencies: No dependencies	
	FPT_TST.1.1	The TSF shall run a suite of self-tests during initial start-up or before calling a security sensitive module[108] to demonstrate the correct operation of the TSF[109].
	FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data[110].
	FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of TSF[111].

13.7 Trusted Path/Channels (FTP)

(114)	**FTP_ITC.1/SVD - Inter-TSF trusted channel**	
	Hierarchical to: No other components. Dependencies: No dependencies.	
	FTP_ITC.1.1/SVD	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.

[105] [assignment*: list of types of failures in the TSF*]
[106] [assignment: physical tampering scenarios]
[107] [assignment: list of TSF devices/elements]
[108] [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions* [assignment: *conditions under which self-test should occur*]]
[109] [selection: *[assignment: parts of TSF], the TSF*]
[110] [selection: *[assignment: parts of TSF data], TSF data*]
[111] [selection: *[assignment: parts of TSF], TSF*]

	FTP_ITC.1.2/SVD	The TSF shall permit another trusted IT product[112] to initiate communication via the trusted channel.
	FTP_ITC.1.3/SVD	The TSF or the **CGA** shall initiate communication via the trusted channel for 1. data Authentication with Identity of Guarantor according to FIA_API.1 and FDP_DAU.2/SVD, 2. export the SVD[113]
(115)	**FTP_ITC.1/VAD - Inter-TSF trusted channel - TC Human Interface Device**	
	Hierarchical to: No other components. Dependencies: No dependencies.	
	FTP_ITC.1.1/VAD	The TSF shall provide a communication channel between itself and another trusted IT product **HID** 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/VAD	The TSF shall permit the remote trusted IT product[114] to initiate communication via the trusted channel.
	FTP_ITC.1.3/VAD	The TSF **or the HID** shall initiate communication via the trusted channel for 1. User authentication according to FIA_UAU.1, 2. none[115]
(116)	**FTP_ITC.1/DTBS - Inter-TSF trusted channel - Signature creation Application**	
	Hierarchical to: No other components. Dependencies: No dependencies.	
	FTP_ITC.1.1/DTBS	The TSF shall provide a communication channel between itself and another trusted IT product **SCA** 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	The TSF shall permit the remote trusted IT product[116] to initiate communication via the trusted channel.
	FTP_ITC.1.3/DTBS	The TSF or the **SCA** shall initiate communication via the trusted channel for 1. signature creation, 2. DTBS/R transfer[117]

13.8 TOE Security Assurance Requirements

(117) TOE assurance requirements are stated in Table 2. The assurance requirements of this evaluation are EAL4 augmented by AVA_VAN.5.

ASSURANCE CLASS	ASSURANCE COMPONENTS

[112] [*selection: the TSF, another trusted IT product*]
[113] [assignment: *list of other functions for which a trusted channel is required*]
[114] [selection: *the TSF, another trusted IT product*]
[115] [assignment: *list of functions for which a trusted channel is required*]
[116] [selection: *the TSF, another trusted IT product*]
[117] [assignment: *list of other functions for which a trusted channel is required*]

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
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.
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

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

13.9 Security Requirements Rationale

(118) The security functional requirements with assignment, selection and refinement operations for the TOE are listed in 13.1 and they map exactly the functional requirements for the TOE [EN 419211-2], [EN 419211-4] and [EN 419211-5].

13.9.1 Security Requirements coverage

(119) The Table 3 is the mapping of TOE security functional requirements to the TOE security objectives

TOE SFR vs TOE Security Objectives	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FCS_CKM.1	x		x	x	x										
FCS_CKM.4	x				x										
FCS_COP.1	x					x						x	x	x	x
FDP_ACC.1/SCD/SVD_Generation	x	x													
FDP_ACC.1/SVD_Transfer	x												x		
FDP_ACC.1/Signature_Creation	x						x								
FDP_AFC.1/SCD/SVD_Generation	x	x													
FDP_AFC.1/SVD_Transfer	x												x		
FDP_AFC.1/Signature_Creation	x						x								
FDP_RIP.1					x		x								
FDP_SDI.2/Persistent				x	x	x									
FDP_SDI.2/DTBS							x	x							
FDP_UIT.1/DTBS															x
FDP_DAU.2/SVD													x		
FIA_UID.1		x					x								
FIA_AFL.1							x								
FIA_UAU.1		x					x					x			
FIA_API.1												x			
FMT_SMR.1	x						x								
FMT_SMF.1	x			x			x								
FMT_MOF.1	x						x								
FMT_MSA.1/Admin	x	x													
FMT_MSA.1/Signatory	x						x								
FMT_MSA.2	x	x					x								
FMT_MSA.3	x	x					x								
FMT_MSA.4	x	x		x			x								
FMT_MTD.1/Admin	x						x								
FMT_MTD.1/Signatory	x						x								
FPT_EMS.1					x				x						
FPT_FLS.1					x										
FPT_PHP.1										x					
FPT_PHP.3					x						x				
FPT_TST.1	x				x	x									
FTP_ITC.1/SVD													x		
FTP_ITC.1/VAD														x	
FTP_ITC.1/DTBS															x

Table 3: TOE Security functional requirements vs TOE Security Objectives

13.9.2 TOE Security Requirements sufficiency

(120) **OT.Lifecycle_Security** (*Lifecycle security*) is provided by the SFR for SCD/SVD generation FCS_CKM.1, SCD usage FCS_COP.1 and SCD destruction FCS_CKM.4 which ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer. The SCD usage is ensured by access control FDP_ACC.1/Signature_Creation, FDP_AFC.1/Signature_Creation which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMF.1 and FMT_SMR.1. The test functions FPT_TST.1 provides failure detection throughout the lifecycle.

(121) **OT.SCD/SVD_Auth_Gen** (*Authorized SCD/SVD generation*) addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The SFR FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute initialisation. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute “SCD operational” of the SCD.

(122) **OT.SCD_Unique (***Uniqueness of the signature creation data*) implements the requirement of practically unique SCD as laid down in [DIRECTIVE_93] (repealed by [REGEU_910/2014][DECESE_650/2016]), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

(123) **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. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT_SMF.1 and by FMT_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

(124) **OT.SCD_Secrecy** (*Secrecy of signature creation data*) is provided by the security functions specified by the following SFR. FCS_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. 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_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.
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_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).
SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

(125) **OT.Sig_Secure** (*Cryptographic security of the electronic signature*) is provided by the cryptographic algorithms specified by FCS_COP.1, which ensures the cryptographic robustness of the signature algorithms. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensures self-tests ensuring correct signature creation.

(126) **OT.Sigy_SigF** (*Signature creation function for the legitimate signatory only*) is provided by an SFR for identification authentication and access control. FIA_UAU.1 and FIA_UID.1 ensure that no signature creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process). The security functions specified by FDP_ACC.1/Signature_Creation and FDP_ACF.1/Signature_Creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory. FMT_MOF.1 restricts the ability to enable the signature creation function to the signatory. FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

(127) **OT.DTBS_Integrity_TOE** (*DTBS/R integrity inside the TOE*) ensures that the DTBS/R is not altered by the TOE. The integrity functions specified by FDP_SDI.2/DTBS require that the DTBS/R has not been altered by the TOE.

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

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

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

(131) **OT.TOE_SSCD_Auth** (*Authentication proof as SSCD*) requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by FIA_API.1 (Authentication Proof of Identity). The SFR FIA_UAU.1 allows (additionally to the core PP SSCD KG) establishment of the trusted channel before (human) user is authenticated. The basic security mechanisms are provided by FCS_COP.1.

(132) **OT.TOE_TC_SVD_Exp** (*TOE trusted channel for SVD export)* requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA, which is directly provided by

- The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer.
- FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor), which requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.
- FTP_ITC.1/SVD Inter-TSF trusted channel), which requires the TOE to provide a trusted channel to the CGA.
- FCS_COP.1 provides the basic security mechanisms to support the TOE thrusted channel.

- (133) **OT.TOE_TC_VAD_Imp** *(Trusted channel of TOE for VAD import)* is provided by FTP_ITC.1/VAD to provide a trusted channel to protect the VAD provided by the HID to the TOE. FCS_COP.1 provides the basic security mechanisms to support the TOE thrusted channel.

(134) **OT.TOE_TC_DTBS_Imp** *(Trusted channel of TOE for DTBS)* is provided by FTP_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by FDP_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS. FCS_COP.1 provides the basic security mechanisms to support the TOE thrusted channel.

The Table 4 and Table 5 below resume all the SFR SAR dependencies.

REQUIREMENT	DEPENDENCY	SATISFIED BY
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FDP_ACC.1/SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACC.1/SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_AFC.1/SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_AFC.1/SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDP_AFC.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_RIP.1	No dependencies	n/a
FDP_SDI.2/Persistent	No dependencies	n/a
FDP_SDI.2/DTBS	No dependencies	n/a
FDP_UIT.1/DTBS	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FDP_DAU.2/SVD	FIA_UID1	FIA_UID1
FIA_UID.1	No dependencies	n/a
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_API.1	No dependencies	n/a
FMT_SMF.1	No dependencies	n/a
FMT_SMR.1	FIA_UID1	FIA_UID1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory

FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FPT_EMS.1	No dependencies	n/a
FPT_FLS.1	No dependencies	n/a
FPT_PHP.1	No dependencies	n/a
FPT_PHP.3	No dependencies	n/a
FPT_TST.1	No dependencies	n/a
FTP_ITC.1/SVD	No dependencies	n/a
FTP_ITC.1/VAD	No dependencies	n/a
FTP_ITC.1/DTBS	No dependencies	n/a

Table 4: Satisfaction of dependencies of security functional requirements

ASSURANCE REQUIREMENT(S)	DEPENDENCY	SATISFIED BY
EAL4 package	(dependencies of EAL4 package are not reproduced here)	By construction, all dependencies are satisfied in a CC EAL package
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1 (all are included in EAL4 package)

Table 5: Satisfaction of dependencies of security assurance requirements

13.9.3 Rationale for chosen security assurance requirements

(135) The assurance level for this ST is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this ST is just such a product. Augmentation results from the selection of:

AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure.

14. TOE SUMMARY SPECIFICATION

(136) This section contains a high-level specification of each TOE Security Function (TSF) that contributes to satisfaction of the Security Functional Requirements of chapter 13.

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

(138) The TOE implements APDU commands compliant to ISO/IEC 7816 part 4 and 8 (see [ISO_7816_4][ISO_7816_8]. For details and format on APDU supported see JSIGN4 - Operational User Guidance.

(139) The TOE interacts with the external environment through the physical contact interfaces ISO/IEC-7816-3 and/or through the physical contactless interfaces ISO/IEC-14443 type B. The following communication protocols are supported: T=0,T=1 and T=CL (contact-less)..

(140) The TOE will be delivered in format: smartcard ID-1/Plug-in and QFN32 or DFN8 plastic packages.

(141) The Table 13 shows that all the SFRs are satisfied by at least one TSF and that every TSF is used to satisfy at least one SFR.

14.1 TOE Security Functions

(142) This part lists the TOE Security Functions. In the following TOE HARDWARE is intended the Integrated Circuit ST31P450 B04 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
OS PLATFORM	SF.OS_PLATFORM	Data integrity memory management, I/O functions, atomic data transaction, RNG, secure cryptographic functions, Test
TOE HARDWARE	SF.HARDWARE	Cryptographic support, TRNG Physical protection

Table 6: List of TOE security functions

14.1.1 Identification and authentication

SF.AUTH	
(143)	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 TDES with 2 or 3 keys, AES or RSA CRT with 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 functionalities are provided by TSF SF.OS_PLATFORM and by the Integrated Circuit ST31P450 B04 with embedded library functionalities and included in the SF.HARDWARE.

SF.RAD	
(144)	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 management are provided by TSF SF.OS_PLATFORM.

14.1.2 Access Control

SF.AC	
(145)	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

14.1.3 Key Management and Cryptography

SF.KEY_GEN	
(146)	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 [PKCS1_v2_2] [RFC8017]), using a length of 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 [FIPS_PUB_186-4][ANSI X9.62]), using a key length of sizes of 160,192,224,256,384,512 and 521 bits. The function checks the SCD/SVD correspondence. The RSA and EC key generation and SCD/SVD correspondence support is provided by TSF SF.OS_PLATFORM and by the Integrated Circuit ST31P450 B04 with embedded library functionalities and included in the SF.HARDWARE.

SF.HASH	
(147)	This function generates a hashing of data, using the algorithm SHA-1 or SHA-256 (see [FIPS_PUB180_2],[FIPS_PUB180_4]). 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 TSF SF.OS_PLATFORM and by the Integrated Circuit ST31P450 B04 with embedded library functionalities and included in the SF.HARDWARE.

SF.SIGN	
(148)	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 RSASSA-PKCS1-v1_5 and RSASSA-PSS (see [PKCS1_v2_2] [RFC8017]). The function signs imported data (DTBS/R), using ECC with private key length of 160,192,224,256,384,512 and 521 bits in conformance with the algorithm ECDSA (see [FIPS_PUB_186-4][ANSI X9.62]). The function is protected against the SPA/DPA/DFA attack The signature algorithm support is provided by the TSF SF.OS_PLATFORM and by the Integrated Circuit ST31P450 B04 with embedded library functionalities and included in the SF.HARDWARE.

14.1.4 Secure Messaging

SF.SM	
(149)	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 encipher of the transmitted message. This operation uses the TDES algorithm with 2 or 3 Keys (see [SP800-67]). The command authentication uses a cryptogram based on MAC. In case of an unsuccessful authentication the command is refused. This operation uses a TDES with 2 or 3 keys as defined in the standards [ISO_9797][FIPS_PUB113] to generate and verify 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 TSF SF.OS_PLATFORM and by the Integrated Circuit ST31P450 B04 with embedded library functionalities and included in the SF.HARDWARE.

14.1.5 Stored Data Protection

SF.OBS_A	
(150)	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 [ST31_DS][STLite_ST31P450] The basic mechanisms required to prevent data disclosure and leakage are provided by the TSF SF.OS_PLATFORM and by the Integrated Circuit ST31P450 B04 with embedded library functionalities and included in the SF.HARDWARE.

SF.INT_A	
(151)	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 value are written at NVM addresses 0x00800024 and 0x00800024. 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 SF.OS_PLATFORM and the Integrated Circuit ST31P450. The Integrated Circuit ST31P450 through the Flash Memory EDC error 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 TSF SF.OS_PLATFORM and by the Integrated Circuit ST31P450 B04 with embedded library functionalities and included in the SF.HARDWARE.

SF.DATA_ERASE
(152) 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 TSF SF.OS_PLATFORM and by the Integrated Circuit ST31P450 B04 with embedded library functionalities and included in the SF.HARDWARE.

SF.DATA_UPDATE
(153) 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 TSF SF.OS_PLATFORM and by the Integrated Circuit ST31P450 B04 with embedded library functionalities and included in the SF.HARDWARE.

14.1.6 Test

SF.TEST
(154) This function ensures the tests of TOE functionalities. It includes the test of Integrated Circuit ST31P450 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 TSF SF.OS_PLATFORM and by the Integrated Circuit ST31P450 B04 with embedded library functionalities and included in the SF.HARDWARE.

14.1.7 Failure

SF.EXCEPTION	
(155)	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 TSF SF.OS_PLATFORM and by the Integrated Circuit ST31P450 B04 with embedded library functionalities and included in the SF.HARDWARE.

14.1.8 TOE Life Cycle

SF.LIFE_CYCLE	
(156)	This function manages the TOE life cycle, as described in chapter 8.5 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.

14.1.9 TOE OS PLATFORM

SF.OS_PLATFORM	
(157)	This TSF is implemented at SW layer JCS and Kernel. Here the TSF is described as a single and cumulative security function representing the following sub-functions which services and characteristics are reported below in the description: **SF.SECURE_MANAGEMENT, SF.CRYPTO_KEY, SF.CRYPTO_OP, SF.PIN, SF.TRANSACTION and SF.OBJECT_DELETION**. The TSF provides optimized services for data integrity, memory management, I/O functions, atomic data transaction, cryptographic support, test and management of HW peripheral of Integrated Circuit ST31P450 B04 with embedded library. The TSF provide and manages the following functionalities: **Secure Management functionalities (SF.SECURE_MANAGEMENT) 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, NVM 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 NVM consistency/integrity check failure. **Crypto Key management functionalities (SF.CRYPTO_KEY) such as**: • key generation • key destruction • integrity and the unobservability of the keys. **Crypto Operation (SF.CRYPTO_OP):** functionalities of encryption/decryption and signature creation/verification with the support of the following algorithms: • TDES ECB and CBC with 16, 24 bytes of key • AES ECB and CBC with 128, 256 bits of key • RSA CRT with key length 1024 and 2048 bits • EC over GF(p) with key length up to 521 bits • Hashing • Deterministic Random Number Generation that meet NIST SP 800-90 – CTR_DRBG with AES-128 as block encryption primitive seeded with random numbers from the physical RNG of the hardware. **PIN management (SF.PIN)**: This functionality manages all operations related to PIN objects. In particular **SF.PIN** performs: PIN Verification, decreases the try counter of PINs in case of PIN verification failure and update PIN value and related try counter. PIN verification procedure consists in the comparison of the PIN provided by the TOE requesting the verification procedure with the PIN stored into a PIN object. SF.PIN guarantees the integrity of the stored PIN value, try counter and verification status. **Data Transaction management (SF.TRANSACTION):** functionalities concerning “persistent memory” changes in order to assures the coherence of the data if a failure occurs during their update **Secure data deletion (SF.OBJECT_DELETION):** de-allocation of memory resources of data no longer accessible. The security functionality also guarantees that, once the method has been invoked, information content of unreachable data cannot be retrieved anymore **HW Platform management**: HW initialisation, logical integrity, Memory manager, Physical tampering protection, Security violation administrator, Unobservability, The OS_Platform provides all the support and services to allow the TOE to interact with the external environment through the physical contact interfaces ISO/IEC-7816-3 and/or through the physical contactless interfaces ISO/IEC-14443 type B. The following communication protocols are supported: T=0, T=1 and T=CL (contact-less).

14.1.10 TOE HARDWARE

SF.HARDWARE

(158) The TSF manages all functionalities implemented by the platform IC ST31P450 B04 with embedded library functionalities. This includes:

- **IC CRYPTO LIBRARIES**: performs symmetric and asymmetric crypto operations. The algorithms supported are AES, TDES with key up to 192-bit and RSA with module up to 4096-bit, EC Cryptography over prime fields with curve order up to 521 bits. Other supported functions are the RSA key pair generation with module up to 4096-bit, ECDSA key generation and the SHA-1, SHA-2 hash function.
- **IC TRNG (Generators of Unpredictable Number)**: generates random numbers used for crypto computation. The generator is compliant with FIPS-142 and AIS31.
- **IC SENSORS**: detects physical integrity and critical operating conditions of the IC (Voltage, Clock frequency).
- **IC Security Manager**: detects memory access violation, bad CPU usage, bad NVM use etc.
- **IC data integrity**: allows the integrity verification of TOE die and TOE NVM.
- **IC data unobservability**: implements mechanisms to prevent data disclosure.

The following platform IC ST31P450 TSF are relevant to the composite TOE:

- **TSF Limited fault tolerance:** The TSF provides limited fault tolerance, by managing a certain number of faults or errors preventing risk of malfunction
- **TSF Failure with preservation of secure state:** The TSF provides preservation of secure state by detecting and managing the following events, resulting in an immediate interruption or reset: Die integrity violation detection, Errors on memories, Glitches, High voltage supply, CPU errors, MPU errors, External clock incorrect frequency, Sequence control, etc.
- **TSF Test and Loader:** The TSF ensures that only very limited test capabilities are available in User configuration. The TSF ensures that the Secure Flash Loader and the final test capabilities are unavailable in User configuration. The TSF ensures the switching and the control of TOE configuration.
- **TSF data confidentiality and integrity monitoring:** The TSF ensures confidentiality of the User Data in all the memories where it can be stored. The TSF ensures stored User data integrity, in all the possible memory areas.
- **TSF resistance to physical attack and internal data transfer protection:** The TSF ensures resistance to physical tampering, thanks to countermeasures that reduce the exploitability of physical probing and by active shields that command an automatic reaction on die integrity violation detection. The TSF prevents the disclosure of internal and user data thanks to: Memories scrambling and encryption, Bus encryption, Mechanisms for operation execution concealment, etc.
- **TSF Random number generation:** The TSF provides 8-bit true random numbers that can be qualified with the test metrics required by the standard [BSI_AIS31] for a PTG.2 class device.
- **TSF Symmetric Key Cryptography:** AES and TDES operations. The AES accelerator provides the following standard AES cryptographic operations for key sizes of 128, 192 and 256 bits, conformant to FIPS PUB 197 with intrinsic countermeasures against attacks: cipher, inverse cipher. The AES accelerator can operate in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode. The TSF provides optionally an EDES accelerator that has the capability to perform TDES encryption and decryption in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode conformant to [SP800-38A]
- **TSF Asymmetric Key Cryptography:** The TSF provides the following RSA functions all conformant to [PKCS1_v2_2]: RSA public key cryptographic operation for modulus sizes up to 4096 bits, RSA private key cryptographic operation with or without CRT for modulus sizes up to 4096 bits, RSA signature formatting, RSA Key Encapsulation Method. The TSF provides the following efficient basic functions for Elliptic Curve Digital Signature Algorithm (ECDSA) generation and verification, as stipulated in [FIPS_PUB_186-4][ANSI X9.62] with Elliptic Curves over prime fields on curves in Weierstrass form.
- **TSF Cryptographic operation: SHA-1 & SHA-2 operation:** The TSF provides the SHA-1, SHA-256 secure hash functions conformant to [FIPS_PUB180_2].
- **TSF Cryptographic key generation: Prime generation and RSA Key Generation:** The TSF provides prime numbers generation for prime sizes up to 2048 bits. The TSF provides standard RSA public and private key computation for key sizes up to 4096 bits.

15. STATEMENT OF COMPATIBILITY CONCERNING COMPOSITE SECURITY TARGET

(159) This is a Statement of Compatibility between this Composite ST and the ST of platform Integrated Circuit ST31P450 B04 with embedded library and Hardware functionalities from now on referred to as Platform ST [STLite_ST31P450]The following mappings regarding SFRs, threats, assumptions, organizational security policies and objectives demonstrate the compatibility between the Composite Security Target and the Platform ST [STLite_ST31P450]

(160) The following table lists the Integrated Circuit ST31P450 B04 Platform Security Functionalities relevant for the Composite TOE. Any other Platform's TSF not referred in the Table 7 has to be considered not relevant for the composite TOE.

Platform Security Functionality
TSF Limited fault tolerance
TSF Failure with preservation of secure state
TSF Test and Loader
TSF data confidentiality and integrity monitoring
TSF resistance to physical attack and internal data transfer protection
TSF Random number generation
TSF Symmetric Key Cryptography
TSF Asymmetric Key Cryptography
TSF Cryptographic operation: SHA-1 & SHA-2 operation
TSF Cryptographic key generation: Prime generation and RSA Key Generation

Table 7 - Platform Security Functionality relevant for the composite TOE

(161) Any other Platform's TSF not referred in the Table 7 has to be considered not relevant for the composite TOE because they are functionalities used only by the IC ST31P450 B04 platform Firmware/Software (Security IC Embedded Software) and not used by the composite TOE

(162) The Table 8 is the mapping of composite TOE SARs with Integrated Circuit ST31P450 B04 Platform SARs

Composite TOE SAR	IC ST31P450 B04 Platform SAR
ASE	

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	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.2 - TOE summary specification with architectural design summary
ALC	
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	ALC_CMC.4 - Production support, acceptance procedures and automation ALC_CMS.5 - Development tools CM coverage ALC_DEL.1 - Delivery procedures ALC_DVS.2 - Sufficiency of security measures ALC_LCD.1 - Developer defined life-cycle model ALC_TAT.2 - Compliance with implementation standards
AGD	
AGD_PRE.1 - Preparative procedures AGD_OPE.1 - Operational user guidance	AGD_PRE.1 - Preparative procedures AGD_OPE.1 - Operational user guidance
ADV	
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	ADV_ARC.1 - Security architecture description ADV_FSP.5 - Complete semi-formal functional specification with additional error information ADV_IMP.1 - Implementation representation of the TSF ADV_TDS.4 – Semiformal modular design ADV_INT.2 - Well-structured internals
ATE	
ATE_COV.2 - Analysis of coverage ATE_DPT.1 - Testing: basic design ATE_FUN.1 - Functional testing ATE_IND.2 - Independent testing – sample	ATE_COV.2 - Analysis of coverage ATE_DPT.3 - Testing: modular design ATE_FUN.1 - Functional testing ATE_IND.2 - Independent testing – sample
AVA	
AVA_VAN.5 - Advanced methodical vulnerability analysis	AVA_VAN.5 - Advanced methodical vulnerability analysis

Table 8 - Platform SARs Vs Composite TOE SARs

(163) The table below shows the mapping between the Integrated Circuit ST31P450 B04 Platform SFRs and the Composite ST SFRs.

IC ST31P450 B04Platform SFRs	Composite TOE SFRs
FPT_FLS.1 - Failure with preservation of secure state	**FPT_FLS.1**
FPT_PHP.3 - Resistance to physical attack	**FPT_PHP.1, FPT_PHP.3**
FDP_SDI.2 - Stored data integrity monitoring and action	**FDP_SDI.2**
FDP_ITT.1 - Basic internal transfer protection FPT_ITT.1 - Basic internal TSF data transfer protection FDP_IFC.1 - Subset information flow control	**FPT_EMS.1**
FCS_RNG.1 - Random number generation	**FPT_TST.1, FTP_ITC.1/SVD, FTP_ITC.1/VAD, FTP_ITC.1/DTBS**
FCS_COP.1 - Cryptographic operation FCS_SAS.1 - Audit storage	**FCS_COP.1, FDP_UIT.1/DTBS, FIA_UAU.1, FIA_API.1**
FCS_CKM.1 - Cryptographic key generation	**FCS_CKM.1**
The following IC ST31P450 B04 platform SFRs are considered RP_SFR_MECH for the composite TOE because of their security properties providing protection against attacks to the TOE as a whole: **FRU_FLT.2, FMT_LIM.1/Test, FMT_LIM.2/Test, FMT_LIM.1/Loader, FMT_LIM.2/Loader, FDP_SDC.1, FDP_SDI.2, FDP_ITT.1,** **FPT_ITT.1, FDP_IFC.1, FDP_ACC.1/Memories, FDP_ACF.1/Memories, FMT_MSA.3/Memories, FMT_MSA.1/Memories,** **FMT_SMF.1/Memories, FDP_ACC.1/Loader, FDP_ACF.1/Loader, FMT_SMR.1/Loader, and FIA_UID.1/Loader**	
The following IC ST31P450 B04 platform SFRs are considered RP_SFR_SERV for the composite TOE: **FAU_SAS.1, FPT_FLS.1, FPT_PHP.3, FDP_SDI.2, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FCS_RNG.1, FCS_COP.1, FCS_CKM.1**	
The other IC ST31P450 B04 platform SFRs are considered IP_SFR for the composite TOE	

Table 9 - Platform SFRs VS Composite TOE SFRs

Additional Composite TOE SFRs
FCS_CKM.4
FDP_ACC.1/SCD/SVD_Generation
FDP_ACC.1/SVD_Transfer
FDP_ACC.1/Signature_Creation
FDP_AFC.1/SCD/SVD_Generation
FDP_AFC.1/SVD_Transfer
FDP_AFC.1/Signature_Creation
FDP_RIP.1
FDP_DAU.2/SVD
FIA_UID.1
FIA_AFL.1
FMT_SMF.1
FMT_SMR.1
FMT_MOF.1
FMT_MSA.1/Admin
FMT_MSA.1/Signatory
FMT_MSA.2
FMT_MSA.3
FMT_MSA.4
FMT_MTD.1/Admin
FMT_MTD.1/Signatory

Table 10 – Additional composite TOE SFRs

(164) There is no conflict between security objectives of the Composite TOE ST and the IC ST31P450 B04 Platform ST. A mapping between security objectives of the Composite TOE and the security objectives for the Platform is reported in Table 11.

IC ST31P450 B04 Platform security Objectives	**Composite TOE security** Objectives
BSI.O.Identification - TOE Identification	**OT.TOE_SSCD_Auth**
BSI.O.Leak-Inherent - Protection against Inherent Information Leakage **BSI.O.Leak-Forced** - Protection against Forced Information Leakage	**OT.SCD_Secrecy** **OT.EMSEC_Design**
BSI.O.Phys-Probing - Protection against Physical Probing **BSI.O.Phys-Manipulation** - Protection against Physical Manipulation **BSI.O.Abuse-Func** - Protection against Abuse of Functionality **AUG4.O.Mem Access** - Dynamic Area based Memory Access Control	**OT.Tamper_ID** **OT.Tamper_Resistance**
BSI.O.RND - Random Numbers	**OT.TOE_TC_SVD_Exp** **OT.TOE_TC_VAD_Imp** **OT.TOE_TC_DTBS_Imp**
AUG1.O.Add-Functions - Additional Specific Security Functionality	**OT.Sig_Secure** **OT.SCD_SVD_Corresp** **OT.DTBS_Integrity_TOE** **OT.SCD_Unique** **OT.TOE_SSCD_Auth** **OT.TOE_TC_SVD_Exp** **OT.TOE_TC_VAD_Imp** **OT.TOE_TC_DTBS_Imp**
BSI.O.Malfunction - Protection against Malfunctions **BSI.O.Cap-Avail-Loader** - Capability and Availability of the Loader	**OT.Lifecycle_Security**
	Additional composite TOE Objectives **OT.SCD/SVD_Auth_Gen** **OT.Sigy_SigF**

Table 11 – Platform security Objectives Vs Composite TOE security Objectives

Any other Platform's Security Objective not referred in the Table 11 has to be considered not relevant for the composite TOE

(165) There is no conflict between security objectives for the environment of the Composite TOE ST and the security objectives for the environment of the IC ST31P450 B04 Platform ST.

IC ST31P450 B04 Platform Objectives for the Environment	Composite TOE Objectives for the Environment/Composite SARs
BSI.OE.Resp-Appl - Treatment of User Data	**OE.CGA_SSCD_Auth** **OE.CGA_TC_SVD_Imp**
BSI.OE.Process-Sec-IC - Protection during composite product manufacturing	**OE.CGA_SSCD_Auth** **OE.CGA_TC_SVD_Imp** **OE.Dev_Prov_Service**
BSI.OE.Lim-Block-Loader - Limitation of capability and blocking the Loader	**Covered by following SAR:** **ALC_LCD** **NOTE:** The blocking of flash memory loader and the blocking of OS platform are performed at the end of **"5-SC finishing process & Testing" life cycle state**. It is managed by the card manufacturer (STMicroelectronics srl) in a secured environment. The blocking operations are irreversible.
	Additional composite TOE Objective for environment **OE.SVD_Auth** **OE.CGA_QCert** **OE.DTBS_Intend** **OE.Signatory** **OE.HID_TC_VAD_Exp** **OE.SCA_TC_DTBS_Exp**

Table 12 – Platform OEs Vs Composite TOE OEs

Any other Platform's Security Objective for the environment not referred in the Table 12 has to be considered not relevant for the composite TOE

16. RATIONALE

16.1 TOE Summary Specification Rationale

(166) 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.

(167) 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.

16.1.1 TOE Security Functions rationale

Following Table 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:

	TOE Security Functions	I &A		Key and Crypto			Stored Data Protection				TST, FAIL, LIFE CYCLE, AC, SM, PLATFORM, 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.OS_PLATFORM	SF.HARDWARE
FCS	FCS_CKM.1			√												√	√
	FCS_CKM.4								√							√	
	FCS_COP.1			√	√											√	√
FDP	FDP_ACC.1/SCD/SVD_Generat.	√	√											√		√	
	FDP_ACC.1/SVD_Transfer	√	√											√		√	
	FDP_ACC.1/Signature_Creation	√	√											√		√	
	FDP_AFC.1/SCD/SVD_Generation	√	√											√		√	
	FDP_AFC.1/SVD_Transfer	√	√											√		√	
	FDP_AFC.1/Signature_Creation	√	√											√		√	
	FDP_RIP.1								√							√	
	FDP_SDI.2/Persistent							√				√	√			√	√
	FDP_SDI.2/DTBS														√	√	√
	FDP_UIT.1/DTBS														√	√	√
	FDP_DAU.2/SVD					√										√	√
FIA	FIA_UID.1	√															
	FIA_AFL.1	√	√													√	
	FIA_UAU.1	√															
	FIA_API.1	√															
FMT	FMT_SMF.1	√												√			
	FMT_SMR.1													√			
	FMT_MOF.1													√			
	FMT_MSA.1/Admin													√			
	FMT_MSA.1/Signatory													√			
	FMT_MSA.2													√			
	FMT_MSA.3													√			
	FMT_MSA.4													√			
	FMT_MTD.1/Admin	√	√											√		√	
	FMT_MTD.1/Signatory	√	√											√		√	
FPT	FPT_EMS.1						√									√	√
	FPT_FLS.1									√	√	√	√			√	√
	FPT_PHP.1							√			√	√	√			√	√
	FPT_PHP.3										√	√	√			√	√
	FPT_TST.1							√			√					√	√
FTP	FTP_ITC.1/SVD	√													√	√	√
	FTP_ITC.1/VAD	√													√	√	√
	FTP_ITC.1/DTBS	√													√	√	√

Table 13: Functional requirements to TOE security functions mapping

17. QUALITY REQUIREMENTS

17.1 Revision History

Version	Subject
A	Initial Release – 13-December-2021
B	Release – 11-January-2022 Added ICC version number
C	Release – 02-February-2022 Update HW ANSSI Surveillance report
D	Release – 07-February-2022
E	Update HW ANSSI Maintenance report Final Release – 17-February-2022

Table 14 - Revision History

18. ENVIRONMENTAL/ECOLOGICAL REQUIREMENTS

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