UM_security_target_lite_ePKI_KeyImp

User manual

ST-Doc ePKI KeyImp on STeID JC Open OS v1.0 - Security Target Lite

Common Criteria
for IT security evaluation

1 Purpose

This document presents the Security Target of the ST-Doc ePKI KeyImp - Secure Signature Creation Device (SSCD) with Key Import on STeID JC Open OS v1.0, implementing a Secure Signature Creation Device (SSCD) in key import configuration.

2 Scope

This document is public.

3 Reference documents

Table 1: List of reference CC documents

Reference	Document
[CC_P1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017
[CC_P2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1 Revision 5. April 2017
[CC_P3]	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
[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
[SOGIS-COMP]	Composite product evaluation for Smart Cards and similar devices, version 1.5.1, May 2018
[CERT_ST31N600]	ST31N600 A03, ANSSI - CC - 2022/21 - R02
[CERT_ STeID_JCOS]	SteID JC Open OS v1.0, v1.3.2, NSCIB-CC-2400079-01

Table 2: List of reference Protection Profiles and Technical Guidelines

Reference	Document
[CC_PP_0075]	BSI-CC-PP-0075-2012-MA-01 EN 419211-3 — Protection profiles for secure signature creation device — Part 3: Device with key import – 2013 [PP0075]
[CC_PP_SCA_0076]	BSI-CC-PP-0076-2013-MA-01 EN 419211-6:2014 — Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application
[CC_PP-0055]	CC Protection Profile – Machine Readable Travel Document with “ICAO Application", Basic Access Control – Version 1.10, 25 March 2009
[CC_PP-0056]	CC Protection Profile – Machine Readable Travel Document with “ICAO Application", Extended Access Control with PACE – Version 1.3.2, 5 December 2012
[CC_PP-0068]	CC Protection Profile – Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP). BSI-CC-PP-0068-V2-2011 – Version 1.0, November 2011
[CC_PP-0086]	BSI-CC-PP-0086-2015, Common Criteria Protection Profile / Electronic document implementing Extended Access Control Version 2 (EAC2) based on BSI TR-03110 (EAC2_PP), BSI, Version 1.01, 2015-05-20
[ICAO_9303]	ICAO Doc 9303, Machine Readable Travel Documents – Part 10 Logical Data Structure (LDS) for Storage of Biometric and Other Data in the Contactless Integrated Circuit (IC) – Eighth Edition, 2021
	ICAO Doc 9303, Machine Readable Travel Documents – Part 11 Security Mechanisms for MRTDs – Eighth Edition, 2021
	ICAO Doc 9303, Machine Readable Travel Documents – Part 12 Public Key Infrastructure for MRTDs – Eighth Edition, 2021
[ICAO_TR]	TECHNICAL REPORT – Supplemental Access Control for Machine Readable Travel Documents – Version 1.1 – April 15, 2014
[TR-03110-1]	Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20. March 2012
[TR-03110-2]	Technical Guideline TR-03110-2: Advanced Security Mechanisms for Machine Readable Travel Documents Part 2, Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-03-20
[TR-03110-3]	Technical Guideline TR-03110-2: Advanced Security Mechanisms for Machine Readable Travel Documents Part 2, Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-03-20
[TR-03111]	Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 1.11, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-04-17

Table 3: List of reference Specifications

Reference	Document
[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
[ETSI-ESI-Suites]	ETSI Technical Specification – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites – ETSI TS 119 312 V1.3.1 (02-2019)
[ALGO_DS]	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
[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]	ISO/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
[FIPS_PUB113]	FIPS 113: Computer Data Authentication (FIPS PUB 113), NIST, 30 May 1985
[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
[PKCS_#3]	Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, November 1, 1993
[RFC8017]	RSA Cryptography Specification Version 2.2 – November 2016
[RFC3447]	NWG Request For Comments 3447 – February 2003
[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
[AIS20/31]	Bundesamt fuer Sicherheit in der Informationstechnik. AIS20/31: A proposal for: Functionality classes for random number generators, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, September 18th, 2011.
[SP-800-22]	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications – Rev.1 – April 2010

Table 4: List of reference STMicroelectronics documents

Reference	Document
[ST_SteidJCOS]	STMicroelectronics, STeID JC Open OS v1.0 Security Target, Version H, 2025-10-24
[AGD_PRE]	STMicroelectronics, ST-Doc ePKI on STeID JC Open OS - Preparative User Guidance for EPKIApplet, Rev.2 – January, 2026
[AGD_OPE]	STMicroelectronics, ST-Doc ePKI on STeID JC Open OS - Operational User Guidance for EPKIApplet, Rev.2 – January, 2026

4 Abbreviations

Term	Definition
AC	Access Conditions
CC	Common Criteria
CGA	Certificate Generation Application
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
HID	Human Interface Device
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
OS	Operating System
RAD	Reference Authentication Data
RADs	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

SecDO	Security Data Object
SF	Security Function
SFP	Security Function Policy
SM	Secure Messaging
SSCD (the TOE)	Secure Signature Creation Device
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

5 Glossary

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] and [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] and [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 STEID_EPKI 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] and [DECESE_650/2016], and is provided by a CSP who fulfils the requirements defined in the [DIRECTIVE_93] repealed by [REGEU_910/2014] and [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 STEID_EPKI this is synonym of PIN.

6 Introduction

The ST-Doc ePKI KeyImp, Secure Signature Creation Device (SSCD) with Key Import, is a Java Card Applet that implements SSCD application supporting thrusted channel with both the Certificate Generation Application (CGA) and the Signature Creation Application (SCA). It is based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) and supports the Extended Access Control (EAC), the Password Authenticated Connection Establishment (PACE) and the Chip Authentication (CA), as described in the 'ICAO Doc 9303' [ICAO_9303]. Moreover, the applet supports user authentication by PACE PIN and PACE PUK.

The applet is integrated with the CC certified STMicroelectronics Java Card™ operating system 'STeID JC Open OS v1.0' [ST_SteidJCOS], designed on the CC certified STMicroelectronics ST31N600 Security Integrated Circuit [CERT_ST31N600].

The TOE certification depends on the certification of the platform 'STeID JC Open OS v1.0' [CERT_ STeID_JCOS].

This document is the Security Target for the Common Criteria evaluation of the ST-Doc ePKI - Secure Signature Creation Device (SSCD) with Key Import on STeID JC Open OS v1.0. It provides information about the Target of Evaluation (TOE), that is the item subject of the Common Criteria evaluation. The TOE is evaluated in composition with the STMicroelectronics Java Card Platform STeID JC Open OS.

6.1 ST Reference

Title:	ST-Doc ePKI KeyImp – Secure Signature Creation Device (SSCD) with Key Import on STeID JC Open OS v1.0 – Security Target Lite
Developer:	STMicroelectronics, Z.I. Marcianise Sud, 81025, Marcianise (CE), ITALY
Version:	Rev. C
Date:	January , 2026

6.2 TOE Reference

TOE Name:	ST-Doc ePKI KeyImp - Secure Signature Creation Device (SSCD) with Key Import
TOE Version:	1.0
com.st.steid.bsi version:	1.4
com.st.steid.epki version:	1.5

The TOE is subject to a composite certification based on the CC certified STMicroelectronics Java Card Platform 'STeID JC Open OS v1.0' [ST_SteidJCOS] with CC certificate number NSCIB-CC-2400079-01

The ST-Doc ePKI KeyImp, Secure Signature Creation Device (SSCD) with Key Import, is made of two Java Card packages: the com.st.steid.bsi library package and the com.st.steid.epki package containing the EPKIApplet class that implements the SSCD application.

The TOE version 1.0 contains the com.st.steid.bsi and the com.st.steid.epki packages with version defined above. The TOE version can be verified using the GET_DATA command. In fact, the concatenation of the two versions is returned by that command, according to the instructions in section "TOE identification" of the Preparative User Guidance for EPKIApplet of this TOE [AGD_PRE].

6.3 Platform Reference

STeID JC Open OS v1.0 on ST31N600 Security Integrated Circuit

OS Identification:	00000900
OS Version:	00010302
CC certificate	[CERT_ STeID_JCOS]

OS Identification and OS Version can be verified using the GET_DATA command according to the instructions in the section "TOE identification" of the Preparative User Guidance of this TOE [AGD_PRE].

6.4 TOE Overview

The TOE is the STMicroelectronics ST-Doc ePKI KeyImp - Secure Signature Creation Device (SSCD) with Key Import, integrated with the STMicroelectronics Java Card™ operating system STeID JC Open OS v1.0, designed on the STMicroelectronics ST31N600 Security Integrated Circuit.

It is a Java Card Applet that implements Secure Signature Creation Device (SSCD) application supporting thrusted channel with both the Certificate Generation Application (CGA) and the Signature Creation Application (SCA). It is based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) and supports the Extended Access Control (EAC), the Password Authenticated Connection Establishment (PACE) and the Chip Authentication (CA), as described in the 'ICAO Doc 9303' [ICAO_9303]. Moreover, the applet supports user authentication by PACE PIN and PACE PUK.

The TOE is a contact/ contactless smartcard.

The TOE is evaluated according to the composition approach.

6.4.1 TOE Description

The TOE is a composite product comprising hardware, software and documentation.

The physical scope is defined as follows:

1. Certified platform (hardware and software): the STMicroelectronics Java Card™ Operating System STeID JC Open OS v1.0 on the STMicroelectronics ST31N600 Secure Integrated Circuit [ST_SteidJCOS]
2. Software: the STMicroelectronics TOE Java Card applet EPKIApplet implementing a Secure Signature-Creation Device with key import and implementing the advanced security methods, Extended Access Control (EAC), the Password Authenticated Connection Establishment (PACE), Chip Authentication (CA)
3. Documentation:
   - ST-Doc ePKI on STeID JC Open OS - Preparative User Guidance for EPKIApplet [AGD_PRE]
   - ST-Doc ePKI on STeID JC Open OS - Operational User Guidance for EPKIApplet [AGD_OPE]

The platform guidance, as described in the ST of the platform [ST_SteidJCOS], is also included

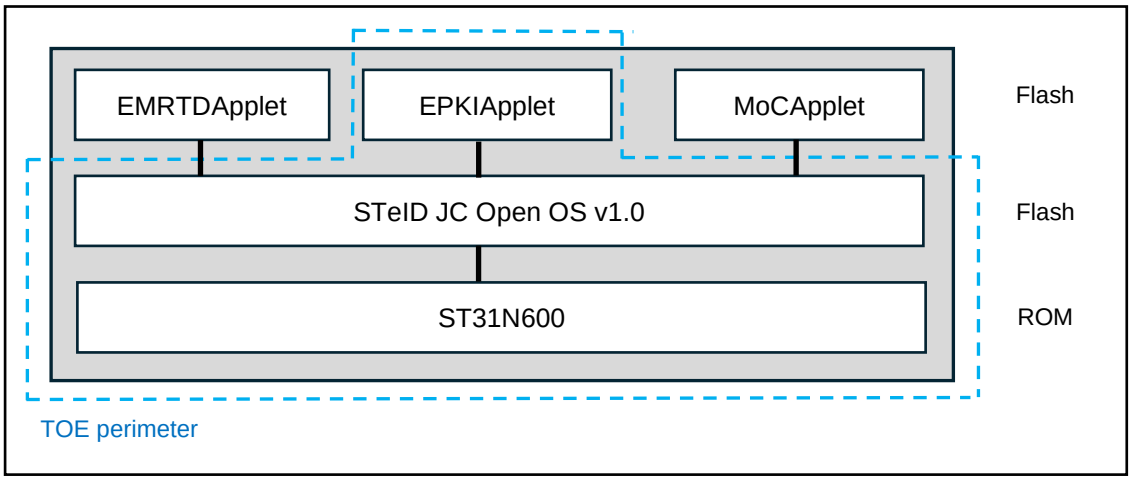
The first two components of the TOE, that is the hardware and the software, are delivered in wafer or micromodule D70, D76, CB6 format by trusted couriers. The last component of the

TOE (that is the documentation) is delivered, by trusted couriers or in enciphered pdf format by e-mail.

The delivery occurs at the end of the step 3 “IC manufacturing & testing” (see section 6.4.3).

The Figure 1 shows the composition of the TOE parts, including their location in the memory areas of the TOE. The TOE is a Java Card Flash memory-based product.

Figure 1: TOE architecture



Important note: The TOE is an open Java Card implementation including pre-loaded packages of EPKIApplet, EMRTDApplet, and MoCApplet. The EMRTDApplet and the MoCApplet are out of the scope of the TOE. The pre-loaded applets are installed and initialized in step 5 “SSCD initialization & pre-personalization” of the TOE lifecycle (see section 6.4.3). Upgrading of the applets and loading of further applets post-issuing is possible.

The STeID JC Open OS Operating System and the EPKIApplet Java Card applet are loaded in the non-volatile memory (NVM) of the IC during the manufacturing phase.

The EPKIApplet uses the IC RAM and NVM for storage of operational and permanent data, to provide security functionality.

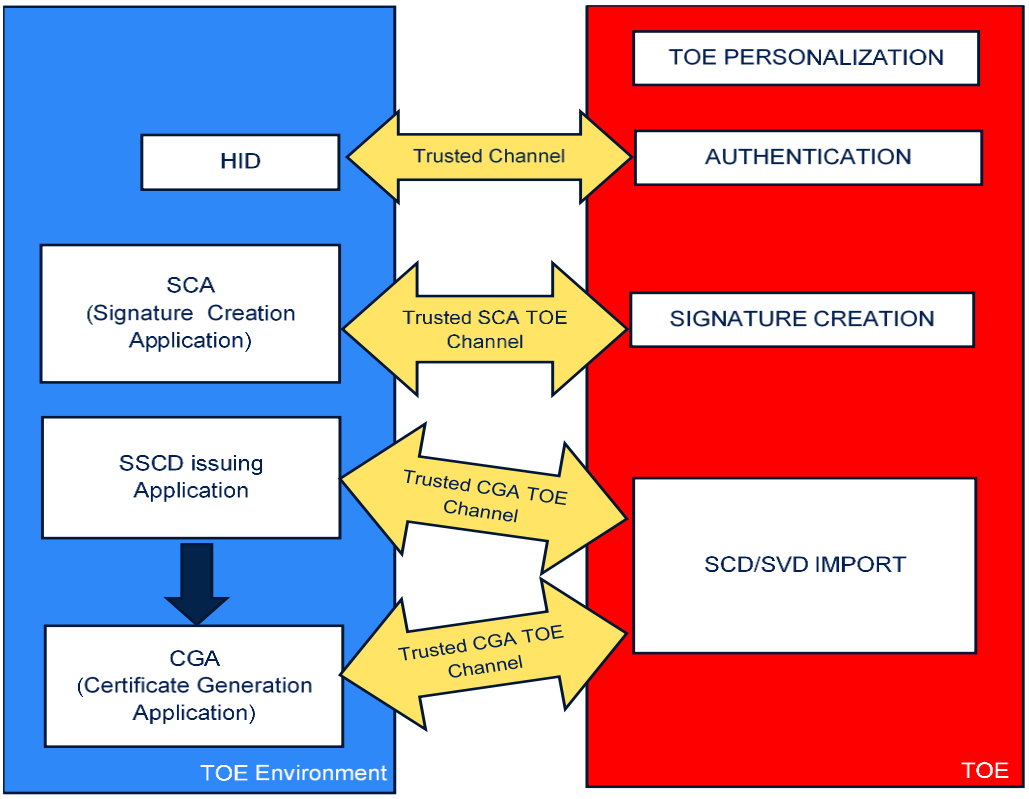
During operational use phase the EPKIApplet interacts with other external entities.

This composite ST is based on the ST of the underlying STeID JC Open OS [ST_SteidJCOS].

6.4.2 TOE Functionalities

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 2: TOE environment and boundaries



The CGA and the SCA are part of the immediate environment of the TOE.

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 Preparative User Guidance of the TOE [AGD_PRE] for more details.

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.

The TOE can import signing key (SCD/SVD pair). In case of RSA key pair importation, the TOE only imports RSA keys in CRT format. The imported key pair (the SCD/SVD pair) should be used for signature generation. An authorized Administrator uses the CGA to initiate SCD/SVD importation along with the corresponding certificate. The TOE provides a trusted channel to maintain the confidentiality and the integrity of the imported key pair (see PP SCD with key import and SCA [CC_PP_SCA_0076]).

The Administrator can generate and store in the TOE the signatory Reference Authentication Data (RAD). The Signatory can change/unblock his RAD stored in the TOE.

The Signatory must be authenticated before signatures creation is allowed, for this reason the signatory uses his authentication data (VAD Verification Authentication Data e.g. a PIN) to establish a trusted path between the interface's device used and the TOE and to authenticate himself with PACE PIN. Then TOE compares the received VAD against the stored RAD, the PIN_{QES}, if there is a match then the signatory is successful authenticated.

The data to be signed (DTBS) or their representation (DTBS/R) are transferred by the SCA to the TOE only over a trusted channel to maintain their integrity. The same channel is used to return the signed data object (SDO) from the TOE to the SCA (see [CC_PP_SCA_0076])

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], and [FIPS_PUB_186-4].

The TOE can perform crypto operations based on TDES, AES. The TOE supports SHA-1, SHA-256, SHA-384 and SHA-512 for digest computation. The TOE also supports RNG.

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

6.4.2.1 Security features and access control

The TOE supports the following methods:

1) **PACE** protocol according to [TR-03110-1], [TR-03110-2], [ICAO_TR] for:

- the identification and authentication of the user as the legitimate card holder
- the establishment of a trusted channel between the terminal and the card
- the protection against tracking and eavesdropping

The TOE provides the following secrets to be used within the PACE protocol (PIN_{QES} assigns an additional password for authentication to create qualified electronic signatures):

Table 5: Secrets used within PACE protocol

Secret	Minimum Length	Initial value set by	Used to authenticate for
PIN	5 digits	Administrator on personalization	Advanced signature creation Signature key importation Certificate Import Verification of PIN_{QES} Change reference data of PIN_{QES} Change reference data of PIN
PUK	8 digits	Administrator on personalization	Reset retry counter of PIN Reset retry counter of PIN_{QES} PIN activation, deactivation Change reference data of PIN
CAN	6 digits	Administrator on personalization	Verification of PIN_{QES} Change reference data of PIN_{QES} Unblock PIN and PUK

PIN is protected against denial-of-service attacks by setting the chip into a suspended state, before the retry counter of the secret in question is exhausted after consecutive failed authentication attempts. Before the very last retry to authenticate against PIN or PUK, respectively, can be done, an authentication against CAN must be performed.

2) **Chip Authentication Version 1** according to **[TR-03110-1]**, to
   - proof the authenticity of the chip to the terminal
   - establish a trusted channel between the terminal and the card

3) **Terminal Authentication Version 1** according to **[TR-03110-1]** to restrict, optionally, the access to authorized SCAs and CGAs.

To create an electronic signature, the legitimate user must authenticate himself against the RAD, which consists of one or more secrets stored on the chip. The RAD also ensures that the SSCD is in a non-operational state when delivered to the signatory. In the preparation phase (see [AGD_PRE]) CAN and PUK are set in the personalization step and delivered to the signatory. The creation of a qualified electronic signature is additionally protected by the secret PIN_{QES}, which is a password with a minimum length of 6 digits stored on the chip The secrets must be activated by the signatory on first usage. For this, authentication against PUK is required. Table 3.2 lists all keys and the corresponding RADs:

Table 6: Signature keys and corresponding RADs

DS Key Usage	Corresponding RAD	Remarks
Qualified Signature	PIN for *PACE-PIN* and PIN_{QES} for *VERIFY PIN*	After each qualified signature creation, the authentication state of PIN_{QES} is reset to not verified'.
Advanced Signature	PIN for *PACE-PIN*	-

6.4.2.2 Configurations

To meet customer requirements, the product is provided in 2 possible configurations:

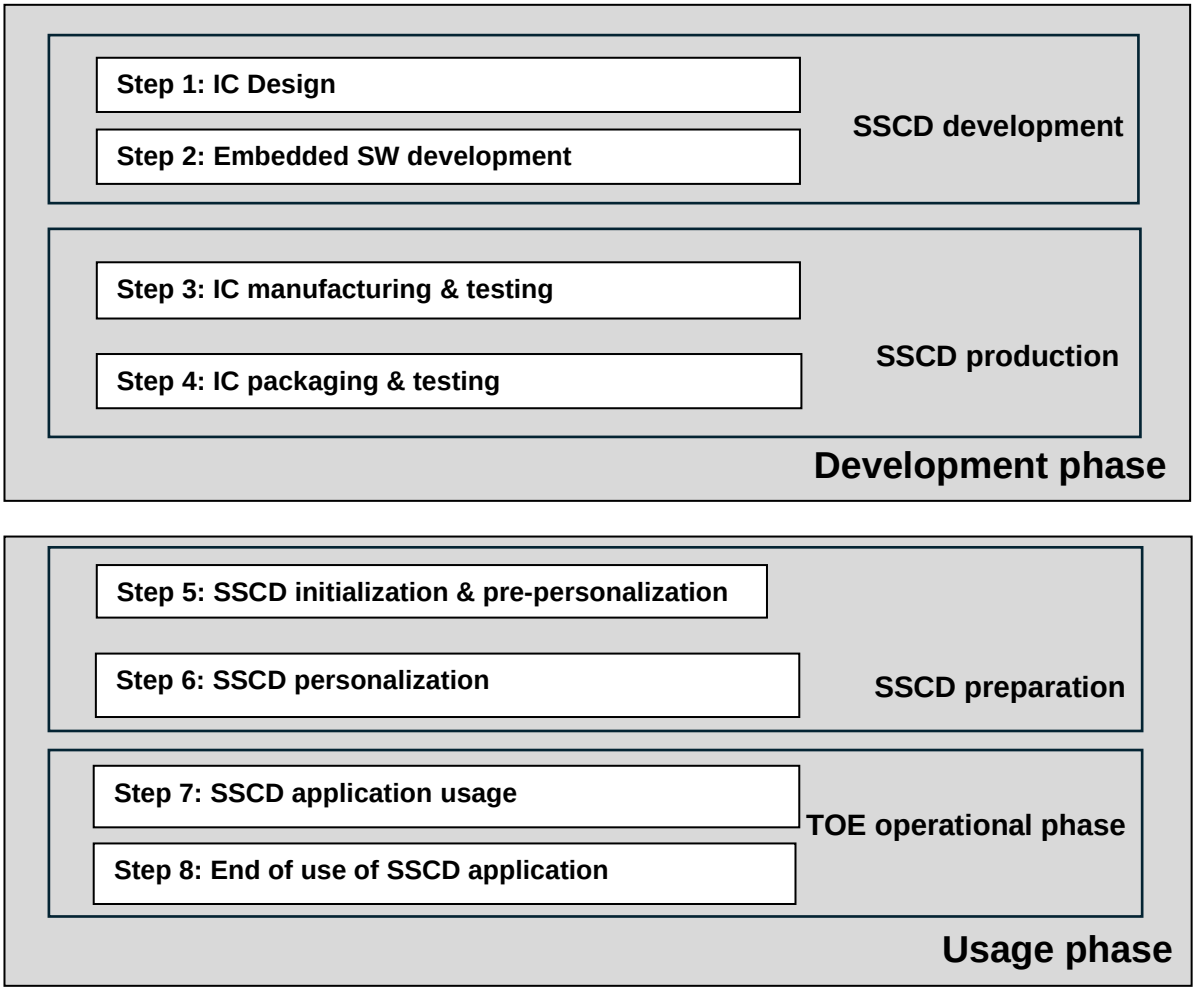
- In the first configuration the access control mechanism is based on **PACE+CA** only: it guarantees the user authentication and chip authentication.
- The second configuration uses the **Terminal Authentication Version 1** for the communication between the TOE and the signature creation application (SCA) or the certificate generation application (CGA), respectively. In this configuration the TOE restricts access to only authorized terminals.

The selection of the layout and all configuration operations are performed before TOE delivery to the signatory.

6.4.3 TOE life cycle

The TOE lifecycle is shown in the following figure. It is made of stages for development, production, preparation and operational use. The development and production of the TOE together constitute the development phase of the TOE. The preparation and operational use of the TOE together constitute the usage phase of the TOE.

Figure 3: TOE life cycle



In SSCD development phase the application binaries are always verified with the off-card verifier during their building and saved on a repository where they cannot be altered. Later the binaries are loaded on the TOE that verifies their integrity.

After the SSCD development, the chip manufacturer (STMicroelectronics Rousset), during the Step 3 IC manufacturing & testing, makes the IC, loads the OS and the SSCD application code in flash memory, and tests the IC. Then the IC packaging & testing can be performed by STMicroelectronics or other embedders. So, the TOE delivery occurs at the end of the Step 3 “IC manufacturing & testing”. After execution of the step 4 “IC packaging & testing and so completion of the Development phase, the TOE is delivered to the SSCD provisioning service provider for the SSCD preparation.

6.4.3.1 SSCD preparation by SSCD provisioning service provider

The SSCD provisioning service provider performs the steps 5 and 6.

In the step 5 **"SSCD initialization & pre-personalization"** the TOE Administrator, according to the Preparative User Guidance of the TOE [AGD_PRE], is responsible for:

- loading of third-parties' packages, if any (post-issuing)
- updating of the EPKIApplet packages, if necessary (application upgrade)
- creating of the EPKIApplet instance (application installation)

In the step 6 **"SSCD personalization"** the TOE Administrator, according to the Preparative User Guidance of the TOE [AGD_PRE], is responsible for:

- setting the TSF data Access conditions and trusted channel (secure messaging) conditions
- creating the SCD/SVD pair and setting relevant Access Conditions and Secure Messaging conditions to grant that the SCD will be used by the legitimate Signatory only
- configuring the SCD in key import mode, by setting the Access Conditions of the SCD/SVD pair so that the SCD can be used only for importing the SCD/SVD pair (and not for generating it)
- creating Signatory Reference Authentication Data to be used for Signatory identification purpose (RADS) and setting its Access Conditions and Secure Messaging conditions
- importing the SCD/SVD pair
- importing the certificate

6.4.3.2 SSCD preparation by card manufacturer

The step 4, 5 and 6 can be performed by the card manufacturer (STMicroelectronics Marcianise), on behalf of the SSCD provisioning service provider, and so in this case the TOE delivery occurs after the **step 6** "SSCD personalization".

6.4.3.3 TOE operational phase

After completion of step 6 "SSCD personalization", the TOE is delivered to the Signatory and starts the TOE operational phase, that is within the scope of the evaluation and represents installation, generation, start-up and operation in the CC terminology. During the TOE operational phase, the TOE implements a mechanism to handle its life-cycle state.

In the step 7 "**SSCD application usage**" the TOE can be used either by the Signatory or Administrator.

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

If a chip integrity violation or unrecoverable failure occurs the TOE enters the step 8 **"End of use of SSCD application"** and, after having performed all actions needed for its secure disposal, the SSCD application is no more available.

6.4.3.4 TOE Environments

The TOE described in this ST is developed in the environments listed in the following table.

Step	Description	Responsible	Environment
1	IC Design	Chip Manufacturer	STMicroelectronics Rousset, France STMicroelectronics Singapore STMicroelectronics Zaventem
2	Embedded SW Development	Chip Manufacturer	STMicroelectronics Marcianise (CE) Italy
3	IC manufacturing & testing	Chip Manufacturer	STMicroelectronics Rousset, France
4	IC Packaging & testing	Card Manufacturer	Card manufacturer site covered by STeID JC Open OS certificate
5	SSCD initialization & pre-personalization	TOE Administrator	STMicroelectronics Marcianise (CE) Italy or other qualified SSCD Provisioning Service Center or Certification authority
6	SSCD personalization	TOE Administrator	STMicroelectronics Marcianise (CE) Italy or other qualified SSCD Provisioning Service Center or Certification authority

6.4.4 Non-TOE hardware/software/firmware required by the TOE

The antenna, the EMRTDApplet Java Card applet, and the MoCApplet Java Card applet are not in the scope of the TOE.

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete travel document, nevertheless these parts are not inevitable for the secure operation of the TOE.

7 Conformance claim

7.1 CC conformance claim

This Security Target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model Version 3.1 Revision 5 [CC_P1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components Version 3.1 Revision 5 [CC_P2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements Version 3.1 Revision 5 [CC_P3]

The ST claims conformance to CC Part 2 extended and CC Part 3 conformant.

For the evaluation the following methodology is used:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology Version 3.1 Revision 5 [CEM]

7.2 PP Claim

This Security Target claims strict conformance to:

- Protection profiles for secure signature creation device — Part 3: Device with key import – [CC_PP_0075]
- Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application [CC_PP_SCA_0076]

7.3 Package Claim

This Security Target claims conformance to the assurance package EAL5+, that is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 as defined in [CC_P3].

7.4 Conformance Claim Rationale

All the contents of the claimed PPs listed in 7.2 have been added to this Security Target. Furthermore, this Security Target adds:

- the Security Function Requirement “**FIA_AFL.1/Suspend_PIN**” taken from EAC v2 PP [CC_PP-0086]
- the Security Function Requirement “**FIA_AFL.1/Block_PIN**” taken from EAC v2 PP [CC_PP-0086]
- the Assets and Security Function Requirements for BAC taken from BAC PP [CC_PP-0055]
- the Assets and Security Function Requirements for PACE taken from PACE PP [CC_PP-0068]
- the Assets and Security Function Requirements for EAC taken from EAC PP [CC_PP-0056]

SFRs are added to address the *Password Authenticated Connection Establishment* (PACE) and *Extended Access Control Version 1* (EACv1) (i.e. Chip Authentication Version 1 (CAv1) and *Terminal Authentication Version 1* (TAv1)) functionalities to provide a secure authentication protocol and a secure channel for the communication with authorized terminals in phase usage/operational.

Furthermore, SFRs taken from [CC_PP-0086] concerning the RAD has been included.

The operations done for the SFRs taken from the claimed PPs are clearly indicated.

The **Security Assurance Requirements** statement for the TOE in this Security Target includes all the requirements for the TOE from the claimed PPs.

8 Security problem definition

The following paragraphs describe the security aspects and the environment in which the TOE is intended to be used.

8.1 Assets and objects

8.1.1 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.

8.1.2 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.

8.1.3 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.

8.1.4 Access to the TOE functions and data

Signature-creation function of the TOE to create digital signature for the DTBS/R with the SCD.

8.1.5 User data stored on the TOE

Assets taken from PACE PP [CC_PP-0068] and EAC PP [CC_PP-0056].

8.1.6 Accessibility to the TOE functions and data only for authorised subjects

Assets for PACE and EAC taken from PACE PP [CC_PP-0068] and EAC PP [CC_PP-0056], respectively.

8.1.7 TOE internal secret cryptographic keys

Assets for PACE and EAC taken from PACE PP [CC_PP-0068] and EAC PP [CC_PP-0056], respectively.

8.2 User and subjects acting for users

8.2.1 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

8.2.2 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.

8.2.3 Signatory

User who holds 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.

8.2.4 Certification Service Provider (CSP)

Subject referring the EACv1 functionality corresponding to “Country Verifying Certification Authority” in EAC PP [CC_PP-0056].

8.2.5 Legitimate Terminal (CGA and SCA)

Subject referring the EACv1 functionality corresponding to “Domestic Extended Inspection System” in EAC PP [CC_PP-0056].

8.3 Threat agents

8.3.1 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.

8.4 Threats to Security

8.4.1 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

8.4.2 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.

8.4.3 T.Hack_Phys (Physical attacks through the TOE interfaces)

An attacker interacts physically with the TOE using the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

8.4.4 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.

8.4.5 T.SigF_Misuse (Misuse of the signature creation function of the TOE)

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

8.4.6 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.

8.4.7 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.

8.5 Organizational Security Policies

8.5.1 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] and [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.

8.5.2 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] and [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] and [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 maintains under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

8.5.3 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] and [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.

8.5.4 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.

8.6 Assumptions

8.6.1 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.

8.6.2 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.

8.6.3 A.CSP (Secure SCD/SVD management by CSP)

The CSP uses only a trustworthy SCD/SVD generation device and ensures that this device can be used by authorized user only. The CSP ensures that the SCD generated practically occurs only once, that generated SCD and SVD actually correspond to each other and that SCD cannot be derived from the SVD. The CSP ensures the confidentiality of the SCD during generation and export to the TOE, does not use the SCD for creation of any signature and irreversibly deletes the SCD in the operational environment after export to the TOE.

9 Security objectives

All the security objects are taken from claimed PP (see section 7.2). When not explicitly specified, the security objects are taken from PP SCD [CC_PP_0075], otherwise the PP, from which the security object is taken, is explicitly specified.

9.1 Security objectives for the TOE

9.1.1 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.

9.1.2 OT.SCD_Auth_Imp (Authorized SCD import)

The TOE shall provide security features to ensure that authorized users only may invoke the import of the SCD.

9.1.3 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 import, signature creation operation, storage and secure destruction

9.1.4 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

9.1.5 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

9.1.6 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

9.1.7 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

9.1.8 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

9.1.9 OT.Tamper_Resistance (Tamper resistance)

The TOE shall prevent or resist physical tampering with specified system devices and components

9.1.10 OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import)

Security Object taken from PP SCD with key import and SCA [CC_PP_SCA_0076].

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 SCD [CC_PP_0075].

While OE.HID_VAD in the PP SCD [CC_PP_0075] requires only the operational environment to protect VAD, the PP SCD with key import and SCA [CC_PP_SCA_0076] 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 SCD with key import and SCA [CC_PP_SCA_0076] 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.

9.1.11 OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS import)

Security Object taken from PP SCD with key import and SCA [CC_PP_SCA_0076].

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 SCD [CC_PP_0075]. While OE.DTBS_Protect in the PP SCD [CC_PP_0075] requires only the operational environment to protect DTBS, the PP SCD with key import and SCA [CC_PP_SCA_0076] 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 SCD with key import and SCA [CC_PP_SCA_0076] 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.

9.2 Security objectives for the operational environment

Following table summarizes the security objectives for the operational environment as defined in [CC_PP_0075] and [CC_PP_SCA_0076].

As stated in [CC_PP_SCA_0076], 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.

The Security objectives for the operational environment **OE.HID_VAD** from PP SCD [CC_PP_0075] is not included because the PP SCD with key import and SCA [CC_PP_SCA_0076] states that it is covered by **OE.HID_TC_VAD_Exp** and **OT.TOE_TC_VAD_Imp**.

The Security objectives for the operational environment **OE.DTBS_Protect** from PP SCD [CC_PP_0075] is not included because the PP SCD with key import and SCA [CC_PP_SCA_0076] states that it is covered by **OE.SCA_TC_DTBS_Exp** and **OT.TOE_TC_DTBS_Imp**.

9.2.1 OE.SCD/SVD_Auth_Gen (Authorized SCD/SVD generation)

The CSP shall provide security features to ensure that authorised users only may invoke the generation of the SCD and SVD.

9.2.2 OE.SCD_Secrecy (SCD Secrecy)

The CSP shall protect the confidentiality of the SCD during generation and export to the TOE. The CSP shall not use the SCD for creation of any signature and shall irreversibly delete the SCD in the operational environment after export to the TOE.

9.2.3 OE.SCD_Unique (Uniqueness of the signature creation data)

The CSP shall ensure the cryptographic quality of the SCD/SVD pair, which is generated in the environment, for the qualified or advanced electronic signature. The SCD used for signature creation shall practically occur only once, i.e. the probability of equal SCDs shall be negligible, and the SCD shall not be reconstructable from the SVD.

9.2.4 OE.SCD_SVD_Corresp (Correspondence between SVD and SCD)

The CSP shall ensure the correspondence between the SVD and the SCD generated by the CSP. This includes the correspondence between the SVD send to the CGA and the SCD exported to the TOE of the signatory identified in the SVD certificate.

9.2.5 OE.SVD_Auth (Authenticity of the SVD)

The operational environment shall ensure the authenticity 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.

9.2.6 OE.CGA_QCert (Generation of qualified certificates)

The CGA shall generate qualified certificate that include (amongst others)

- the name of the signatory controlling the TOE,
- the SVD matching the SCD stored in the TOE and being under sole control of the signatory
- 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

9.2.7 OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD-provisioning service)

The SSCD-provisioning service shall initialise and personalise for the signatory an authentic copy of the TOE and deliver this copy as SSCD to the signatory.

9.2.8 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.

9.2.9 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.

9.2.10 OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD Export)

Security Object taken from PP SCD with key import and SCA [CC_PP_SCA_0076] .

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.

9.2.11 OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS export)

Security Object taken from PP SCD with key import and SCA [CC_PP_SCA_0076].

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.

9.3 Security Objectives Rationale

9.3.1 Security Objectives backtracking

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.

Table 7: Mapping of security problem definition to security objectives

Security Objectives / Threats, Assumptions, Policies	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.DTBS_Intend	OE.Signatory	OE.HID_TC_VAD_Exp	OE.SCA_TC_DTBS_Exp
T.SCD_Divulg		x	x									x	x									
T.SCD_Derive				x										x								
T.Hack_Phys			x				x	x	x													
T.SVD_Forgery															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				
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
A.CGA																x	x					
A.SCA																			x			
A.CSP												x	x	x	x							

9.3.2 Security Objectives Sufficiency

9.3.2.1 Countering of threats by security objectives

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 [DECESE_650/2016]).

This threat is countered by:

- OE.SCD_Secrecy, which assures the secrecy of the SCD in the CSP environment, and
- OT.SCD_Secrecy, which assures the secrecy of the SCD during use by the TOE for signature creation.

Furthermore, generation and/or import of SCD known by an attacker is countered by:

- OE.SCD/SVD_Auth_Gen, which ensures that only authorized SCD generation in the environment is possible, and
- OT.SCD_Auth_Imp, which ensures that only authorised SCD import is possible.

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.

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

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.

T.SVD_Forgery (*Forgery of the signature verification data*) deals with the forgery of the SVD given to the CGA for certificate generation. T.SVD_Forgery is addressed by:

- OE.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD, and
- OE.SVD_Auth that ensures the authenticity of the SVD given to the CGA of the CSP.

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.
- OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE.
- 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.

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.

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.

T.Sig_Forgery (*Forgery of the electronic signature***)** deals with non-detectable forgery of the electronic signature.

- OT.Sig_Secure,
- OE.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.
- OE.SCD_Unique 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.

9.3.3 Enforcement of OSPs by security objectives

P.CSP_QCert (*CSP generates qualified certificates*) establishes the CSP, generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD, under sole control of this signatory. It is addressed by

- OT.Lifecycle_Security ensures that the TOE detects flaws during the initialisation, personalisation and operational usage.
- OE.SCD/SVD_Auth_Gen ensures that SCD/SVD generation can be invoked by authorized users only.
- OT.SCD_Auth_Imp ensures that authorised users only may invoke the import of SCD.
- OE.SCD_SVD_Corresp ensures that the CSP checks the correspondence between the SVD and the SCD during their generation.
- OE.CGA_QCert ensures that the CGA certifies the SVD matching the SCD implemented in the TOE under sole control of the signatory.

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.

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

- OE.SCD_Unique requiring that the SCD used for signature creation can practically occurs only once.

Then,

- OE.SCD_Unique
- OT.SCD_Secrecy
- OE.SCD_Secrecy and

address the secrecy of the SCD (cf. [DIRECTIVE_93] repealed by [REGEU_910/2014] and [DECESE_650/2016]). Specific objectives to ensure secrecy of the SCD against specific attacks are addressed by:

- OT.EMSEC_Design and
- OT.Tamper_Resistance

Then,

- 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.

Then,

- OT.Sigy_SigF
- OE.SCD_Secrecy

meets the requirement in [DIRECTIVE_93] (repealed by [REGEU_910/2014] and [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.

Then,

- 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, which detects flaws during the initialization, personalization and operational usage
- OE.SCD/SVD_Auth_Gen, which limit invocation of the generation of the SCD and the SVD to authorized users only.
- OT.SCD_Auth_Imp, which limits SCD import to authorized users only.
- OE.SCD_Secrecy, which ensures the confidentiality of the SCD during generation andexport to the TOE, and deletes the SCD a_er export to the TOE. The CSP does not usethe SCD for signature creation.OT.Sigy_SigF.
- OT.Sigy_SigF, which requires the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.
- OE.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, initialized and personalized as SSCD from the SSCD-provisioning service.

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.SSCD_Prov_Service ensures that the signatory uses an authentic copy of the TOE, initialised and personalised for the signatory.
- OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy and OE.SCD_Unique ensure the security of the SCD in the CSP environment.
- OE.SCD_Secrecy ensures the confidentiality of the SCD during generation, during and after export to the TOE. The CSP does not use the SCD for creation of any signature and deletes the SCD irreversibly after export to the TOE.

- OE.SCD_Unique (Uniqueness of the signature creation data) provides that the signatory's SCD can practically occur just once.
- OE.SCD_SVD_Corresp (Correspondence between SVD and SCD) ensures that the SVD in the certificate of the signatory corresponds to the SCD that is implemented in the copy of the TOE of the signatory. ensures that the signatory uses an authentic copy of the 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 the authenticity of the SVD included in the certificate and to ensure correspondence of the SVD to the SCD stored in the SSCD.
- 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)
- 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 ensures that the signatory keeps their VAD confidential.
- OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and
- OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD) protect the confidentiality of VAD during transmission between the HI device and TOE.
- OE.DTBS_Intend, OE.SCA_TC_DTBS_Exp, OT.TOE_TC_DTBS_Imp and
- OT.DTBS_Integrity_TOE ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS.
- OT.Sig_Secure (Cryptographic security of the electronic signature) ensure that only this SCD may create 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.

9.3.4 Upkeep of assumptions by security objectives

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.

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.

A.CSP *(Secure SCD/SVD management by CSP)* establishes several security aspects concerning handling of SCD and SVD by the CSP.

- OE.SCD/SVD_Auth_Gen (Authorized SCD/SVD Generation), which ensures the SCD/SVD generation device can only be used by authorized users.
- OE.SCD_Unique (Uniqueness of the signature creation data), which ensures the generated SCD is unique and cannot be derived by the SVD.
- OE.SCD_SVD_Corresp (Correspondence between SVD and SCD), which ensures the SCD and SVD correspond to each other.
- OE.SCD_Secrecy (SCD Secrecy), which ensures the SCD are kept confidential.

10 Extended components definition

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 define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

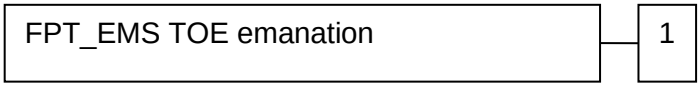
10.1 Family FPT_EMS TOE Emanation

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

FPT_EMS TOE Emanation

Family behavior This family defines requirements to mitigate intelligible emanations.

Component leveling



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.

10.1.1 FPT_EMS.1 (Intelligible emissions)

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*].

10.1.2 FPT_EMS.2 (Interface Emanation)

Hierarchical to: No other components.

Dependencies: No dependencies.

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*].

10.2 Family FCS_RND Generation of random numbers

The component FCS_RND is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

The family FCS_RND (Generation of random numbers) is specified as follows.

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

Component leveling

FCS_RND Generation of random numbers	1

FCS_RND.1 Generation of random numbers requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

10.2.1 FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment*: a defined quality metric*].

11 Security requirements

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

11.1 Overview

This part of the PP defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in section 8.1 of Part 1 of the Common Criteria [CC_P1]. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in bold text and removed are crossed out.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections made by the ST author appear slanted and underlined.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments made by the ST author appear slanted and underlined.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier.

This part defines the detailed security requirements that are satisfied by the TOE. These requirements comprise functional components from CC Part 2 [CC_P1] Extended components as defined in Chapter 11, and the assurance components as defined for the Evaluation Assurance Level EAL5+ from CC Part 3 [CC_P1] augmented with ALC_DVS.2 and AVA_VAN.5

The definition of the subjects “Manufacturer”, “Personalisation Agent”, “Extended Inspection System”, “Country Verifying Certification Authority”, “Document Verifier” and “Terminal” used in the following chapter is given in section 11. Note, that all these subjects are acting for homonymous external entities. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [CC_P2]. The operation “load” is synonymous to “import” used in [CC_P2].

11.2 Security Functional Requirement

The TOE consists of a combination of hardware and software components implementing the specific TOE Security Functions (TSF) for the functional requirements defined in the PP SCD [CC_PP_0075] and PP SCD with key import and SCA [CC_PP_SCA_0076].

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.

This paragraph fully restates TOE security functional requirements (the PP SCD [CC_PP_0075] and PP SCD with key import and SCA [CC_PP_SCA_0076]).

11.3 Class FCS Cryptographic support (FCS)

The TOE shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below. The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

11.3.1 FCS_CKM.1/BAC Cryptographic key generation – Personalization Agent

Defined in: BAC PP [CC_PP-0055]

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/BAC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[1] and specified cryptographic key sizes 128 bit[2] that meet the following: [ICAO_9303], normative appendix 5[3].

Application note: The TOE is equipped with the Personalization Agent Access Key generated and downloaded by the Manufacturer. The Basic Access Control Authentication Protocol described in [ICAO_9303], normative appendix A5.2, produces agreed parameters to generate the AES key (instead of Triple-DES key) and the C-MAC (instead of Retail-MAC) message authentication keys for secure messaging by the algorithm in [ICAO_9303], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

11.3.2 FCS_CKM.1/CA Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys

Defined in: EAC PP [CC_PP-0056]

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/CA-DH-3DES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *DH Key Agreement Algorithm*[4] and specified cryptographic key sizes *112 bits*[5] that meet the following: *based on the Diffie-Hellman key derivation protocol compliant to [TR-03110-1] and [PKCS_#3]*[6].

[1] [assignment: *cryptographic key generation algorithm*]
[2] [assignment: *cryptographic key sizes*]
[3] [assignment: *list of standards*]
[4] [assignment*: cryptographic key generation algorithm*]
[5] [assignment*: cryptographic key sizes*]
[6] [assignment: *list of standards]*

FCS_CKM.1.1/CA-DH-AESThe TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *DH Key Agreement Algorithm*[7] and specified cryptographic key sizes *128, 192 and 256 bits*[8] that meet the following: *based on the Diffie-Hellman key derivation protocol compliant to [TR-03110-1] and [PKCS_#3]*[9].

FCS_CKM.1.1/CA- ECDH-3DES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH Key Agreement Algorithm*[10] and specified cryptographic key sizes *112 bits*[11] that meet the following: *based on an ECDH protocol compliant to [TR-03111]*[12].

FCS_CKM.1.1/CA- ECDH-AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH Key Agreement Algorithm*[13] and specified cryptographic key sizes *128, 192 and 256 bits*[14] that meet the following: *based on an ECDH protocol compliant to [TR-03111]*[15].

Application note: For [PKCS_#3] the RSA key length supported are 1024 and 2048 bits and for [TR-03111] the EC key length supported are 192, 224, 256, 320, 384, 512 and 521 bits.

Application note: The TOE implements the hash functions for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms. The Chip Authentication Protocol v.1 may use SHA-1. The TOE implements additional hash functions SHA-224, SHA-256, SHA 384 and SHA 512.

Application note: The TOE destroys any session keys in accordance with FCS_CKM.4

11.3.3 FCS_CKM.1/DH_PACE Cryptographic key generation – Diffie-Hellman for PACE session keys

Defined in: PACE PP [CC_PP-0068]

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] fulfilled by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case. FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_CKM.1.1/DH-PACE-3DES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Diffie-Hellman-Protocol compliant to [PKCS_#3]*[16] and specified cryptographic key sizes *112 bits*[17] that meet the following: [ICAO_TR][18].

[7] [assignment: *cryptographic key generation algorithm*]
[8] [assignment: *cryptographic key sizes*]
[9] [assignment: *list of standards]*
[10] [assignment: *cryptographic key generation algorithm*]
[11] [assignment: *cryptographic key sizes*]
[12] [assignment: *list of standards]*
[13] [assignment: *cryptographic key generation algorithm*]
[14] [assignment: *cryptographic key sizes*]
[15] [assignment: *list of standards]*
[16] [assignment: *cryptographic key generation algorithm*]
[17] [assignment: *cryptographic key sizes*]
[18] [assignment: list of standards]

FCS_CKM.1.1/DH-PACE-AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Diffie-Hellman-Protocol compliant to [PKCS_#3]*[19] and specified cryptographic key sizes *128, 192 and 256 bits* **[20]** that meet the following: [ICAO_TR][21].

FCS_CKM.1.1/ ECDH-PACE-3DES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to [TR-03111]*[22] and specified cryptographic key sizes *112 bits*[23] that meet the following: [ICAO_TR][24].

FCS_CKM.1.1/ ECDH-PACE-AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to [TR-03111]*[25] and specified cryptographic key sizes *128, 192 and 256 bits* **[26]** that meet the following: [ICAO_TR][27].

Application note: For [PKCS_#3] the DH key length supported are 1024 and 2048 bits and for [TR-03111] the EC key length supported are 192, 224, 256, 320, 384, 512 and 521 bits.

Application note: The TOE generates a shared secret value K with the terminal during the PACE protocol. This protocol may be based on the Diffie-Hellman-Protocol compliant to [PKCS_#3] or on the ECDH compliant to [TR-03111]. The shared secret value K is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{ENC}) according to [ICAO_TR] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Application note: The TOE supports the following standardized elliptic curve and DSA key:

- 1024-bit MODP Group with 160-bit Prime Order Subgroup
- 2048-bit MODP Group with 224-bit Prime Order Subgroup
- 2048-bit MODP Group with 256-bit Prime Order Subgroup
- NIST P-192 (secp192r1), NIST P-224 (secp224r1), NIST P-256 (secp256r1), NIST P-384 (secp384r1), NIST P-521 (secp521r1)
- BrainpoolP192r1, BrainpoolP224r1, BrainpoolP256r1, BrainpoolP320r1, BrainpoolP384r1, BrainpoolP512r1

11.3.4 FCS_CKM.4 Cryptographic key destruction

Defined in: PP SCD [CC_PP_0075]

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]: fulfilled by FCS_CKM.1

[19] [assignment: *cryptographic key generation algorithm*]
[20] [assignment*: cryptographic key sizes*]
[21] [assignment: list of standards]
[22] [assignment: *cryptographic key generation algorithm*]
[23] [assignment*: cryptographic key sizes*]
[24] [assignment: list of standards]
[25] [assignment: *cryptographic key generation algorithm*]
[26] [assignment*: cryptographic key sizes*]
[27] [assignment: list of standards]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting the cryptographic key with zeros or random data*[28] that meets the following: *none*[29].

11.3.5 FCS_COP.1 Cryptographic operation

The TOE shall meet the following requirements for the cryptographic operations. The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

11.3.5.1 FCS_COP.1/SCD/RSA Cryptographic operation – SCD (RSA)

Defined in: PP SCD [CC_PP_0075]

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/SCD/RSA The TSF shall perform digital signature creation[30] in accordance with a specified cryptographic algorithm raw RSA, RSA with padding PKCS1-v1_5 and padding PSS[31] and cryptographic key sizes 2048, 3072, and 4096[32] bits that meet the following: Public-Key Cryptography Standards (PKCS#1): RSA Cryptography Specifications Version 2.2 - [PKCS1_v2_2] and [RFC8017].[33]

11.3.5.2 FCS_COP.1/SCD/ECDSA Cryptographic operation – SCD (ECDSA)

Defined in: PP SCD [CC_PP_0075]

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/SCD/ECDSA The TSF shall perform digital signature creation[34] in accordance with a specified cryptographic algorithm ECDSA[35] and cryptographic key sizes 192, 224 256, 384, 512, and 521 bits[36] that meet the following: [FIPS_PUB_186-4] and [ANSI X9.62][37].

11.3.5.3 FCS_COP.1/PACE_ENC Cryptographic operation – Encryption/Decryption AES/3DES

Defined in: PACE PP [CC_PP-0068]

Hierarchical to: No other components

[28] [assignment: *cryptographic key destruction method*]
[29] [assignment: *list of standards*]
[30] [assignment: *list of cryptographic operations*]
[31] [assignment*: cryptographic algorithm*]
[32] [assignment*: cryptographic key sizes*]
[33] [assignment: *list of standards]*
[34] [assignment: *list of cryptographic operations*]
[35] [assignment*: cryptographic algorithm*]
[36] [assignment*: cryptographic key sizes*]
[37] [assignment: *list of standards*]

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/PACE_ENC The TSF shall perform secure messaging – encryption and decryption[38] in accordance with a specified cryptographic algorithm *AES and 3DES* in CBC mode[39] and cryptographic key sizes *128, 192, 256 bit for AES and 112 for 3DES*[40] that meet the following: compliant to [ICAO_TR][41].

11.3.5.4 FCS_COP.1/PACE_MAC Cryptographic operation – MAC

Hierarchical to: PACE PP [CC_PP-0068]

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/PACE_MAC The TSF shall perform secure messaging – message authentication code[42] in accordance with a specified cryptographic algorithm *CMAC and Retail-MAC*[43] and cryptographic key sizes *128, 192, 256 bit for CMAC and 112 bit for Retail-MAC*[44] that meet the following: compliant to [ICAO_TR][45].

11.3.5.5 FCS_COP.1/CA_ENC Cryptographic operation – Encryption/Decryption AES/3DES

Defined in: EAC PP [CC_PP-0056]

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/CA_ENC The TSF shall perform secure messaging – encryption and decryption[46] in accordance with a specified cryptographic algorithm *AES and 3DES*[47] and cryptographic key sizes *128, 192, 256 bit for AES and 112 bit for 3DES*[48] that meet the following: *compliant to [TR-03110-1]*[49].

Application note: The TOE implements the cryptographic primitives (e.g. 3DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol v.1.

11.3.5.6 FCS_COP.1/CA_MAC Cryptographic operation – MAC

Defined in: EAC PP [CC_PP-0056]

[38] [assignment: *list of cryptographic operations*]
[39] [assignment: *cryptographic algorithm*]
[40] [assignment: *cryptographic key sizes*]
[41] [assignment: *list of standards*]
[42] [assignment: *list of cryptographic operations*]
[43] [assignment: *cryptographic algorithm*]
[44] [assignment: *cryptographic key sizes*]
[45] [assignment: *list of standards*]
[46] [assignment: *list of cryptographic operations*]
[47] [assignment: *cryptographic algorithm*]
[48] [assignment: *cryptographic key sizes*]
[49] [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/CA_MAC The TSF shall perform secure messaging – message authentication code[50] in accordance with a specified cryptographic algorithm *CMAC and Retail-MAC*[51] and cryptographic key sizes *128, 192, 256 bit for CMAC and 112 bit for Retail-MAC*[52] that meet the following: *compliant to [TR-03110-1]*[53].

Application note: The TOE implements the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol v.1.

11.3.5.7 FCS_COP.1/SIG_VER Cryptographic operation – Signature Verification

Defined in: EAC PP [CC_PP-0056]

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/SIG_VER The TSF shall perform digital signature verification[54] in accordance with a specified cryptographic algorithm *ECDSA, RSA PSS and RSA PKCS#1*[55] and cryptographic key sizes *192, 224, 256, 320, 384, 512, and 521 bits for EC key and 1024 and 2048 bits for RSA key* that meet the following *[TR-03111], [RFC3447] and* [PKCS1_v1_5][56].

Application note: This SFR has been adapted from [CC_PP-0056]. It applies only to the configurations requiring Terminal Authentication for the communication between the TOE and the SCA and the CGA.

11.3.5.8 FCS_COP.1/SHA Cryptographic operation – Hashes

Defined in: EAC v2 PP [CC_PP-0086]

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

[50] [assignment: *list of cryptographic operations*]
[51] [assignment: *cryptographic algorithm*]
[52] [assignment: *cryptographic key sizes*]
[53] [assignment: *list of standards*]
[54] [assignment: *list of cryptographic operations*]
[55] [assignment: *cryptographic algorithm*]
[56] [assignment: *list of standards*]

FCS_COP.1.1/SHA The TSF shall perform hashing[57] in accordance with a specified cryptographic algorithms *SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512*[58] and cryptographic key sizes *none*[59] that meet the following: [FIPS_PUB180_4][60].

Application note: The hashing function are used to calculate the DTBS. The requirements for the hashing functions used for PACE and Chip Authentication are included in SFRs FCS_CKM.1/DH_PACE, FCS_CKM.1/CA/DH and FCS_CKM.1/CA/ECDH implicitly.

11.3.6 FCS_RND.1 Random Number Generation

The TOE shall meet the following requirements for the generation of random numbers.

11.3.6.1 FCS_RND.1 Quality metric for random numbers

Defined in: PACE PP [CC_PP-0068]

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet *DRG.3 capabilities defined in [AIS20/31] standard* [61].

Application note: The TOE implements a deterministic random number generator. When initialized with a random seed using a PTRNG of class PTG.2 as random source, the internal state of the RNG has at least 100 bits of min-entropy. The TOE's RNG is initialized with a random seed at each TOE startup/reset/power-up. It generates output, for which 2^{34} strings of bit length 128 are mutually different with probability greater than $1-2^{-16}$. The TOE's RNG provides forward secrecy. It provides backward secrecy even if the current internal state is known. Statistical test suites cannot practically distinguish the TOE's RNG sequences from output sequences of an ideal RNG. The TOE's RNG pass test procedure A and the NIST statistical test suite [SP-800-22].

Application note: TOE to generate random numbers (random nonce) used for the authentication protocol (PACE).

11.4 Class FDP 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

11.4.1 FDP_ACC.1/TRM Subset access control – Terminal Access

Defined in: PACE PP [CC_PP-0068]

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

[57] [assignment: *list of cryptographic operations*]
[58] [assignment: *cryptographic algorithm*]
[59] [assignment: *cryptographic key sizes*]
[60] [assignment: *list of standards*]
[61] [assignment: *a defined quality metric*]

FDP_ACC.1.1/TRM The TSF shall enforce the Access Control SFP on terminals gaining access to the User Data of the electronic document.

Application note: This SFR has been adapted from [CC_PP-0068]. The term *logical travel document* has been changed to *electronic document*.

11.4.2 FDP_ACF.1/TRM Security attribute based access control – Terminal Access

Defined in: PACE PP [CC_PP-0068]

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/TRM The TSF shall enforce the Access Control SFP to objects based on the following:

1) Subjects:
   a) Legitimate Terminal
2) Objects:
   a) user data stored on the TOE,
   b) all TOE intrinsic secret cryptographic keys stored in the electronic document.
3) Security attributes:
   a) authorization of the Legitimate Terminal

FDP_ACF.1.2/TRM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: A Legitimate Terminal is allowed to read data objects from FDP_ACF.1.1/TRM according to [ICAO_TR] after a successful PACE authentication as required by FIA_UAU.1[62].

FDP_ACF.1.3/TRM The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[63].

FDP_ACF.1.4/TRM The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the electronic document.
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the electronic document.

Application note: This SFR has been adapted from [CC_PP-0068]. The term *logical travel document* has been changed to *electronic document*.

11.4.3 FDP_ACC.1/SCD_Import – Subset based access control

Defined in: PP SCD [CC_PP_0075]

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

[62] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[63] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

FDP_ACC.1.1/SCD_Import The TSF shall enforce the SCD Import SFP[64] on

1. subjects: S.User,
2. objects: SCD
3. operations: import of SCD[65].

11.4.4 FDP_ACF.1/SCD_Import – Security attributes based access control

Defined in: PP SCD [CC_PP_0075]

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/SCD_Import The TSF shall enforce the SCD Import SFP[66] to objects based on the following: the S.User is associated with the security attribute "SCD/SVD Management"[67].

FDP_ACF.1.2/SCD_Import 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 import SCD.

FDP_ACF.1.3/ SCD_Import The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[68].

FDP_ACF.1.4/SCD_Import 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 import SCD.

11.4.5 FDP_ACC.1/Signature_Creation – Subset access control

Defined in: PP SCD [CC_PP_0075]

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[69] on

1. subjects: S.User,
2. objects: DTBS/R, SCD,
3. operations: signature creation[70].

11.4.6 FDP_ACF.1/Signature_Creation – Security attribute access control

Defined in: PP SCD [CC_PP_0075]

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

---

[64] [assignment: *access control SFP*]
[65] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[66] [assignment: *access control SFP*]
[67] 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*]
[68] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[69] [assignment: *access control SFP*]
[70] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

FDP_ACF.1.1/Signature_Creation The TSF shall enforce the Signature Creation SFP[71] 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" [72].

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" [73]

Refinement for the configurations requiring Terminal Authentication for the communication between the TOE and the SCA and the CGA: R.Sigy is allowed to create qualified electronic signatures for DTBS/R with SCD after successful Terminal Authentication and successful authentication against RAD.

FDP_ACF.1.3/Signature_Creation The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[74]

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" [75]

11.4.7 FDP_ITC.1/SCD – Import of user data without security attributes

Hierarchical to: PP SCD [CC_PP_0075]

Dependencies: FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1/SCD The TSF shall enforce the SCD_Import_SFP[76] when importing user data, controlled under the SFP, from outside of the TOE

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

FDP_ITC.1.3/SCD The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none[77]

11.4.8 FDP_UCT.1/SCD – Basic data exchange confidentiality

Hierarchical to: PP SCD [CC_PP_0075]

Hierarchical to: No other components.

[71] [assignment: *access control SFP*]
[72] [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*]
[73] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[74] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[75] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[76] [assignment: *access control SFP*]
[77] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

Dependencies: FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1/SCD The TSF shall enforce the SCD_Import_SFP[78] to receive ~~user data~~ **SCD** in a manner protected from unauthorized disclosure.

11.4.9 FDP_RIP.1 – Subset residual information protection

Defined in: PP SCD [CC_PP_0075]

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[79] the following objects: SCD[80].

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":

11.4.10 FDP_SDI.2/Persistent – Stored data integrity monitoring and action

Defined in: PP SCD [CC_PP_0075]

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[81] on all objects, based on the following attributes: integrity checked stored data[82]

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[83]

11.4.11 FDP_SDI.2/DTBS – Stored data integrity monitoring and action

Defined in: PP SCD [CC_PP_0075]

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[84] on all objects, based on the following attributes: integrity checked stored DTBS[85]

[78] [assignment: *access control SFP*]
[79] [selection: *allocation of the resource to, deallocation of the resource from*]
[80] [assignment: *list of objects*]
[81] [assignment: *integrity errors*]
[82] [assignment: *user data attributes*]
[83] [assignment: *action to be taken*]
[84] [assignment: *integrity errors*]
[85] [assignment: *user data attributes*]

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[86]

11.4.12 FDP_UIT.1/DTBS – Data exchange integrity

Defined in: PP SCD with key import and SCA [CC_PP_SCA_0076]

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[87] to receive[88] user data in a manner protected from modification and insertion[89] errors.

FDP_UIT.1.2/DTBS The TSF shall be able to determine on receipt of user data, whether modification and insertion[90] has occurred.

11.5 Class FIA Identification and Authentication (FIA)

Class defined in Common Criteria Par 2 [CC_P2].

The unambiguous identification of authorised users and the correct association of security attributes with users and subjects is critical to the enforcement of the intended security policies.

Other classes of requirements (e.g. User Data Protection, Security Audit) are dependent upon correct identification and authentication of users in order to be effective.

Application note: The following table provides an overview on the authentication mechanisms used by the TOE.

Name	SFR for the TOE
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4/PACE
Chip Authentication Protocol v.1	FIA_UAU.5/PACE, FIA_UAU.6
Terminal Authentication Protocol v.1	FIA_UAU.5/PACE
PACE protocol	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE

Note the Chip Authentication Protocol v.1 includes:

- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol v.1,
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

The Chip Authentication Protocol v.1 may be used independent of the Terminal Authentication Protocol v.1. But if the Terminal Authentication Protocol v.1 is used the terminal shall use the same public key as presented during the Chip Authentication Protocol v.1.

[86] [assignment: *action to be taken*]
[87] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[88] [selection: *transmit, receive*]
[89] [selection: *modification, deletion, insertion, replay*]
[90] [selection: *modification, deletion, insertion, replay*]

11.5.1 FIA_UID.1 Timing of Identification

Defined in: PP SCD [CC_PP_0075]

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. to establish the communication channel,
3. carrying out the PACE Protocol according to **[ICAO_TR]** ,
4. to carry out the Chip Authentication Protocol v.1 according to [TR-03110-1]
5. to carry out the Terminal Authentication Protocol v.1 according to [TR-03110-1]
6. *Personalization agent authentication by authentication key*[91].
7. *none*

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.

Application Note: This SFR has been amended with items from [CC_PP-0056]

Item (5) of FIA_UID.1.1 applies only to the configurations requiring Terminal Authentication for the communication between the TOE and the SCA and the CGA.

Application note: in the step 5 “SSCD initialization & pre-personalization” the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalisation Data in the audit records of the IC. The electronic document manufacturer may create the Personalisation Agent role for transition from step 5 to step 6 “SSCD personalization & pre-personalization“. The users in Personalisation Agent role identify themselves by means of selecting the authentication key. During personalisation in the step 6 the PACE domain parameters, the Chip Authentication data, the Reference Authentication Data, the Terminal Authentication Reference Data and the Digital signature keys are written into the TOE. The Signatory or the Administrator is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol v.1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol v.1 or (ii) if necessary and available by authentication as Personalisation Agent (using the Personalisation Agent Key).

Application note: a Personalisation Agent acts on behalf of the electronic document Issuer under his CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role ‘Personalisation Agent’, when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).

11.5.2 FIA_UAU.1 Timing of Authentication

Defined in: PP SCD [CC_PP_0075], PP SCD with key import and SCA [CC_PP_SCA_0076]

Hierarchical to: No other components.

Dependencies: FIA_UID.1.1 Timing of Identification

FIA_UAU.1.1 The TSF shall allow:

1. self-test according to FPT_TST-1

[91] [assignment: *list of TSF-mediated actions*]

2. identification of the user by means of TSF required by FIA_UID.1
3. establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD[92]
4. *none*

on behalf of the user to be performed before the user is identified.

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.

11.5.3 FIA_UAU.4/PACE Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

Defined in: [CC_PP-0056]

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1/PACE The TSF shall prevent reuse of authentication data related to:

1. PACE Protocol according to [ICAO_TR],
2. Authentication Mechanism based on *AES*[93].
3. Terminal Authentication Protocol v.1 according to [TR-03110-1]

Application note: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

This SFR has been adapted from [CC_PP-0056]. Item (3) of FIA_UAU.4.1 applies only to the configurations requiring Terminal Authentication for the communication between the TOE and the SCA and the CGA.

The TOE shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below.

11.5.4 FIA_UAU.5/PACE Multiple authentication mechanisms

Defined in: [CC_PP-0056]

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/PACE The TSF shall provide:

1. PACE Protocol according to [ICAO_TR],
2. Secure messaging in MAC-ENC mode according to [ICAO_TR] ,
3. Symmetric Authentication Mechanism based on AES[94].
4. Chip Authentication protocol v.1 according to [BSI_TR-03110-1],
5. Terminal Authentication Protocol v.1 according to [TR-03110-1] to support user authentication

FIA_UAU.5.2/PACE The TSF shall authenticate any user’s claimed identity according to the following rules:

[92] [assignment: *list of TSF-mediated actions*]
[93] [assignment: *identified authentication mechanism(s)*]
[94] [assignment: *list of multiple authentication mechanisms]*

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.
2. The TOE accepts the authentication attempt as Personalisation Agent by the *Symmetric Authentication Mechanism with Personalisation Agent Key(s)*.
3. After run of the Chip Authentication Protocol v.1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.
4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1.
5. The TOE accepts the authentication attempt by means of the Chip Authentication protocol v.1 only if Secure Messaging is established by PACE.
6. *none*[95]

Application note: This SFR has been adapted from [CC_PP-0056]. Item (5) of FIA_UAU.5.1 and item (3) of FIA_UAU.5.2 apply only to the configurations requiring Terminal Authentication for the communication between the TOE and the SCA and the CGA.

11.5.5 FIA_UAU.6 Re-authenticating of Terminal by the TOE

Defined in: [CC_PP-0056]

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE protocol or the Chip Authentication protocol version 1 shall be verified as being sent by the Legitimate Terminal.

Application note: This SFR has been adapted from [CC_PP-0068] or [CC_PP-0056] , respectively.

Application note: The PACE protocol specified in [ICAO_TR] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

11.5.6 FIA_AFL.1/RAD Authentication failure handling

Defined in: PP SCD [CC_PP_0075]

Hierarchical to: No other components.

Dependencies: FIA_UAU.1.1 Timing of authentication.

[95] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

FIA_AFL.1.1/RAD The TSF shall detect when 3[96] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[97]

FIA_AFL.1.2/RAD When the defined number of unsuccessful authentication attempts has been met[98], the TSF shall block RAD[99]

11.5.7 FIA_AFL.1/Suspend_PIN Authentication failure handling – Suspending PIN

Defined in: EAC v2 PP [CC_PP-0086]

Hierarchical to: No other components

Dependencies: FIA_UAU.1.1 Timing of authentication.

FIA_AFL.1.1/Suspend_PIN The TSF shall detect when 2 unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the PIN as the shared password for PACE.

FIA_AFL.1.2/Suspend_PIN When the defined number of unsuccessful authentication attempts has been met, the TSF shall suspend the reference value of the PIN according to [TR-03110-2].

Application note: R.Sigy is able to resume the suspended PIN using PACE with the CAN and subsequently PACE with the PIN.

11.5.8 FIA_AFL.1/Block_PIN Authentication failure handling – Blocking PIN

Defined in: EAC v2 PP [CC_PP-0086]

Hierarchical to: No other components.

Dependencies: FIA_UAU.1.1 Timing of authentication.

FIA_AFL.1.1/Block_PIN The TSF shall detect when 1 unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the suspended PIN as the shared password for PACE.

FIA_AFL.1.2/Block_PIN When the defined number of unsuccessful authentication attempts has been met, the TSF shall block the reference value of the PIN according to [TR-03110-2].

11.5.9 FIA_AFL.1/PACE (Authentication failure handling – PACE authentication using non-blocking authorization data)

Defined in: PP PACE [CC_PP-0068]

Hierarchical to: No other components.

Dependencies: FIA_UAU.1.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE.

FIA_AFL.1.1/PACE The TSF shall detect when *1*[100] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password[101].

[96] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[97] [assignment: *list of authentication events*]
[98] [selection: *met, surpassed*]
[99] [assignment: *list of actions*]
[100] [assignment: *positive integer number*]
[101] [assignment: *list of authentication events*]

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been met[102], the TSF shall *consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords*[103].

11.6 Class FMT Security Management (FMT)

11.6.1 FMT_SMR.1 Security Roles

Defined in: PP SCD [CC_PP_0075]

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[104].

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

11.6.2 FMT_SMF.1 Specification of Management Functions

Defined in: PP SCD [CC_PP_0075]

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[105].

11.6.3 FMT_MOF.1 Management of security functions behaviour

Defined in: PP SCD [CC_PP_0075]

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1 The TSF shall restrict the ability to enable[106] the signature creation function[107] to R.Sigy[108].

11.6.4 FMT_MSA.1/Admin Management of security attributes

Defined in: PP SCD [CC_PP_0075]

Hierarchical to: No other components.

[102] [selection: *met, surpassed*]
[103] [assignment: *list of actions*]
[104] [assignment: *the authorized identified roles*]
[105] [assignment: *list of security management functions to be provided by the TSF*]
[106] [selection: *determine the behavior of, disable, enable, modify the behavior of*]
[107] [assignment: *list of functions*]
[108] [assignment: *the authorized identified roles*]

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 Import SFP[109] to restrict the ability to modify[110] the security attributes SCD/SVD management[111] to R.Admin[112]

11.6.5 FMT_MSA.1/Signatory Management of security attributes

Defined in: PP SCD [CC_PP_0075]

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[113] to restrict the ability to modify[114] the security attributes SCD operational[115] to R.Sigy[116]

11.6.6 FMT_MSA.2 Secure security attributes

Defined in: PP SCD [CC_PP_0075]

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[117]

11.6.7 FMT_MSA.3 Static attribute initialization

Defined in: PP SCD [CC_PP_0075]

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 Import SFP and Signature Creation SFP[118] to provide restrictive [119] default values for security attributes that are used to enforce the SFP.

[109] [assignment: *access control SFP(s), information flow control SFP(s)*]
[110] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[111] [assignment: *list of security attributes*]
[112] [assignment: *the authorized identified roles*]
[113] [assignment: *access control SFP(s), information flow control SFP(s)*]
[114] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[115] [assignment: *list of security attributes*]
[116] [assignment: *the authorized identified roles*]
[117] [selection: *list of security attributes*]
[118] [assignment: *access control SFP, information flow control SFP*]
[119] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

FMT_MSA.3.2 The TSF shall allow the R.Admin[120] to specify alternative initial values to override the default values when an object or information is created.

11.6.8 FMT_MSA.4 Security attribute value inheritance

Defined in: PP SCD [CC_PP_0075]

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 imports SCD while S.Sigy is not currently authenticated, the security attribute “SCD operational” of the SCD shall be set to “no” as a single operation.
2. If S.Admin imports SCD while S.Sigy is currently authenticated, the security attribute “SCD operational” of the SCD shall be set to “yes” after import of the SCD as a single operation.

11.6.9 FMT_MTD.1/Admin Management of TSF data

Defined in: PP SCD [CC_PP_0075]

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[121] the RAD[122] to R.Admin[123]

11.6.10 FMT_MTD.1/Signatory Management of TSF data

Defined in: PP SCD [CC_PP_0075]

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[124] the RAD[125] to R.Sigy[126].

11.6.11 FMT_MTD.1/CVCA_INI Management of TSF data – Initialization of CVCA Certificate and Current Date

Defined in: EAC PP [CC_PP-0056]

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

[120] [assignment: *the authorized identified roles*]
[121] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[122] [assignment: *list of TSF data*]
[123] [assignment: *the authorized identified roles*]
[124] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[125] [assignment: *list of TSF data*]
[126] [assignment: *the authorized identified roles*]

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to write[127] the

1. initial Certification Authority Public Key,
2. initial Certification Authority Certificate,
3. initial Current Date,
4. *None*[128]

to the *Personalization Agent*[129].

11.6.12 FMT_MTD.1/CVCA_UPD Management of TSF data – Certification Authority

Defined in: EAC PP [CC_PP-0056]

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to update[130] the

1. Certification Authority Public Key,
2. Certification Authority Certificate,

to Certification Service Provider[131].

Application note: The Certification Service Provider updates its asymmetric key pair and distributes the public key be means of the CA Link-Certificates ([TR-03110-1]). The TOE updates its internal trust-point if a valid CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal ([TR-03110-1]).

Application note: This SFR has been adapted from [CC_PP-0056]. The objects Country Verifying Certification Authority Public Key and Country Verifier Certification Authority Certificate have been changed to Certification Authority Public Key and Certification Authority Certificate, respectively. The role Country Verifying Certification Authority, which does not exist in this context, has been changed to Certification Service Provider. This SFR applies only to the configurations requiring Terminal Authentication for the communication between the TOE and the SCA and the CGA.

11.6.13 FMT_MTD.1/DATE Management of TSF data – Current date

Defined in: EAC PP [CC_PP-0056]

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1/DATE The TSF shall restrict the ability to modify[132] the Current Date[133] to

1. Certification Service Provider,
2. Document Verifier,
3. Legitimate Terminal[134].

Application note: The authorized roles are identified in their certificate ([TR-03110-1]) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the

[127] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[128] [assignment: *list of TSF data*]
[129] [assignment: *the authorized identified roles*]
[130] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[131] [assignment: *the authorized identified roles*]
[132] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[133] [assignment: *list of TSF data*]
[134] [assignment: *the authorized identified roles*]

terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication v.1 ([TR-03110-1]).

Application note: This SFR has been adapted from [CC_PP-0056]. The role Country Verifying Certification Authority, which does not exist in this context, has been changed to Certification Service Provider. The role Domestic Extended Inspection System, which does not exist in this context, has been changed to Legitimate Terminal. This SFR applies only to the configurations requiring Terminal Authentication for the communication between the TOE and the SCA and the CGA.

11.6.14 FMT_MTD.1/CA_PK Management of TSF data – Chip Authentication Private Key

Defined in: EAC PP [CC_PP-0056]

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to *load*[135] the Chip Authentication Private Key[136] to the *Personalization Agent* [137].

Application note: The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory.

11.6.15 FMT_MTD.1/KEY_READ Management of TSF data – Key Read

Defined in: EAC PP [CC_PP-0056]

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read[138] the

1. PACE passwords ,
2. Chip Authentication Private Key,
3. Personalisation Agent Keys[139]
4. Electronic signature keys

to none[140].

The TOE shall meet the requirement “Secure TSF data (FMT_MTD.3)” as specified below ([CC_P2]):

This SFR has been adapted from [CC_PP-0056]. The object electronic signature keys have been added.

Application note: This SFR has been adapted from [CC_PP-0056]. The object electronic signature keys has been added.

11.6.16 FMT_MTD.3 Secure TSF data

Defined in: EAC PP [CC_PP-0056]

[135] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[136] [assignment: *list of TSF data*]
[137] [assignment: *the authorized identified roles*]
[138] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[139] [assignment: *list of TSF data*]
[140] [assignment: *the authorized identified roles*]

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data: fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD

FMT_MTD.3.1 The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control[141].

Refinement: The certificate chain is valid if and only if:

- the digital signature of the Legitimate Terminal Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Legitimate Terminal Certificate is not before the Current Date of the TOE,
- the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Certification Authority and the expiration date of the Certificate of the Certification Authority is not before the Current Date of the TOE and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,
- the digital signature of the Certificate of the Certification Authority can be verified as correct with the public key of the Certification Authority known to the TOE.

The Legitimate Terminal Public Key contained in the Legitimate Certificate in a valid certificate chain is a secure value for the authentication reference data of the Legitimate Terminal

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Legitimate Terminal.

Application note: The Terminal Authentication v.1 is used for Legitimate Terminal as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

Application note: This SFR has been adapted from [CC_PP-0056-V2]. The objects Country Verifying Certification Authority Public Key and Country Verifier Certification Authority Certificate have been changed to Certification Authority Public Key and Certification Authority Certificate, respectively.

The role Country Verifying Certification Authority, which does not exist in this context, has been changed to Certification Service Provider. This SFR applies only to the configurations requiring Terminal Authentication for the communication between the TOE and the SCA and the CGA.

11.7 Class FPT Protection of the TSF (FPT)

11.7.1 FPT_EMS.1/SSCD TOE Emanation

Defined in: PP SCD [CC_PP_0075]

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_EMS.1.1/SSCD The TOE should not emit Side Channel Current and Electromagnetic emanation[142] in excess of limits exploitable by State-of-the-Art attacks[143] enabling access to RAD[144] and SCD[145].

[141] [assignment: *list of TSF data*]
[142] [assignment: types of emissions]
[143] [assignment: specified limits]
[144] [assignment*: list of types of TSF data*]
[145] [assignment*: list of types of user data*]

FPT_EMS.1.2/SSCD The TOE shall ensure all users[146] are unable to use the following interface external contacts/contactless[147] to gain access to RAD[148] and SCD[149].

11.7.2 FPT_EMS.1/KEYS TOE Emanation

Defined in: EAC PP [CC_PP-0056]

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_EMS.1.1/KEYS The TOE shall not emit power variations, timing variations during command execution[150] in excess of non-useful information[151] enabling access to

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K MAC, PACE-KEnc),
3. the ephemeral private key ephem SK PICC-PACE,
4. *none*,
5. Personalisation Agent Key(s),
6. Chip Authentication Private Key[152] and
7. *none*[153].

FPT_EMS.1.2/KEYS The TSF shall ensure any users[154] are unable to use the following interface smart card circuit contacts[155] to gain access to

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K MAC, PACE-KEnc),
3. the ephemeral private key ephem SK PICC-PACE,
4. *none*,
5. Personalisation Agent Key(s),
6. Chip Authentication Private Key[156] and
7. none[157].

Application note: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip can provide a smart card contactless interface and contact based interface according to ISO/IEC 7816-2 as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to, variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

[146] [assignment: type of users]
[147] [assignment: type of connection]
[148] [assignment: *list of types of TSF data*]
[149] [assignment: *list of types of user data*]
[150] [assignment: *types of emissions*]
[151] [assignment: *specified limits*]
[152] [assignment: *list of types of TSF data*]
[153] [assignment: *list of types of user data*]
[154] [assignment: *type of users*]
[155] [assignment: *type of connection*]
[156] [assignment: *list of types of TSF data*]
[157] [assignment: *list of types of user data*]

The TOE shall meet the requirement “Failure with preservation of secure state (FPT_FLS.1)” as specified below ([CC_P2]).

11.7.3 FPT_FLS.1 Failure with preservation of secure state

Defined in: PP SCD [CC_PP_0075]

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. exposure to out-of-range (e.g. power shortage, over voltage) operating conditions where therefore a malfunction could occur. [158]

11.7.4 FPT_PHP.1 Passive detection of physical attack

Defined in: PP SCD [CC_PP_0075]

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.

11.7.5 FPT_PHP.3 Resistance physical attack

Defined in: PP SCD [CC_PP_0075]

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_PHP.3.1 The TSF shall resist operating changes by the environment[159], to the clock, voltage supply and shield layers[160] by responding automatically such that the SFRs are always enforced

Application note: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, ‘automatic response’ means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

11.7.6 FPT_TST.1 TSF Testing

Defined in: PP SCD [CC_PP_0075]

Hierarchical to: No other components.

Dependencies: No Dependencies.

[158] [assignment: *list of types of failures in the TSF*]
[159] [assignment: physical tampering scenarios]
[160] [assignment: list of TSF devices/elements]

FPT_TST.1.1 The TSF shall run a suite of self-tests during initial start-up or before calling a security sensitive module[161] to demonstrate the correct operation of the TSF[162].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data[163].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of TSF[164].

Application note: If the electronic document's chip uses state of the art smart card technology, it will run some self tests at the request of an authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the 'authorised user' Manufacturer in the life cycle phase 'Manufacturing'. Other self tests may automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as a countermeasure against Differential Failure Analysis.

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below ([CC_P2]).

11.8 Class FTP Trusted Path/Channels (FTP)

11.8.1 FTP_ITC.1/SCD Inter-TSF trusted channel

Defined in: PP SCD [CC_PP_0075]

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FTP_ITC.1.2/SCD The TSF shall permit another trusted IT product[165] to initiate communication via the trusted channel.

FTP_ITC.1.3/SCD The TSF shall initiate communication via the trusted channel for:

1. Data exchange integrity according to FDP_UCT.1/SCD[166]
2. none.

11.8.2 FTP_ITC.1/VAD Inter-TSF trusted channel – TC Human Interface Device

Defined in: PP SCD with key import and SCA [CC_PP_SCA_0076]

Hierarchical to: No other components.

Dependencies: No dependencies.

[161] [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*]]
[162] [selection: *[assignment: parts of TSF], the TSF*]
[163] [selection: *[assignment: parts of TSF data], TSF data*]
[164] [selection: *[assignment: parts of TSF], TSF*]
[165] [selection: *the TSF, another trusted IT product*]
[166] [assignment: *list of functions for which a trusted channel is required*]

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[167] 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[168]

11.8.3 FTP_ITC.1/DTBS Inter-TSF trusted channel – Signature creation Application

Defined in: PP SCD with key import and SCA [CC_PP_SCA_0076]

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[169] 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[170]

11.9 TOE Security Assurance Requirements

TOE assurance requirements are stated in Table 8. The assurance requirements of this evaluation are EAL5 augmented by AVA_VAN.5.

Table 8: Assurance Requirements - EAL 5+ extended with AVA_VAN.5

Assurance Class	Assurance Components
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.5 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures

[167] [selection: *the TSF, another trusted IT product*]
[168] [assignment: *list of functions for which a trusted channel is required*]
[169] [selection: *the TSF, another trusted IT product*]
[170] [assignment: *list of other functions for which a trusted channel is required*]

	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.2 Compliance with implementation standards
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ADV: Development	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_INT.2 Well-structured internals
	ADV_TDS.4 Semiformal modular design
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.3 Testing: modular design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

11.10 Security Requirements Rationale

The security functional requirements with assignment, selection and refinement operations for the TOE are listed in section 11.2 and they map exactly the functional requirements for the TOE.

11.10.1 Security Functional Requirements (SFRs) Coverage

The following Table 9 provides an overview for security objectives coverage.

Table 9: TOE Security functional requirements vs TOE Security Objectives

Security Objectives / SFR	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FCS_CKM.1/BAC	x										
FCS_CKM.1/DH_PACE	x				x					x	x
FCS_CKM.1/CA	x									x	x
FCS_CKM.4	x		x								
FCS_COP.1/RSA	x			x							
FCS_COP.1/ECDSA	x			x							
FCS_COP.1/SHA	x										
FCS_COP.1/CA_ENC	x									x	x
FCS_COP.1/CA_MAC	x									x	x
FCS_COP.1/PACE_ENC	x				x					x	x
FCS_COP.1/PACE_MAC	x				x					x	x
FCS_COP.1/SIG_VER	x									x	x
FCS_RND.1	x				x					x	x
FDP_ACC.1/TRM	x										
FDP_ACF.1/TRM	x										
FDP_ACC.1/SCD_Import	x	x									
FDP_ACC.1/Signature_Creation	x				x						
FDP_ACF.1/SCD_Import	x	x									

FDP_ACF.1/Signature_Creation	x				x						
FDP_ITC.1/SCD	x										
FDP_UCT.1/SCD	x		x								
FDP_RIP.1			x		x						
FDP_SDI.2/Persistent			x	x							
FDP_SDI.2/DTBS					X	x					
FDP_UIT.1/DTBS											x
FIA_UID.1		x			x						
FIA_UAU.1		x			x						
FIA_UAU.4/PACE	x				x					x	x
FIA_UAU.5/PACE	x				x					x	x
FIA_UAU.6	x				x					x	x
FIA_AFL.1/RAD					x						
FIA_AFL.1/Suspend_PIN					x						
FIA_AFL.1/Block_PIN					x						
FIA_AFL.1/PACE					x						
FMT_SMR.1	x				x						
FMT_SMF.1	x				x						
FMT_MOF.1	x				x						
FMT_MSA.1/Admin	x										
FMT_MSA.1/Signatory	x				x						
FMT_MSA.2	x				x						
FMT_MSA.3	x				x						
FMT_MSA.4	x				x						
FMT_MTD.1/Admin	x				x						
FMT_MTD.1/Signatory	x				x						
FMT_MTD.1/CVCA_INI	x										
FMT_MTD.1/CVCA_UPD	x									x	x
FMT_MTD.1/DATE	x										x
FMT_MTD.1/CA_PK	x										
FMT_MTD.1/KEY_READ	x									x	x
FMT_MTD.3											
FPT_EMS.1/SSCD			x				x				
FPT_EMS.1/KEYS							x				
FPT_FLS.1			x								
FPT_PHP.1								x			
FPT_PHP.3			x						x		
FPT_TST.1	x		x	x							
FTP_ITC.1/SCD	x		x								
FTP_ITC.1/VAD										x	
FTP_ITC.1/DTBS											x

11.10.2 Security Functional Requirements Sufficiency

In the following, a detailed justification as required to show the suitability and sufficiency of the security functional requirements to achieve the security objectives defined for the TOE is given.

11.10.2.1 OT.Lifecycle_Security (*Lifecycle security*)

The security objective is provided by the SFRs

- FCS_CKM.1/BAC
- FCS_COP.1/RSA (for SCD Usage)
- FCS_COP.1/ECDSA (for SCD Usage
- FCS_CKM.4 (SCD destruction)

which ensure cryptographically secure lifecycle of the SCD.

The SCD import is controlled by TSF according to

- FDP_ACC.1/SCD_Import

- FDP_ACF.1/SCD_Import and
- FDP_ITC.1/SCD

The confidentiality of the SCD is protected during the import according to

- FDP_UCT.1/SCD in the trusted channel
- FTP_ITC.1/SCD

The SCD usage is ensured by access control

- FDP_ACC.1/Signature_Creation,
- FDP_ACF.1/Signature_Creation

which are based on the security attribute secure TSF management according to SFRs:

- 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 function:

- FPT_TST.1

provides failure detection throughout the lifecycle.

OT.Lifecycle_Security, regarding integrity, confidentiality and authenticity, is ensured by the usage of a trusted channel. The means for the trusted channel are provided by the SFRs:

- FCS_CKM.1/DH_PACE (generation of PACE session keys),
- FCS_CKM.4 (destruction of session key),
- FCS_CKM.1/CA (DH and ECDH for CA session keys),
- FCS_COP.1/CA_ENC (symmetric encryption and decryption, CA),
- FCS_COP.1/CA_MAC (message authentication code, CA),
- FCS_COP.1/SIG_VER (signature verification, TA),
- FCS_COP.1/PACE_ENC (symmetric encryption and decryption, PACE),
- FCS_COP.1/PACE_MAC (message authentication code, PACE),
- FCS_RND.1 (PTG.3 random number generation),
- FCS_COP.1/SHA (DTBS calculation)
- FIA_UAU.4/PACE (single use authentication, Legitimate Terminal),

- FIA_UAU.5/PACE (authentication mechanisms) and
- FIA_UAU.6 (re-authentication, Legitimate Terminal).
- Further access permissions are addressed by the SFRs
- FDP_ACC.1/TRM (access control, Legitimate Terminal),
- FDP_ACF.1/TRM (security attribute-based access control, Legitimate Terminal),
- FMT_MTD.1/CVCA_UPD (management of TSF data, CVCA),
- FMT_MTD.1/DATE (management of TSF data, date),
- FMT_MTD.1/KEY_READ (management of TSF data, key read),
- FMT_MTD.1/CVCA_INI (Management of TSF data, Initialization of CVCA Certificate and Current Date), and
- FMT_MTD.1/CA_PK (management of TSF data, Chip Authentication Private Key).

11.10.2.2 OT.SCD_Auth_Imp (Authorized SCD import)

It addresses that import of SCD requires proper user authentication.

The TSF specified by

- FIA_UID.1 and
- FIA_UAU.1

provide user identification and user authentication prior to SCD can be imported.

The SFRs

- FDP_ACC.1/SCD_Import and
- FDP_ACF.1/SCD_Import

ensure that only authorised users can import SCD.

11.10.2.3 OT.SCD_Secrecy (Secrecy of signature creation data)

The security functions specified by

- FDP_UCT.1/SCD and
- FTP_ITC.1/SCD

ensures the confidentiality for SCD import.

The security objective is provided by the SFRs

- 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/SSCD and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

11.10.2.4 OT.Sig_Secure (Cryptographic security of the electronic signature)

It is provided by the cryptographic algorithms specified by

- FCS_COP.1/RSA
- FCS_COP.1/ECDSA

which ensure the cryptographic robustness of the signature algorithms.

The SFR

- FDP_SDI.2/Persistent

corresponds to the integrity of the SCD implemented by the TOE.

The SFR

- FPT_TST.1

ensures self-tests ensuring correct signature creation

11.10.2.5 OT.Sigy_SigF (Signature creation function for the legitimate signatory only)

It 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 SFR

- FMT_MTD.1/Admin and
- FMT_MTD.1/Signatory

manage the authentication function.

The SFR

- FIA_AFL.1/RAD

provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.

The SFR

- FIA_AFL.1/Suspend_PIN

provides protection against a denial-of-service attacks and the security functions specified by

- FIA_AFL.1/Block_PIN
- FIA_AFL.1/PACE

provides protection against brute force attacks against authentication.

The SFR

- 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 SFR

- 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.

The SFR

- FMT_MOF.1

restricts the ability to enable the signature creation function to the signatory.

The SFR

- FMT_MSA.1/Signatory

restricts the ability to modify the security attributes SCD operational to the signatory.

The signature creation function for the legitimate signatory only is additionally protected by the SFRs

- FCS_CKM.1/DH_PACE (generation of PACE session keys),
- FCS_COP.1/PACE_ENC (symmetric en- and decrytion, PACE)
- FCS_COP.1/PACE_MAC (message authentication code, PACE),
- FCS_RND.1 (PTG.3 random number generation),
- FIA_UID.1 (timing of dentification),
- FIA_UAU.4/PACE (single use authentication, Legitimate Terminal),
- FIA_UAU.5/PACE (authentication mechanisms) and
- FIA_UAU.6 (re-authentication, Legitimate Terminal)

providing a trusted channel

11.10.2.6 OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE)

It 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.

11.10.2.7 OT.EMSEC_Design (Provide physical emanations security)

It covers that no intelligible information is emanated. This is provided by

- FPT_EMS.1/SSCD
- FPT_EMS.1/KEYS

11.10.2.8 OT.Tamper_ID (Tamper detection)

It is provided by the SFR

- FPT_PHP.1 (Passive detection of physical attack)

by the means of passive detection of physical attacks.

11.10.2.9 OT.Tamper_Resistance (*Tamper resistance*)

It is provided by the SFR

- FPT_PHP.3 (Resistance physical attack)

to resist physical attacks.

11.10.2.10 OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import) is provided by

It is provided by

- FTP_ITC.1/VAD (TC Human Interface Device)

to provide a trusted channel to protect the VAD provided by the HID to the TOE.

The functionality for integrity and confidentiality is provided by

- FCS_CKM.1/DH_PACE (generation of PACE session keys),
- FCS_CKM.1/CA
- FCS_CKM.4 (destruction of session key),
- FCS_COP.1/CA_ENC (symmetric en- and decrytion, CA),
- FCS_COP.1/CA_MAC (message authentication code, CA),
- FCS_COP.1/PACE_ENC (symmetric en- and decrytion, PACE),
- FCS_COP.1/PACE_MAC (message authentication code, PACE),
- FCS_RND.1 (PTG.3 random number generation),
- FIA_UID.1 (timing of identification),
- FIA_UAU.4/PACE (single use authentication, Legitimate Terminal),
- FIA_UAU.5/PACE (authentication mechanisms), and
- FIA_UAU.6 (re-authentication, Legitimate Terminal).

The functionality for terminal authentication is provided by:

- FCS_COP.1/SIG_VER (signature verification)

Further access permissions are addressed by the SFRs

- FMT_MTD.1/CVCA_UPD (management of TSF data, CVCA) and
- FMT_MTD.1/KEY_READ (management of TSF data, key read).
- FMT_MTD.3

11.10.2.11 OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS)

It is provided by

- FTP_ITC.1/DTBS (Signature creation Application),

to provide a trusted channel to protect the DTBS provided by the SCA `to the TOE, and by

- FDP_UIT.1/DTBS (Data exchange integrity),

which requires the TSF to verify the integrity of the received DTBS.

The functionality for integrity and confidentiality is provided by

- FCS_CKM.1/DH_PACE (generation of PACE session keys),
- FCS_CKM.1/CA,
- FCS_CKM.4 (destruction of session key),
- FCS_COP.1/CA_ENC (symmetric en- and decrytion, CA),
- FCS_COP.1/CA_MAC (message authentication code, CA),
- FCS_COP.1/PACE_ENC (symmetric en- and decrytion, PACE),
- FCS_COP.1/PACE_MAC (message authentication code, PACE),
- FCS_RND.1 (PTG.3 random number generation),
- FIA_UID.1 (timing of identification),
- FIA_UAU.4/PACE (single use authentication, Legitimate Terminal),
- FIA_UAU.5/PACE (authentication mechanisms) and
- FIA_UAU.6 (re-authentication, Legitimate Terminal).

The functionality for terminal authentication is provided by:

- FCS_COP.1/SIG_VER

Further access permissions are addressed by the SFRs

- FMT_MTD.1/CVCA_UPD (management of TSF data, CVCA) and
- FMT_MTD.1/KEY_READ (management of TSF data, key read).
- FMT_MTD.1/DATE (management of TSF data, date).

11.10.3 Satisfaction of Dependencies of Security Requirements

The Table 10 and Table 11 below resume all the SFR SAR dependencies.

Table 10: Satisfaction of dependencies of security functional requirements

SFR	Dependencies	Satisfied By
FCS_CKM.1/BAC	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_CKM.4
FCS_CKM.1/DH_PACE	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_CKM.4
FCS_CKM.1/CA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/DH_PACE FCS_CKM.1/CA

FCS_COP.1/SCD/RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.4
FCS_COP.1/SCD/ECDSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.4
FCS_COP.1/SHA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	See justification 1
FCS_COP.1/CA_ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA FCS_CKM.4
FCS_COP.1/CA_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA FCS_CKM.4
FCS_COP.1/PACE_ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/DH_PACE FCS_CKM.4
FCS_COP.1/PACE_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/DH_PACE FCS_CKM.4
FCS_RND.1	No dependencies	n/a
FDP_ACC.1/TRM	FDP_ACF.1	FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1, FDP_ACC.1/TRM, FMT_MSA.3	FDP_ACF.1/TRM, See justification 2
FDP_ACC.1/SCD_Import	FDP_ACF.1	FDP_ACF.1/SCD_Import
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACF.1/SCD_Import	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_ACF.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_ITC.1/SCD	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_UCT.1/SCD	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	FPT_ITC.1/SCD, FDP_ACC.1/SCD_Import
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
FIA_UID.1	No dependencies	n/a
FIA_UAU.4/PACE	No dependencies	n/a
FIA_UAU.5/PACE	No dependencies	n/a
FIA_UAU.6	No dependencies	n/a
FIA_AFL.1\RAD	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1\Suspend_PIN	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1\Block_PIN	FIA_UAU.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1	FIA_UID.1
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_Import, 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_Import, 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_Import, FDP_ACC.1/Signature_Creation
FMT_MTD.1/CVCA_INI	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/ CVCA_UPD	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/DATE	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/CAPK	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/KEY_READ	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
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/SSCD	No dependencies	n/a
FPT_EMS.1/KEYS	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/SCD	No dependencies	n/a
FTP_ITC.1/VAD	No dependencies	n/a
FTP_ITC.1/DTBS	No dependencies	n/a

Justification for non-satisfied dependencies between the SFR for TOE:

Justification n. 1: The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore, neither a key generation (FCS_CKM.1 nor an import (FDP_ITC.1/2) is necessary.

Justification n. 2: The access control TSF according to FDP_ACF.1/TRM uses security attributes which are defined during the personalisation and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

Table 11: Satisfaction of dependencies of security assurance requirements

Assurance requirement(s)	Dependency	Satisfied By
EAL5 package	(dependencies of EAL5 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.5, ADV_TDS.4, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3 (all are included in EAL5 package)

11.10.4 Rationale for chosen security assurance requirements

The assurance level for this ST is EAL5 augmented. EAL5 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, EAL5 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.

12 TOE summary specification

This section contains a high-level specification of each TOE Security Function (TSF) that contributes to satisfaction of the Security Functional Requirements of chapter 11.

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.

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 STEID_EPKI - Operational User Guidance.

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)..

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

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.

12.1 TOE Security Functions

This part lists the TOE Security Functions. In the following TOE HARDWARE is intended the Integrated Circuit ST31N600 with embedded library. The TOE Security Functions are grouped as shown in the table below:

Table 12: List of TOE security functions

Family	Security Function	Description
Identification and Authentication	SF.AUTH SF.RAD SF.PACE SF.EAC	Personalization Agent authentication RAD management PACE Protocol EAC
Access Control	SF.AC	Access Control
Key Management and Cryptography	SF.CRY SF.SHA SF.SIGN	Cryptographic Support Hash computation Signature functions
Secure Messaging	SF.SM	Secure Messaging
Data Protection	SF.PRO	Self Test and Audit Un-observability TOE logical integrity Secure destruction of the data Anti-tearing function
OSPlat	SF.OS_PLAT	Data integrity memory management, I/O functions, atomic data transaction, RNG, secure cryptographic functions, Test Physical protection

12.1.1 SF.AUTH – Personalization Agent authentication

The purpose of this TOE security function is to authenticate the role of “Personalization Agent” when the TOE is in the life cycle step 6 “SSCD personalization”. After a successful authentication, the “Personalization Agent” takes control of the TOE and executes the steps and operations as described section 6.4.3.

The authentication mechanism is based on challenge-response protocol according to [ICAO_9303] using the AES algorithm and key length of 128 bits. It is detailed in the Preparative User Guidance of this TOE [AGD_PRE]. The Personalization Agent Authentication Key(s) are pre-loaded in the TOE during the step 5 “SSCD initialization & pre-personalization”.

With the personalization agent is authenticated, this security function grants:

- FCS_CKM.1/BAC (for key derivation)
- FCS_RND.1
- FIA_UAU.4/PACE
- FIA_UAU.5/PACE
- FMT_MSA.1/Admin
- FMT_MTD.1/Admin
- FMT_MTD.1/CVCA_INI
- FMT_MTD.1/CA_PK
- FMT_SMR.1 (Security Roles)
- FMT_SMF.1 (Specification of Management Functions)

12.1.2 SF.RAD – User authentication and RAD management

This TOE security function controls all operations related to the user authentication and Reference Authentication Data (RAD) management. It includes unblock and change of the RAD.

12.1.2.1 Verification

The user authentication is realized with the PIN, whose minimum length is set to 6 characters. The character set is composed by all the symbols that can be represented using two hexadecimal digits.

The TOE verifies that his VAD corresponds to RAD presented by the user.

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.

The maximum PIN retry counter is set to the value 3.

With the user authentication based on PIN mechanism, this security function grants:

- FIA_UAU.1 allowing or denying access to the TSFs. The SF.RAD is adequate for FIA_UAU.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1/RAD to be 3 prevents successful PIN attack.
- FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FDP_ITC.1/SCD, FDP_UCT.1/SCD allowing or denying the SCD importation.
- FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation so that only to the “Signatory” is allowed to sign the DTBS/R sent by an authorized SCA. The “Signatory”

authentication is based on PIN mechanism. The SF.RAD is adequate for FDP_ACF.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1/RAD to be 3 prevents successful PIN attack.

- FTP_ITC.1/SCD, FTP_ITC.1/VAD and FTP_ITC.1/DTBS so that the TOE establishes a trusted channel with a trusted IT product CGA. This function addresses the CGA authentication.
- FMT_MTD.1/Signatory so that only to the “Signatory is allowed unblock/change the RAD_S. This function addresses the “Signatory” authentication by the TOE allowing or denying the RAD change functionality.
- FMT_SMR.1 (Security Roles)
- FMT_SMF.1 (Specification of Management Functions) so that during TOE Operational phase a user must be successfully identified and authenticated before allowing any command execution on behalf of that user.

12.1.2.2 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.

12.1.2.3 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.

SF.RAD contributes to:

- FDP_ACC.1/Signature Creation, FDP_ACF.1/Signature Creation as a support mechanism in the “Signatory” authentication process performing a match between a VAD and a RAD_S stored in the TOE.
- FIA_AFL.1/RAD as a support mechanism in the user authentication process.
- FMT_MTD.1/Signatory as a support mechanism in the “Signatory” authentication process performing a match between a VAD and a RAD_S stored in the TOE.

12.1.3 SF.AC – Access Control

The TOE operates in accordance with the access policies according to FDP_ACC.1/TRM, FDP_ACF.1/TRM and considers the management functions and user roles.

This TSF checks that, for each operation initiated by a subject on data and keys, the security attributes for that role’s authorization are satisfied. For example:

- To authorized user is allowed import the SCD.
- To the “Administrator” is allowed the management of the SCD 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

SF AC contributes to:

- FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FDP_ITC.1/SCD, FDP_UCT.1/SCD so that, during TOE Operational phase only to authorized user is allowed import the SCD. This function compares the security status required to process the command and allows or denies the SCD importation.
- FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation so that, during TOE Operational phase only to the “Signatory” is allowed sign DTBS/R. This function compares the security status required to process the command and allows or denies the DTBS/R signing.
- FMT_MTD.1/Admin so that, during TOE Operational phase only to the “Administrator” is allowed change the RAD_S This function compares the security status required to process the command and allows or denies the change of the RAD_S.
- FMT_MTD.1/Signatory so that, during TOE Operational phase only to the “Signatory” is allowed change the RAD_S. This function compares the security status required to process the command and allows or denies the change of the RAD_S.

SF AC grant:

- FMT_MOF.1 so that, during TOE Operational phase, only to the “Signatory” is allowed sign DTBS/R.
- FMT_MSA.1/Admin so that, during TOE Personalization phase, only to the “Administrator” is allowed the management of the SCD/SVD security attributes.
- FMT_MSA.1/Signatory so that, during TOE Operational phase, only to the “Signatory” is allowed to change in “active” the operational state of the SCD.
- FMT_MSA.2 so that, during TOE Operational phase only to authorized user is allowed to set and change security attributes. Moreover, the function specifies that the security attribute change is possible only when the change doesn’t compromise the TOE security state. This function compares the security status required to process the command and allows or denies the set or the change of the security attributes.
- FMT_MSA.3.1 so that, during TOE Operational phase only to authorized user is allowed to set and change security attributes. This function compares the security status required to process the command and allows or denies the set or the change of the security attributes. When the SCD is generated, the authorized user shall set the SCD’s security attribute “SCD operational” to “no”.
- FMT_MSA.3.2 so that, during TOE Operational phase only to authorized user is allowed to set and change security attributes. This function compares the security status required to process the command and allows or denies the set or the change of the security attributes. At object creation time the “Administrator” decides the security attributes related to the created object.
- FMT_MSA.4 so that, during TOE Operational phase only to authorized user is allowed to generate an SCD/SVD pair. When the SCD is generated, the authorized user shall set the SCD’s security attribute “SCD operational” according to proper role.

Moreover, the function covers the management, write, update and read of stored keys and data as defined in FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CA_PK and FMT_MTD.1/KEY_READ.

The TSF SF_AC access control allows the users in Personalisation Agent role during the step 6 “SSCD personalization” to write in TOE final and genuine personalisation data.

12.1.4 SF.PACE – PACE Protocol

The TOE implements security mechanism to authenticate external entities and assigns roles and right.

The TOE implements the PACE protocol with negotiation of session keys (FCS_CKM.1/DH-PACE). This protocol provides key component (FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC) to set up a secured channel (FTP_ITC.1/SCD, FTP_ITC.1/VAD, FTP_ITC.1/DTBS) and to ensure a secure key exchange between the TOE and a terminal. This protocol provides authentication mechanisms implementing the SFRs FIA_UID.1, FIA_UAU.1, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6, FMT_SMR.1. The implementation of PACE considers the SFR FIA_AFL.1/PACE requirement to prevent hacker attacks.

PACE protocol is configured to set the card to a suspended state (FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN) before the secret is finally blocked (only PIN) or to delay the processing of the authentication command after a failed authentication (CAN).

The negotiated session keys are used to establish secure channels to protect data confidentiality and integrity during communication implementing the SFRs FDP_UCT.1/SCD, FTP_ITC.1/SCD, FTP_ITC.1/VAD and FTP_ITC.1/DTBS.

12.1.5 SF.EAC – Extended Access Control

The TOE implements security mechanism to authenticate external entities and assign roles and right.

The TOE implements the Extended Access Control (EAC) mechanism to protects and restricts access to the usage and management of SCDs and RADs contained in the TOE and the SVD for preventing unauthorized access and skimming. The TOE chip protected by EAC will allow that this SCD/SVD/RAD operations and management shall be performed (through an encrypted channel) only by authorized terminals (FDP_ACF.1/TRM).

The Extended Access Control is a mutual device authentication mechanism defined in [TR-03110-1] and [ICAO_9303] more precisely, the composition of the Terminal Authentication v.1 protocol and the Chip Authentication v.1 protocol, allows mutual authentication between a terminal and a chip and the establishment of an authenticated and encrypted connection between the TOE and the terminal (FIA_UID.1 , FIA_UAU.1, FIA_UAU.5/PACE, FMT_MTD.3).

The TOE checks by secure messaging in MAC_ENC mode each command whether it was sent by the successfully authenticated terminal (FIA_UAU.6)

The authentication mechanisms as part of EAC Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging (FDP_UCT.1/SCD, FTP_ITC.1/SCD, FTP_ITC.1/VAD and FTP_ITC.1/DTBS).

12.1.6 SF.HASH – Hash Computation

This function generates a hashing of data, using the algorithms SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 [FIPS_PUB180_4] . The obtained hash (160 bits) or (256 bits) is stored in the TOE and may be used for the digital signature computation.

This function contributes to FCS_COP.1/SHA satisfaction.

12.1.7 SF.SIGN –Electronic Signature Calculation

The function signs imported data (DTBS/R), using a RSA with private key length of 2048, 3072 and 4096 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 raw RSA, RSASSA-PKCS1-v1_5 and RSASSA-PSS (see [PKCS1_v2_2] and [RFC3447]).

The function signs imported data (DTBS/R), using ECC with private key length of 192, 224, 256, 384, 512 and 521 bits in conformance with the algorithm ECDSA (see [FIPS_PUB_186-4] and [ANSI X9.62]).

The function is protected against the SPA/DPA/DFA attack.

SF.SIGN grants:

- the FCS_COP.1/RSA satisfaction specifying that the TOE correctly performs a digital signature generation using a key of length up to 4096 bits and the RSA CRT algorithms.
- the FCS_COP.1/ECDSA satisfaction specifying that the TOE correctly performs a digital signature generation using a key of length 192, 224, 256, 384, 512 and 521 bit and the ECC algorithms.

12.1.8 SF.CRY – Cryptographic Support

This TOE Security Function is responsible for providing cryptographic support to all the other TOE Security Functions including secure key generation and operations on data such as signature creation/verification, encrypt, decryption, hashing, MAC generation/verification and random number generation:

- The TSF provides all the cryptographic basic mechanisms to implement the EAC protocol Terminal authentication v.1 (FCS_COP.1/SIG_VER):
  - EAC RSA, with 1024-, 2048-, 3072-, and 4096-bits RSA key, v1.5 and PSS
  - EAC RSA, with SHA-1, SHA-256, and SHA-512
  - EAC ECDSA with 192-, 224-, 256-, 320-, 384-, 512-, and 521-bits EC Key
  - EAC ECDSA with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512
- The TSF provides all the cryptographic basic mechanisms to implement the Chip authentication v.1:
  - DH, with 1024- and 2048-bits DSA key
  - DH, with secure messaging based on DES keys and 128, 192, and 256 bits AES keys
  - ECDH, with 192, 224, 256, 320, 384, 512, and 521 bits EC Key
  - ECDH, with secure messaging based on DES keys and 128, 192, and 256 bits AES keys
- The TSF provides the secure generation of symmetric Key for secure messaging (FCS_CKM.1/BAC,FCS_CKM.1/DH-PACE, FCS_CKM.1/CA). The TSF produces agreed parameters to generate the 3DES/AES key and the Retail-MAC/AES CMAC message authentication keys for secure messaging by the algorithm in [ICAO_9303], Normative appendix A5.1. The algorithm uses the random number generated by TSF as required by FCS_RND.1.
- The TSF provides the secure generation of symmetric Key for secure messaging (FCS_CKM.1/DH-PACE, FCS_CKM.1/CA). The TSF produces agreed parameters to generate the AES key and the AES CMAC message authentication keys for secure messaging by the algorithm in [ICAO_9303], Normative appendix A5.1. The algorithm uses the random number generated by TSF as required by FCS_RND.1.
- The TSF provides high quality Random Number Generator (FCS_RND.1) compliant with the [AIS20/31]. This generator is a deterministic RNG of level DRG.3 according to supporting enhanced backward and forward secrecy.

- The TSF provides Hashing Cryptographic operations (FCS_COP.1/SHA) SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 for key generation and digital signature generation/verification.
- The TSF provides 3DES cipher for encryption/decryption in CBC mode and cryptographic key size 112 bits (FCS_COP.1/PACE_ENC, FCS_COP.1/CA_ENC).
- The TSF provides AES cipher for encryption/decryption in CBC mode and cryptographic key size 128, 192 and 256 bits (FCS_COP.1/PACE_ENC, FCS_COP.1/CA_ENC).
- The TSF provides message authentication based on Retail-MAC and cryptographic key size 112 bits (FCS_COP.1/PACE_MAC, FCS_COP.1/CA_MAC).
- The TSF provides message authentication based on CMAC and cryptographic key size 128, 192 and 256 bits (FCS_COP.1/PACE_MAC, FCS_COP.1/CA_MAC).
- The TSF provides all the cryptographic basic mechanisms to implement the PACE DH, with Generic Mapping, dynamic binding, based on DES keys and 128, 192, and 256-bits AES keys derived from CAN, PIN or PUK.
- The TSF provides all the cryptographic basic mechanisms to implement the PACE ECDH, with Generic Mapping, static or dynamic binding, based on DES keys and 128, 192 and 256 bits AES keys derived from CAN, PIN or PUK.
- The TSF provides RSA digital signature algorithm with raw RSA, PKCS1_v1.5 and PSS padding based on RSA keys size 2048, 3072 and 4096 bits (FCS_COP.1/RSA).
- The TSF provides ECC digital signature algorithm based on EC keys size 192, 224, 256, 384, 512 and 521 bits (FCS_COP.1/ECDSA).
- The TSF provides support for secure destruction of cryptographic key secret or private material (FCS_CKM.4).

12.1.9 SF.SM – Secure Messaging

The TOE implements a trusted channel providing confidentiality and integrity of transferred data according to the FTP.ITC.1/PACE, FIA_UAU.5/PACE requirements. The trusted channel is using AES and 3DES cipher for encryption in CBC mode and cryptographic key sizes 112, 128, 192 and 256 bits as selected and defined in the SFRs FCS_COP.1/PACE_ENC and FCS_COP.1/CA_ENC. The trusted channel is using a message authentication code generation in CMAC and Retail-MAC mode and cryptographic key sizes 112, 128, 192 and 256 bits as selected and defined in the SFRs FCS_COP.1/PACE_MAC and FCS_COP.1/CA_MAC. The TSF SF_SM uses new fresh random (FCS_RND.1) at each set up of the trusted channel between TOE and terminal.

The TSF grants the FDP_SDI.2/DTBS and FDP_UIT.1/DTBS satisfaction. The DTBS integrity is checked before its use. When an integrity error is found the TOE aborts the current operation and notifies the condition externally and the current PACE or Chip Authentication session is closed.

The TSF also grants the FTP_ITC.1/SCD, FTP_ITC.1/VAD and FTP_ITC.1/DTBS satisfaction. The function establishes a trusted channel with a remote IT product CGA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure.

12.1.10 SF.PRO – Data Protection

This TOE Security Function is responsible for protection of the TSF data, user data, and TSF functionality. The TSF SF_PRO Data Protection is composed of software implementations of test and security functions including:

- Performing self-tests of the TOE at each power-up including a set of tests to verify that the underlying cryptographic algorithms are operating correctly (FPT_TST.1)
- Initializing memory after reset
- Initializing memory of de-allocated data and secure destruction of cryptographic key, secrets and private material (FCS_CKM.4, FDP_RIP.1).
- Protecting the integrity of all stored cryptographic keys before use and preventing use of corrupted data by stopping the operation involved and setting an error (FCS_CKM.4, FDP_RIP.1, FDP_SDI.2/Persistent, FPT_PHP.1,).
- Preventing electromagnetic and power emissions or associated information like timing behavior, to preserve the confidentiality of stored keys or residual key material information (FPT_EMS.1/SSCD and FPT_EMS.1/KEYS).
- Preserving secure state after sensitive processing failure (RNG, power loss, memory or functional failure) or potential physical tampering or intrusion detection (FPT_FLS.1, FPT_PHP.3)

This TSF enforces protection of Key material during cryptographic functions processing and Key Generation, against state-of-the-art attacks, including IC power consumption analysis (FPT_EMS.1).

12.1.11 SF.OSPlat – Java Platform and OS

This TSF is implemented at SW layer JCS and OS 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: **SECURE_MANAGEMENT, CRYPTO, PIN_MANAGEMENT, ROLLBACK, and 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 ST31N600 including crypto library NESLIB V.6.2.1. The TSF provide and manages the following functionalities:

- Secure Management functionalities (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, (supporting fulfilment of, FPT_EMS.1/SSCD and FPT_EMS.1/KEYS).
  - Preservation of a secure state when the following types of failures occur: loss of power or card tearing, NVRAM memory wear-out, failed checksum verification on sensitive data (Supporting fulfilment of FPT_FLS.1).
  - 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 NVRAM consistency/integrity check failure (Supporting fulfilment of FPT_PHP.3).
  - Exception handling: 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.

- Testing: This function ensures the tests of TOE functionalities. It includes the test of Integrated Circuit ST31N600 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 (Supporting fulfilment of FPT_TST.1).

- Crypto Key management functionalities (CRYPTO) such as:
  - key destruction (supporting the fulfilment of SFRs: FCS_CKM.4)
  - Integrity and the unobservability of the keys.
- **Crypto Operation (CRYPTO)**: functionalities of encryption/decryption and signature creation/verification with the support of the following algorithms:
  - DES ECB and CBC
  - Triple DES ECB and CBC with 16, 24 bytes of key
  - AES ECB and CBC with 128, 192, 256 bits of key
  - RSA CRT raw, padding PKCS-v1_5 and padding PSS with key length 1024-, 2048-, 3072- and 4096-bits
  - ECC (ECDSA, ECKA) with key length up to 521 bits
  - Hashing (SHA-1, SHA224, SHA-256, SHA-384, SHA-512)
  - Deterministic Random Number Generation

Supporting the fulfilment of SFRs:

- FCS_CKM.1/BAC
- FCS_CKM.1/DH-PACE-3DES, FCS_CKM.1/DH-PACE-AES,
- FCS_CKM.1/ECDH-PACE-3DES, FCS_CKM.1/ECDH-PACE-AES,
- FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES,
- FCS_CKM.1/CA-ECDH-3DES, FCS_CKM.1/CA-ECDH-AES,
- FCS_COP.1/RSA
- FCS_COP.1/ECDSA
- FCS_COP.1/PACE_ENC, FCS_COP.1/CA_ENC,
- FCS_COP.1/PACE_MAC, FCS_COP.1/CA_MAC,
- FCS_COP.1/SIG_VER, FCS_RND.1,
- FCS_COP.1/SHA
- FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation,
- FDP_DAU.2/SVD
- FDP_RIP.1, FDP_SDI.2/Persistent, FDP_UIT.1/DTBS
- FPT_PHP.1

- **PIN Management Operation (PIN_MANAGEMENT)**: This functionality manages all operations related to PIN objects. 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. The integrity of the stored PIN value, try counter and verification status is guaranteed (supporting the fulfillment of SFRs FIA_AFL.1/RAD).

- **Data Transaction management (ROLLBACK)**: functionalities concerning NVRAM changes in order to assure the coherence of the data if a failure or power interruption occurs during their update.
- **Secure data deletion (OBJECT_DELETION)**: de-allocation of memory resources of data no longer accessible. The security functionality also guarantees that the information content of unreachable data cannot be retrieved anymore (supporting the fulfilment of SFRs: FCS_CKM.4).

12.1.12 Security Functional Requirements Coverage

The following table provides an overview for security functional requirements coverage.

Table 13: Functional requirements to TOE security functions mapping

SFR \ TSF	SF_AUTH	SF_RAD	SF_AC	SF_EAC	SF_PACE	SF_HASH	SF_SIGN	SF_SM	SF_CRY	SF_PRO	SF_OSPlat
FCS_CKM.1/BAC	x								x		x
FCS_CKM.1/DH-PACE					x				x		x
FCS_CKM.1/CA									x		x
FCS_CKM.4									x	x	x
FCS_COP.1/RSA							x		x		x
FCS_COP.1/ECDSA							x		x		x
FCS_COP.1/SHA						x			x		x
FCS_COP.1/PACE_ENC					x			x	x		x
FCS_COP.1/PACE_MAC					x			x	x		x
FCS_COP.1/CA_ENC								x	x		x
FCS_COP.1/CA_MAC								x	x		x
FCS_COP.1/SIG_VER									x		x
FCS_RND.1								x	x		x
FDP_ACC.1/TRM			x								
FDP_ACF.1/TRM			x	x							
FDP_ACC.1/SCD_Import		x	x								
FDP_ACC.1/Signature_Creation		x	x								x
FDP_ACF.1/SCD_Import		x	x								
FDP_ACF.1/Signature_Creation		x	x								x
FDP_ITC.1/SCD		x	x								
FDP_UCT.1/SCD		x	x	x	x						
FDP_RIP.1										x	x
FDP_SDI.2/Persistent										x	x
FDP_SDI.2/DTBS								x			
FDP_UIT.1/DTBS								x			x
FIA_UID.1				x	x						
FIA_UAU.1	x			x	x						
FIA_UAU.4/PACE	x				x						

FIA_UAU.5/PACE	x			x	x			x			
FIA_UAU.6	x			x							
FIA_AFL.1/RAD		x									x
FIA_AFL.1/Suspend_PIN					x						
FIA_AFL.1/Block_PIN					x						
FIA_AFL.1/PACE					x						
FMT_SMF.1	x	x									
FMT_SMR.1	x	x			x						
FMT_MOF.1			x								
FMT_MSA.1/Admin	x		x								
FMT_MSA.1/Signatory			x								
FMT_MSA.2			x								
FMT_MSA.3			x								
FMT_MSA.4			x								
FMT_MTD.1/Admin	x		x								
FMT_MTD.1/Signatory		x	x								
FMT_MTD.1/CVCA_INI	x		x								
FMT_MTD.1/CVCA_UPD			x								
FMT_MTD.1/DATE			x								
FMT_MTD.1/CA_PK	x		x								
FMT_MTD.1/KEY_READ			x								
FMT_MTD.3				x							
FPT_EMS.1/SSCD										x	x
FPT_EMS.1/KEYS										x	x
FPT_TST.1										x	x
FPT_FLS.1										x	x
FPT_PHP.1										x	x
FPT_PHP.3										x	x
FTP_ITC.1/SCD		x		x	x			x			
FTP_ITC.1/VAD		x		x	x			x			
FTP_ITC.1/DTBS		x		x	x			x			

13 Statement of compatibility

This is a Statement of Compatibility between this Security Target of the composite TOE and the Security Target of the STeID JC Open OS v1.0 platform [ST_SteidJCOS].

The following tables show the mapping between SARs, SFRs, and Objectives of the platform ST and this ST, demonstrating the compatibility between the two STs.

13.1 Security Assurance Requirements (SARs) mapping

The following table shows the mapping between the STeID JC Open OS platform SARs and this composite TOE SARs. The platform is certified EAL6 augmented with ALC_FLR.2. The composite TOE is certified EAL5 augmented with ALC_DVS.2 and AVA_VAN.5. There is no conflict regarding the Security Assurance Requirements (SARs) because the composite TOE SARs represent a subset of the platform SARs.

Table 14: Platform SARs vs composite TOE SARs

STeID JC Open OS platform SARs (EAL6 augmented with ALC_FLR.2)	Composite TOE SARs (EAL5 augmented with ALC_DVS.2 and AVA_VAN.5)
ADV_ARC.1	ADV_ARC.1
ADV_FSP.5	ADV_FSP.5
ADV_IMP.2	ADV_IMP.1
ADV.INT.3	ADV.INT.2
ADV_SPM.1	-
ADV_TDS.5	ADV_TDS.4
AGD_OPE.1	AGD_OPE.1
AGD_PRE.1	AGD_PRE.1
ALC_CMC.5	ALC_CMC.4
ALC_CMS.5	ALC_CMS.5
ALC_DEL.1	ALC_DEL.1
ALC_DVS.2	ALC_DVS.2 (augmentation)
ALC_FLR.2 (augmentation)	-
ALC_LCD.1	ALC_LCD.1
ALC_TAT.3	ALC_TAT.2
ASE_CCL.1	ASE_CCL.1
ASE_ECD.1	ASE_ECD.1
ASE_INT.1	ASE_INT.1
ASE_OBJ.2	ASE_OBJ.2
ASE_REQ.2	ASE_REQ.2
ASE_SPD.1	ASE_SPD.1
ASE_TSS.1	ASE_TSS.1
ATE_COV.3	ATE_COV.2
ATE_DPT.3	ATE_DPT.3
ATE_FUN.2	ATE_FUN.1
ATE_IND.2	ATE_IND.2
AVA_VAN.5	AVA_VAN.5 (augmentation)

13.2 Threats compatibility

The following table shows the compatibility between the STeID JC Open OS platform Threats and this composite TOE Threats.

Table 15: Compatibility between Platform and composite TOE Threats

STeID JC Open OS platform Threats	Rationale
T.CONFID-APPLI-DATA	The attacker executes an application to disclose data belonging to another application. Threat considered in the composite TOE.
T.CONFID-JCS-CODE	The attacker executes an application to disclose the Java Card System code. Threat covered by the platform evaluation.
T.CONFID-JCS-DATA	The attacker executes an application to disclose data belonging to the Java Card System. Threat covered by the platform evaluation.
T.INTEG-APPLI-CODE	The attacker executes an application to alter (part of) its own code or another application's code. Threat considered in the composite TOE.
T.INTEG-APPLI-CODE.LOAD	The attacker modifies (part of) its own or another application code when an application package is transmitted to the card for installation. Threat considered in the composite TOE.
T.INTEG-APPLI-DATA	The attacker executes an application to alter (part of) another application's data. Threat considered in the composite TOE.
T.INTEG-APPLI-DATA.LOAD	The attacker modifies (part of) the initialization data contained in an application package when the package is transmitted to the card for installation. The threat has been considered in the composite TOE.
T.INTEG-JCS-CODE	The attacker executes an application to alter (part of) the Java Card System code. Threat covered by the platform evaluation.
T.INTEG-JCS.DATA	The attacker executes an application to alter (part of) Java Card System or API data. Threat covered by the platform evaluation.
T.SID.1	An applet impersonates another application, or even the Java Card RE, in order to gain illegal access to some resources of the card or with respect to the end user or the terminal. Threat considered in the composite TOE.
T.SID.2	The attacker modifies the TOE's attribution of a privileged role (e.g. default applet and currently selected applet), which allows illegal impersonation of this role. Threat considered in the composite TOE.
T.EXE-CODE.1	An applet performs an unauthorized execution of a method. Threat considered in the composite TOE.
T.EXE-CODE.2	An applet performs an execution of a method fragment or arbitrary data. Threat considered in the composite TOE.
T.NATIVE	An applet executes a native method to bypass a TOE Security Function such as the firewall. Threat covered by the platform evaluation.

T.RESOURCES	An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM. Threat covered by the platform evaluation.
T.DELETION	The attacker deletes an applet or a package already in use on the card, or uses the deletion functions to pave the way for further attacks (putting the TOE in an insecure state). Threat covered by the platform evaluation.
T.INSTALL	The attacker fraudulently installs post-issuance of an applet on the card. This concerns either the installation of an unverified applet or an attempt to induce a malfunction in the TOE through the installation process). Threat covered by the platform evaluation.
T.OBJ-DELETION	The attacker keeps a reference to a garbage collected object in order to force the TOE to execute an unavailable method, to make it to crash, or to gain access to a memory containing data that is now being used by another application. Threat covered by the platform evaluation.
T.PHYSICAL	The attacker discloses or modifies the design of the TOE, its sensitive data or application code by physical (opposed to logical) tampering means. This threat includes IC failure analysis, electrical probing, unexpected tearing, and DPA. That also includes the modification of the runtime execution of Java Card System or SCP software through alteration of the intended execution order of (set of) instructions through physical tampering techniques. Threat covered by the platform evaluation.
T.LOADER_MISUSE	The attacker performs unauthorised use of the software loader functionality to upload a modified or malicious software version. Threat covered by the platform evaluation.

13.3 Assumptions compatibility

The following table shows the compatibility between the STeID JC Open OS platform Assumptions and this composite TOE Assumptions.

Table 16: Compatibility between Platform and composite TOE Assumptions

STeID JC Open OS platform Assumptions	Rationale
A.CAP_FILE	CAP files loaded post-issuance do not contain native methods. Assumption covered by ADV_IMP.1 of the composite TOE.
A.DELETION	Deletion of applets through the card manager is secure. Assumption not related to the composite TOE.
A.VERIFICATION	All the bytecodes are verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. Assumption ensured by ALC_DVS.2 of the composite TOE.

13.4 Objectives compatibility

The following table shows the compatibility between the STeID JC Open OS platform Objectives and this composite TOE Objectives.

Table 17: Platform Objectives vs composite TOE Objectives

STeID Open JCOS Objectives	Rationale
O.SID	Objective covered by the platform evaluation
O.FIREWALL	Objective covered by the platform evaluation
O.GLOBAL_ARRAYS_CONFID	Objective covered by the platform evaluation
O.GLOBAL_ARRAYS_INTEG	Objective covered by the platform evaluation
O.NATIVE	Objective covered by the platform evaluation
O.OPERATE	Objective covered by the platform evaluation
O.REALLOCATION	Objective covered by the platform evaluation
O.RESOURCES	Objective covered by the platform evaluation
O.ALARM	Objective also covered by the composite TOE
O.CIPHER	Objective also covered by the composite TOE
O.RNG	Objective covered by platform evaluation
O.KEY-MNGT	Objective also covered by the composite TOE
O.PIN-MNGT	Objective also covered by the composite TOE
O.TRANSACTION	Objective covered by the platform evaluation
O.OBJ-DELETION	Objective covered by the platform evaluation
O.DELETION	Objective covered by the platform evaluation
O.LOAD	Objective covered by the platform evaluation
O.INSTALL	Objective covered by the platform evaluation
O.SENSITIVE_RESULTS_INTEG	Objective covered by the platform evaluation
O.CARD-MANAGEMENT	Objective covered by the platform evaluation
O.SCP.RECOVERY	Objective also covered by the composite TOE
O.SCP.SUPPORT	Objective also covered by the composite TOE
O.SCP.IC	Objective covered by the platform evaluation
OT.ACCESS_CONTROL	Objective covered by the platform evaluation

13.5 Security objectives for the environment (OEs) compatibility

The following table shows the compatibility between the STeID JC Open OS platform OEs and this composite TOE OEs.

Table 18: Platform OEs vs Composite TOE OEs

STeID JC Open OS platform OEs	Rationale
OE.CAP_FILE	No applet loaded post-issuance shall contain native methods. This security objective is still relevant for the composite TOE and must be taken into account by the TOE user during the loading of additional applets.
OE.VERIFICATION	All the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. Additionally, the applet shall follow all the recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform. This security objective is still relevant for the composite TOE and must be taken into account by the TOE user during the loading of additional applets.
OE.CODE-EVIDENCE	For application code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that loaded application has not been changed since the code verifications required in OE.VERIFICATION. This security objective is still relevant for the composite TOE and must be taken into account by the TOE user during the loading of additional applets.
OE.KEY_PERSO	When the TOE life cycle is in manufacturing state, and before it is set to release state, all the default keys in the TOE are updated with final usage phase keys, FW authentication keys and the content loading keys. Objective covered by the platform evaluation.

13.6 Organizational security policies (OSPs) compatibility

The following table shows the compatibility between the STeID JC Open OS platform OSPs and this composite TOE OSPs.

STeID JC Open OS platform OSPs	Rationale
OSP.VERIFICATION	This policy shall ensure the consistency between the export files used in the verification and those used for installing the verified file. The policy must also ensure that no modification of the file is performed in between its verification and the signing by the verification authority. Policy covered by the platform evaluation

13.7 Compatibility between SFRs

The following table shows the compatibility between the STeID JC Open OS platform SFRs and this composite TOE SFRs. STeID JC Open OS platform SFRs are separated in the following groups as defined in [SOGIS-COMP]:

- IP_SFR: irrelevant Platform SFR not being used by the composite TOE

- RP_SFR-MECH: relevant Platform SFR being used by the composite TOE because its security properties providing protection attacks to the composite TOE
- RP_SFR-SERV: relevant Platform SFR being used by the composite TOE to implement a security service with associated TSFI

Table 19: Platform SFRs vs composite TOE SFRs

STeID JC Open OS platform SFRs	Rationale
FDP_ACC.2/FIREWALL	FIREWALL access control. RP_SFR-MECH
FDP_ACF.1/FIREWALL	FIREWALL access control. RP_SFR-MECH
FDP_IFC.1/JCVM	JCVM information flow control. RP_SFR-MECH
FDP_IFF.1/JCVM	JCVM information flow control. RP_SFR-MECH
FDP_RIP.1/OBJECTS	Any previous information content of a resource is made unavailable upon the allocation of the resource. RP_SFR-MECH
FMT_MSA.1/JCRE	FIREWALL access control. RP_SFR-MECH
FMT_MSA.1/JCVM	FIREWALL access control and JCVM information flow control. RP_SFR-MECH
FMT_MSA.2/FIREWALL_JCVM	FIREWALL access control and JCVM information flow control. RP_SFR-MECH
FMT_MSA.3/FIREWALL	FIREWALL access control. RP_SFR-MECH
FMT_MSA.3/JCVM	JCVM information flow control. RP_SFR-MECH
FMT_SMF.1/CM	Management Functions. RP_SFR-MECH
FMT_SMR.1/CM	Security roles. RP_SFR-MECH
FCS_CKM.1	Cryptographic key generation. RP_SFR-SERV
FCS_CKM.4	Cryptographic key destruction. RP_SFR-SERV
FCS_COP.1	Cryptographic operation. RP_SFR-SERV
FCS_RNG.1/IC	Random number generation. RP_SFR-SERV
FCS_RNG.1/DRBG	Random number generation. RP_SFR-SERV
FDP_RIP.1/ABORT	Subset residual information protection. RP_SFR-MECH
FDP_RIP.1/APDU	Subset residual information protection. RP_SFR-MECH
FDP_RIP.1/bArray	Subset residual information protection. RP_SFR-MECH
FDP_RIP.1/GlobalArray	Subset residual information protection. RP_SFR-MECH
FDP_RIP.1/KEYS	Subset residual information protection. RP_SFR-MECH
FDP_RIP.1/TRANSIENT	Subset residual information protection. RP_SFR-MECH
FDP_ROL.1/FIREWALL	Basic rollback. RP_SFR-MECH
FAU_ARP.1	Security alarms. RP_SFR-MECH
FDP_SDI.2/DATA	Stored data integrity monitoring and action. RP_SFR-MECH
FPR_UNO.1	Unobservability. RP_SFR-MECH
FPT_FLS.1	Failure with preservation of secure state. RP_SFR-MECH
FPT_TDC.1	Inter-TSF basic TSF data consistency. RP_SFR-MECH
FIA_ATD.1/AID	User attribute definition. RP_SFR-MECH
FIA_UID.2/AID	User identification before any action. RP_SFR-MECH
FIA_USB.1/AID	User-subject binding. RP_SFR-MECH
FMT_MTD.1/JCRE	Management of TSF data. RP_SFR-MECH
FMT_MTD.3/JCRE	Secure TSF data. RP_SFR-MECH
FDP_ITC.2/Installer	Import of user data with security attributes. RP_SFR-MECH
FMT_SMR.1/Installer	Security roles. RP_SFR-MECH
FPT_FLS.1/Installer	Failure with preservation of secure state. RP_SFR-MECH
FPT_RCV.3/Installer	Automated recovery without undue loss. RP_SFR-MECH
FDP_ACC.2/ADEL	Complete access control by Applet deletion manager. RP_SFR-MECH
FDP_ACF.1/ADEL	Security attribute based access control of the Applet deletion manager. RP_SFR-MECH
FDP_RIP.1/ADEL	Subset residual information protection by Applet deletion manager. RP_SFR-MECH
FMT_MSA.1/ADEL	Management of security attributes by Applet deletion manager. RP_SFR-MECH

FMT_MSA.3/ADEL	Static attribute initialisation by Applet deletion manager. RP_SFR-MECH
FMT_SMF.1/ADEL	Management Functions of the Applet deletion manager. RP_SFR-MECH
FMT_SMR.1/ADEL	Security roles of the Applet deletion manager. RP_SFR-MECH
FPT_FLS.1/ADEL	Failure with preservation of secure state by Applet deletion manager. RP_SFR-MECH
FDP_RIP.1/ODEL	Subset residual information protection of the object deletion. RP_SFR-MECH
FPT_FLS.1/ODEL	Failure with preservation of secure state of the object deletion. RP_SFR-MECH
FCO_NRO.2/CM	Enforced proof of origin of package loading. RP_SFR-MECH
FDP_IFC.2/CM	Complete information flow control of package loading. RP_SFR-MECH
FDP_IFF.1/CM	Simple security attributes of package loading. RP_SFR-MECH
FDP_UIT.1/CM	Data exchange integrity of package loading. RP_SFR-MECH
FIA_UID.1/CM	Timing of identification of package loading. RP_SFR-MECH
FMT_MSA.1/CM	Management of security attributes of package loading. RP_SFR-MECH
FMT_MSA.3/CM	Static attribute initialisation of package loading. RP_SFR-MECH
FMT_SMF.1/CM	Specification of Management Functions. RP_SFR-MECH
FMT_SMR.1/CM	Security roles. RP_SFR-MECH
FTP_ITC.1/CM	Inter-TSF trusted channel. RP_SFR-MECH
FDP_SDI.2/RESULT	Integrity_Sensitive_Result. RP_SFR-MECH
FPT_TST.1	TSF Testing. RP_SFR-MECH
FTP_ITC.1/Loader	Inter-TSF trusted channel of the flash loader. IP_SFR
FDP_UIT.1	Data exchange integrity of the flash loader. IP_SFR
FDP_ACC.1/Loader	Subset access control of the flash loader. IP_SFR
FDP_ACF.1/Loader	Security attribute based access control of the flash loader. IP_SFR

13.8 Conclusion

There are no contradictions between the ST of this composite TOE and the ST of the underlying STeID JC Open OS platform [ST_SteidJCOS].

14 Safety requirements

N/A

15 Environmental requirements

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

16 Revision history

Date	Revision	Changes
October 22, 2025	A	Initial release
October 31, 2025	B	TOE physical scope includes platform guidance
December 22, 2025	C	Add CC certificate platform reference Update revision for ST of the platform

17 Contents

18 List of tables

19 List of figures