Public Security Target

CombICAO Applet v3

on ID-One Cosmo X

SSCD Configuration

Reference: FQR 550 0284 Ed 6

DOCUMENT EVOLUTION

Date	Version	Name	Revision
29/11/2021	Ed 1	IDEMIA	Sanitized version created for Public Issue.
01/02/2022	Ed 2	IDEMIA	Sanitized version created for Public Issue after incorporating ANSSI feedbacks.
16/01/2023	Ed 3	IDEMIA	Remove BIO PIN from Evaluation scope see chapters **Erreur ! Source du renvoi introuvable.** and **Erreur ! Source du renvoi introuvable.**. Update [AGD_PRE], [AGD_OPE], [ST_PTF] and [PTF_CERT] references
28/03/2023	Ed 4	IDEMIA	Update [PTF_CERT] and [ST_PTF] references.
19/07/2023	Ed 5	IDEMIA	Update [PTF_CERT] and [ST_PTF] references. Add ALC_FLR.1
19/01/2026	Ed 6	INSI	Update for re-evaluation 2025

Table of contents

Table of figures

Table of tables

1 Security Target Introduction

1.1 ST Identification

Title	CombICAO Applet v3 in SSCD configuration on ID-One Cosmo X Public Security Target
ST Identification	FQR 550 0284 Ed 6
CC Version	3.1 revision 5
Assurance Level	EAL5 augmented with ALC_DVS.2, ALC_FLR.1 and AVA_VAN.5
ITSEF	CEA-LETI
Certification Body	ANSSI
Compliant to Protection Profile	[PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6]

1.2 TOE Reference

TOE Commercial Name	CombICAO Applet v3 in SSCD configuration on ID-One Cosmo X
Applet Code Versions (SAAAAR Code)	'20 37 42 FF'
Applet Internal Version	'00 00 02 0D'
Platform Name	ID-One Cosmo X
Platform Certificate	[PTF_CERT]
Guidance Documents	[AGD_PRE], [AGD_OPE].

2 Technical Terms, Abbreviations and Associated References

2.1 Technical Terms

Term	Definition
Agreement	This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
Authenticity	Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organization
Basic Access Control	Security mechanism defined in [ICAO_9303] by which means the travel document's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
Biographical data (bio data).	The personalised details of the bearer of the travel document appearing as text in the visual and machine readable zones on the biographical data page of a travel document [ICAO_9303].
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data.
Card Access Number (CAN)	Password derived from a short number printed on the front side of the data-page.
Certificate chain	A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means.
Country Signing CA Certificate (C_{CSCA})	Self-signed certificate of the Country Signing CA Public Key ($K_{Pu\ CSCA}$) issued by CSCA stored in the inspection system.
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the

Term	Definition
	PKI for the travel documents and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO_9303], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-3].
Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [TR-03110-3]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organizational entity within this ST. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO_9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-3].
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CV Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Details Data	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state,

Term	Definition
	document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (CDS). [ICAO_9303]
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [ICAO_9303]. This role is usually delegated to a Personalisation Agent.
Document Verifier (DV)	An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, see [TR-03110-3]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this ST. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy) [1] [2]
Eavesdropper	A threat agent with low attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip.

[1] The form of such an agreement may be of formal and informal nature; the term 'agreement' is used in the current ST in order to reflect an appropriate relationship between the parties involved.

[2] Existing of such an agreement may be technically reflected by means of issuing a CCVCA-F for the Public Key of the foreign CVCA signed by the domestic CVCA.

Term	Definition
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO_9303]
travel document (electronic)	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
ePassport application	[PP-EAC] definition Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes the file structure implementing the LDS [ICAO_9303], the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and the TSF Data including the definition the authentication data but except the authentication data itself.
Extended Access Control	Security mechanism identified in [ICAO_9303] by which means the travel document's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalisation Agent may use the same mechanism to authenticate themselves with Personalisation Agent Authentication Private Key and to get write and read access to the logical travel document and TSF data.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all travel document's. [ICAO_9303]
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

Term	Definition
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document.
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO_9303]
Initialisation	Process of writing Initialisation Data (see below) to the TOE (TOE life-cycle, Phase 2 Manufacturing, Step 3).
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as travel document material (IC identification data).
Inspection	The act of a State examining an travel document presented to it by a traveller (the travel document's holder) and verifying its authenticity. [ICAO_9303]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO_9303]]
Issuing State	The Country issuing the travel document. [ICAO_9303]

Term	Definition
Logical travel document	Data of the travel document holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) personal data of the travel document holder the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), the digitized portraits (EF.DG2), the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and the other data according to LDS (EF.DG5 to EF.DG16). EF.COM and EF.SOD
Machine Readable Travel Document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO_9303]
Machine Readable Zone (MRZ)	Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [ICAO_9303].
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO_9303]
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [TR-03110-3]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date.
Optional biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.

Term	Definition
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [ICAO_9303] part 11. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
PACE passwords	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO_9303] part 11 or a user PIN or PUK as specified in [TR-03110-3]
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the "Enrolment" (cf. paragraph 1.7.4.3, TOE life-cycle, Phase 3, Step 6).
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: ICAO travel document (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [TR-03110-1], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO_9303] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.

Term	Definition
Personalisation Data	A set of data incl. individual-related data (biographic and biometric data) of the travel document holder, dedicated document details data and dedicated initial TSF data (incl. the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing.
Personalisation Agent Authentication Information	TSF data used for authentication proof and verification of the Personalisation Agent.
Personalisation Agent Key	Symmetric cryptographic key or key set (MAC, ENC) used by the Personalisation Agent to prove his identity and get access to the logical travel document.
Physical part of the travel document	travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) biographical data, data of the machine-readable zone, photographic image and other data.
Pre-personalisation	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (TOE life-cycle, Phase 2, Step 5)
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the travel document Manufacturer (Phase 2) for traceability of non-personalised travel document's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalisation Agent Key Pair and Chip Life-Cycle Production data (CPLC data).
Pre-personalised travel document's chip	travel document's chip equipped with a unique identifier.
Receiving State	The Country to which the travel document holder is applying for entry. [ICAO_9303]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.

Term	Definition
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443].
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means [ICAO_9303].
Secure messaging in encrypted /combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]
Service Provider	An official organisation (inspection authority) providing inspection service which can be used by the travel document holder.
Skimming	Imitation of a rightful terminal to get access to the user data stored on or transferred between the TOE and the Inspection authority connected via the contactless/contact communication channel of the TOE without knowledge of the MRZ, CAN, PIN and PUK PACE passwords.
Standard Inspection Procedure [SIP]	A specific order of authentication steps between an travel document and a terminal as required by [ICAO_9303] and [TR-03110-1], namely PACE or BAC and Passive Authentication with SO_D.
Inspection Procedure for multi-application travel document's	This section describes an inspection procedure designed for travel document's containing one or more applications besides the travel document's application ("LDS2-documents"): [LDS2_TR] Annex A2.
Terminal	A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE.
Terminal Authorization	Intersection of the Certificate Holder Authorizations of the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be valid for the Current Date.
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
travel document	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use,

Term	Definition
	reflecting essential data elements capable of being machine read; see [ICAO_9303] (there "Machine readable travel document").
travel document (electronic)	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: *ePassport*.
travel document Holder	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document.
travel document's Chip	A contact based / contactless integrated circuit chip complying with ISO/IEC 14443 [15] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO_9303], sec III.
Traveller	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [CC1]).
Unpersonalised travel document	The travel document that contains the travel document chip holding only Initialisation Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.
User data	All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [5] and being allowed to be read out solely by an authenticated terminal. CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC2]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO_9303]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

2.2 Abbreviations

Acronym	Definition
ADF	Application Dedicated File
BAC	Basic Access Control
BAT	Basic Authentication Terminal
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
CHAT	Certificate Holder Authorization Template
CLFDB	Ciphered Load File Data Block
CMT	Certificate Management Terminal
DES	Data Encryption Standard
DH	Diffie Hellman
DSK	Dump Secret Key
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EF	Elementary File
GP	Global Platform
IC	Integrated Chip
ICAO	International Civil Aviation Organization
ICC	Integrated Chip card
IS	Inspection System
LSK	Load Secure Key
MAC	Message Authentication code
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine readable zone
OE	Security Objectives for the Operational Environment
OSP	Organisational security policy
OT	Security Objectives for the TOE
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMT	Password Management Terminal
PP	Protection Profile
PS	Personalisation System
PT	Personalisation Terminal
QSCD	Qualified Signature Creation Device
RF	Radio Frequency
ROM	Read Only Memory
RSA	Rivest Shamir Adleman

RSA CRT	Rivest Shamir Adleman – Chinese Remainder Theorem
SAR	Security Assurance Requirement
SCP	Secure Channel Procotol
SFR	Security functional requirement
SHA	Secure Hashing Algorithm
SIP	Standard Inspection Procedure
SSCD	Secure Signature Creation Device
ST	Security Target
TA	Terminal Authentication
TOE	Target Of Evaluation
TSF	TOE Security Functions

2.3 References

Reference	Description
[ADDENDUM]	20190821-Module-PP0056 - v1.1
[AGD_OPE]	FQR 220 1641 Ed 4 - CombICAO Applet V3 on ID-One Cosmo X - AGD_OPE
[AGD_PRE]	FQR 220 1640 Ed 4 - CombICAO Applet V3 on ID-One Cosmo X - AGD_PRE
[ANSSI_NOTE_10]	JIL – Certification of "open" smart card products – Version 1.1 – 4 February 2013
[ANSIX9.31]	"Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (DSA)" – ANSI X9.31-1998, American Bankers Association
[ANSIX9.62]	ANSI x9.62-2005 Public Key Cryptography for the Financial Services Industry – The Elliptic Curve Digital Signature Algorithm (ECDSA)
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017. CCMB-2017-04-001.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-002.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004.
[CEN_14890]	CEN/EN 14890:2013 Application Interface for smart cards used as Secure Signature Creation.
[Directive]	Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a community framework for electronic signatures
[eIDAS_Regulation]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Reference	Description
[FIPS_180_4]	FIPS 180-4, Federal Information Processing Standards Publication (FIPS PUB) 180-4, Secure Hash Standard, August 2015
[FIPS_186_3]	FIPS 186-3, Federal Information Processing Standards Publication (FIPS PUB) 186-3, Digital Signature Standard (DSS), June 2009
[FIPS_197]	FIPS 197, Federal Information Processing Standards Publication (FIPS PUB 197), Advanced Encryption Standard (AES)
[FIPS_46_3]	FIPS 46-3, Federal Information Processing Standards Publication (FIPS PUB) 46-3, Data Encryption Standard (DES), 1999 October 25
[GP2.3]	Global Platform, Card Specification – Version 2.3 – October 2015.
[GPC_SPE_014]	GlobalPlatform Card Technology - Secure Channel Protocol '03', Card Specification v2.3 – Amendment D" Version 1.1.2 - Public Release March 2019
[GPC_SPE_034]	"GlobalPlatform Card Specification" Version 2.3.1 Public Release - March 2018
[ICAO_9303]	International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – 7th and 8th edition.
[IEEE]	IEEE Std 1363a-2004 Standard Specification of Public-Key Cryptography
[ISO_15946]	ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002
[ISO_18013-3]	ISO/IEC 18013-3: Information technology — Personal identification — ISO-compliant driving licence. Part 3: Access control, authentication and integrity validation, April, 2017
[ISO_TR_19446]	ISO/IEC TR 19446:2015 Differences between the driving licences based on the ISO/IEC 18013 series and the European Union specifications
[ISO_9796-2]	ISO/IEC 9796-2:2002 - Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function

Reference	Description
[ISO_9797_1]	ISO/IEC 9797-1 Information technology – Security techniques – Message Authentication codes (MACs) – part 1: Mechanisms using a block cipher, Second edition 2011-03-01
[ISO11770-2]	ISO/IEC 11770-2. Information Technology – Security techniques – Key management – part 2: Mechanisms using symmetric techniques, 1996
[ISO11770-3]	ISO/IEC 11770-3. Information Technology – Security techniques – Key management – part 3: Mechanisms using asymmetric techniques, 2015
[ISO14443]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2016
[ISO7816]	ISO/IEC 7816: Identification cards — Integrated circuit cards.
[NIST_800_38A]	NIST Special Publication 800-38A: 2001, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, December 2001
[NIST_800_38B]	NIST Special Publication 800-38B: 2005, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005
[PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard – June 14, 2002
[PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4 Revised November 1, 1993
[PP_BAC]	Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009
[PP_EAC]	EAC- Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0056 v1.10 25th march 2009
[PP_EACwPACE]	Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP0056-V2-2012-MA-02, version 1.3.2, 5th December 2012
[PP_IC]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014.

Reference	Description
[PP_PACE]	Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01, 22 July 2014
[PP-SSCD2]	Protection profiles for secure signature creation device — Part 2: Device with key Generation, EN 419211-2 : 18th May 2013, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, June 30 2016
[PP-SSCD3]	Protection profiles for secure signature creation device – Part3: Device with key import, EN 419211-3 : 14th September 2013, CEN/TC 224, BSI-CC-PP-0075-2012-MA-01, June 30 2016
[PP-SSCD4]	Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, EN 419211-4 : 12th October 2013, CEN/TC 224, BSI-CC-PP-0071-2012-MA-01, June 30 2016
[PP-SSCD5]	Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, EN 419211-5: 12th October 2013, CEN/TC 224, BSI-CC-PP-0072-2012-MA-01, June 30 2016
[PP-SSCD6]	Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application, EN 419211-6 : 25th July, 2014, CEN/TC 224, BSI-CC-PP-0076-2013-MA-01, June 30 2016
[PTF_CERT]	ANSSI-CC-2023/06-R01 - 18/12/2024
[ST_PTF]	Security Target Lite ID-ONE Cosmo X, FQR 110 A19A Ed 3
[QR_Guide]	FQR 220 1646 Ed 1 - CombICAO Applet V3 - Recommendations for Compatibility with QR
[RGS2_B1]	GUIDE DES MÉCANISMES CRYPTOGRAPHIQUES RÈGLES ET RECOMMANDATIONS CONCERNANT LE CHOIX ET LE DIMENSIONNEMENT DES MÉCANISMES CRYPTOGRAPHIQUES, Version 2.04 du 01 Janvier 2020
[SCP03]	Global Platform Card Technology, Secure Channel Protocol 03, Card Specification v 2.2 - Amendment D - Version 1.1 - September 2009

Reference	Description
[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 2.20, 26.02.2015 by BSI
[TR-03110-2]	Technical Guideline TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 2 – Extended Access Control Version 2 (EACv2),Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI), Version 2.21, 21.12.2016 by BSI
[TR-03110-3]	TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3: Common Specifications, version 2.21, 21-12-2016 by BSI
[TR-03111]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, 17.04.2009

3 TOE Overview and Description

3.1 TOE Overview

The TOE is a composite product made up of an embedded software developed by INSI using Java Card technology, composed on a Java Card open platform developed by IDEMIA.
The Java Card open platform has already been certified. For more details see [PTF_CERT].

The embedded software is made up of Java Card CombICAO Applet v3, which relies on Java Card API provided by the underlying Java Card open platform.

The CombICAO Applet v3 is a configurable applet designed primarily for Identification, Authentication, Signature generation, and as a Machine Readable Travel document (MRTD). This security target focuses on **Secure Signature Creation Device (SSCD)**. In addition, the product can be used as a **Qualified Signature Creation Device (QSCD)** used to create advanced or qualified signature in the sense of new [eIDAS_Regulation] provided the appropriate [QR_Guide] is respected.

In addition, the CombICAO Applet v3 supports the following secure authentication protocols defined in [TR-03110-1] and [TR-03110-3]:

- PACE protocol to ensure a trusted channel for secure communication between the TOE and a CGA and/or SCA, with
  - support for ECDH in Generic and Integrated Mapping modes (PACE-GM, PACE-IM),
  - MRZ, CAN, PIN and PUK passwords and
  - PIN/PUK suspend and resume mechanism
- Chip Authentication v1 (CAv1)
- Terminal Authentication v1 (TAv1)

The CombICAO Applet v3 is also evaluated in other configurations as mentioned in the Table below.

This ST considers the CombICAO Applet v3 in the **SSCD configuration**.

Configuration	PP Conformity	Extensions to the PP
BAC and CA	[PP_BAC]	- Active Authentication (AA) - Chip Authentication Protocol (v1) - Restart secure messaging in AES128, AES192 or AES256 secure messaging (in addition to 3DES) after Chip Authentication Protocol (v1)
EAC in combination with BAC	[PP_EAC]	- Active Authentication (AA) - Enhanced protection over Sensitive biometric data reading

Configuration	PP Conformity	Extensions to the PP
EAC with PACE	[PP_PACE]	- Active Authentication (AA) - PACE-CAM (Optional) - Automatic BAC phasing out - Enhanced protection over Sensitive biometric data reading
	[PP_EACwPACE]	
EAC with PACE for French ID	[PP_PACE]	- [ADDENDUM] - Active Authentication (AA) - PACE-CAM (Optional) - Automatic BAC phasing out - Enhanced protection over Sensitive biometric data reading
	[PP_EACwPACE]	
SSCD	**[PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], and [PP-SSCD6]**	- **ADMIN role** - **Integrity token** - **EAC v1 (Chip Authentication v1 and Terminal Authentication v1)** - **PACE**

Table 1 Different evaluated configurations of the CombICAO application

3.2 TOE Description

The TOE is compliant with the specification [CEN_14890], with the following types of data structures:

- Files (MF, EF's and ADF's);
- Keys;
- PINs;

All these files are organized within a File System compliant to part 4 of [ISO7816]. It represents the hierarchy between all the files. At the top of the structure stands the Master File, it is the default selected file after applet selection. Under the Master File, are located the Application Dedicated File(s). The Master File, as well as each ADF, may contain Elementary File, keys and/or PINs.

Each file is characterized by its own attributes, such as:

- Access conditions for read and write access (for EF) or selection (for ADF);
- File identifier;
- Location within the File System;
- Size (for EF);

The TOE allows to:

- create two types of file (Application Dedicated File and Elementary File), which updates the File System;
- read, update, resize any Elementary File;
- move within the File Structure by use of file selection;

3.2.1 Physical scope of the TOE

The TOE is physically made up of several components hardware and software.
Once constructed, the TOE is a bare microchip with its external interfaces for communication.

The TOE may be used on several physical medium like wafer, module, smart card or inlay, eCover, eDatapage and eMRTD booklet.

The physical medium on which the microchip is mounted is not part of the target of evaluation as it does not alter nor modify any security functions of the TOE. Also, the inlay production (if any) including the application of the antenna is not part of the TOE

3.2.2 Logical scope of the TOE

The TOE is made up of:

- The underlying Java Card open platform,
- The Java Card CombICAO Applet v3 code [Applet],
- The associated guidance documentation in [AGD_PRE] and [AGD_OPE] (delivered in electronic version),
- The (pre)personalization Agent Key sets.

Moreover, as the underlying platform is certified as a Java Card open platform and complies with the requirements of the Application note 10 [ANSSI_NOTE_10], and as the TOE complies also with [ANSSI_NOTE_10], the TOE may also contain any other applets that comply with [ANSSI_NOTE_10] and the specific requirements of the TOE stated in the guidance documents.

The TOE scope is shown in figure 1. Once constructed, the TOE is a bare microchip with its external interfaces for communication. The physical medium on which the microchip is mounted does not alter nor modify any security functions of the TOE.

A schematic overview of the TOE's logical architecture is shown in below figure:

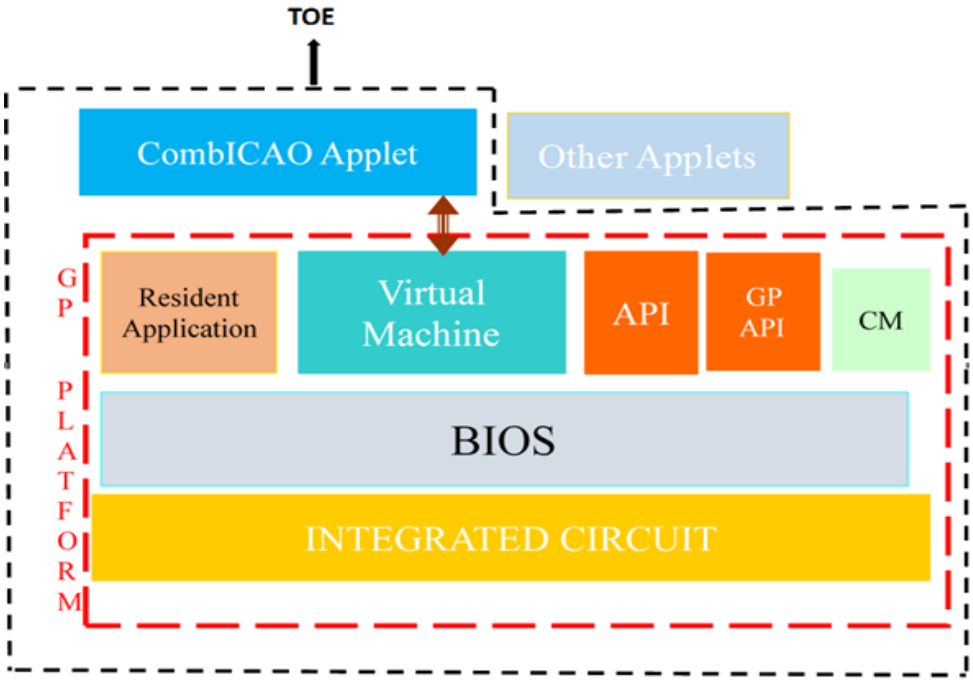


Figure 1 TOE's logical architecture

The following guidance documents will be provided with the TOE:

Guidance	Audience	Form Factor of Delivery
[AGD_PRE]	Personalising Agent	Electronic Version
[AGD_OPE]	End user of the TOE	

The following guide is provided only in case compliancy with QR scheme is required:

Guidance	Purpose	Form Factor of Delivery
[QR_Guide]	Recommendations for QR	Electronic Version

An ST Lite version of this Security Target will also be provided along with above-mentioned documents.

Platform related guidance documents are mentioned in [ST_PTF].

"Life Cycle" section in this ST provides more details about the TOE delivery for the different options.

3.3 Required non-TOE hardware/Software/firmware

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

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

3.4 TOE Usage and major security features of the TOE

The TOE intended usage is to be used as a "qualified signature creation device" with key generation and/or key import, with respect to the new [eIDAS_Regulation].

Since the TOE claims compliancy to protection profiles from CEN-EN 419 211-2 to CEN-EN 419 211-6 (Signature Protection Profiles **[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]** and **[PP-SSCD6]**), the TOE can be used as (depending on its configuration during personalization):

- Config#1 claiming compliancy to CEN/EN 419 211-2/3/4/5/6 (**[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]** and **[PP-SSCD6]**).
- Config#2 claiming compliancy to CEN/EN 419 211-2/3/4 (**[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**). This configuration does not support the trusted channel between the TOE and the SCA.
- Config#3 claiming compliancy to CEN/EN 419 211-2/3 (**[PP-SSCD2]**, **[PP-SSCD3]**). This configuration does not support the trusted channel between: (i) the TOE and the SCA; (ii) the TOE and the CGA.

Within the framework described by [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6], the TOE allows to:

- perform basic, advanced and qualified signature;
- authenticate the signatory thanks to PIN verification;
- authenticate one (or several) administrator(s) of the TOE, that may have special rights to administrate the SCD and SVD (generation, import);
- establish trusted channel, protected in integrity, authenticity and confidentiality, with trusted IT entities such as a CGA and SCA;
- Secure execution of services.

The scope of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6] is extended in several ways:

- Personalization phase including:
  - authentication protocol;
  - access control;
  - encryption mechanism involved in key loading;
  - initialization of the data structure;
  - data loading;
  - phase switching.

- All authentication protocols (PACE-GM/IM) and secure messaging type (DES-128,AES128/192/256);

- The integrity token of a public key that has been generated on card may be retrieved. It ensures that the public key is originated from an identified card and also ensures the integrity and the authenticity of the public key;

- All supported digital signature algorithm;

- Authentication of the TOE using asymmetric cryptography;

- All PIN management operations available after delivery point (spanning the three types of PIN : PIN_{Auth}, PIN_{Sig} (called also RAD) & PUK):
  - PIN initialization;
  - Upgrade of PIN attributes;
  - PIN change, unlocking, (re-)initialization;
  - Certificate management.

- PACE authentication;

- Extended Access Control Version 1 as defined in [TR-03110-1] and [TR-03110-3]. It consists of two parts: Chip Authentication Protocol Version 1 and Terminal Authentication Protocol Version 1;

- Signature key import in personalization phase and use phase;

- Signature key generation in personalization phase and use phase;

- Signature key public key export in personalization phase and use phase;

- Digital authentication feature including :
  - the corresponding key management operation (generation, import), and (
  - security policies applicable to each of these operations (authentication, generation, import);

The TOE may be used for various use cases requiring qualified signature:
- Digital signature application;
- Electronic health card;
- Electronic services cards etc.

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

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

3.4.1 Keys and PINs

The TOE handles as well cryptographic data objects, such as keys (for digital signature, authentication, and encryption key decipherment) and PINs.
The TOE enables to create, update and use PINs as detailed in [AGD_OPE].
For keys, the TOE enables to create, import, generate and erase keys as detailed in [AGD_OPE].

3.4.2 Access Control Management

The TOE ensures access control on any operations acting on any objects it handles (files, keys or PINs).

Each EF is configured at creation with access conditions protecting read and write access, while the ADF may be configured at creation with access conditions protecting their selection. Keys used for digital authentication, digital signature creation, encryption key decipherment and PINs require specific conditions before they can be used, updated or managed.

Prior to granting access to a given operation, the TOE checks the requested access rights are fulfilled. The access conditions can only be fulfilled upon successful authentication of an entity (see below).

3.4.3 Authentication of entities

The TOE allows authenticating several types of entities in order to grant them some access rights:

- **Authentication of a natural person**. It relies on a successful verification of a PIN code presented to the TOE by the natural person. (only available in phase 7)
- **Authentication of a remote server**. It relies on a mutual authentication - based on PKI - generating a trusted channel ensuring authenticity, integrity and confidentiality of the messages, used to securely communicate. (only available in phase 7)
- **Authentication of personalization agent** (only in phase 6);

These authentication mechanisms allows fulfilling the access control mechanisms described above.

3.4.4 Digital Authentication

The TOE supports digital authentication based on RSA and elliptic curves cryptography (ECC). Digital authentication is the process by which (1) the holder of TOE authenticates itself to the TOE using a PIN, releasing access right to an authentication key stored in the TOE, (2) subsequently the authentication key is used by the TOE to authenticate itself on behalf of the TOE holder. Digital authentication is useful so that the TOE holder can authenticate himself on line, without compromising any sensitive assets (PINs or authentication key).

3.4.5 Electronic Services

The TOE supports as well several electronic services:

- **Digital signature**: this feature enables the signatory to electronically signs documents. The signature may be either advanced or qualified (compliant with [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6]).
- **Encryption key decipherment**: this feature enables the document holder to store secret data on an electronic vault. The key needed to decipher the key encrypting these data is securely stored in the TOE. The document holder's computer sends the encrypted encryption key to the TOE to get the plain encryption key.

3.4.6 Trusted Channel function

This feature realizes a secure communication channel to verify authenticity and integrity as well as securing confidentiality of user data between the TOE and other devices connected. The TOE provides:

- Secure messaging with external applications such as CGA and SCA
- GP secure messaging in phase 6 and 7.
- PACE protocol for 3DES, AES128, AES192 and AES256 [ICAO_9303] secure messaging.
- TDES for encryption/decryption and MAC generation/verification
- AES128, AES192 and AES256 for encryption/decryption and MAC generation/verification
- Chip Authentication v1 (CAv1) used to establish new session keys for secure messaging

This feature is provided by the platform and used for secure messaging.

3.4.7 Secure execution

The TOE ensures a secure execution of its services. First, the TOE ensures its execution is protected against physical manipulation or attempt to tamper with. Secondly, should the execution of the TOE be tampered with in any manner, the TOE ensures it remains in a safe state protecting its assets and the TSFs, so that no vulnerabilities can be exploited by an attacker.

3.4.8 Other features

3.4.8.1 Key Usage Counter

The TOE supports an optional feature that allows the issuing country to limit the number of times a key may be used in the field, in particular the Chip Authentication key, the BAC key and the generated secure messaging key.

When configured, the corresponding Key Usage Counter is decremented for every operation the key is used and once the counter reaches zero (i.e. key is blocked), the key can no longer be used.

3.4.8.2 CA Key Renewal / Invalidation

When configured, the Chip Authentication key may be renewed or invalidated. This operation is protected by the Administration Agent key.

4 Life Cycle

The TOE life cycle in the following figure distinguishes stages for development, production, preparation and operational use in accordance with the standard smart card life cycle [PP_IC].

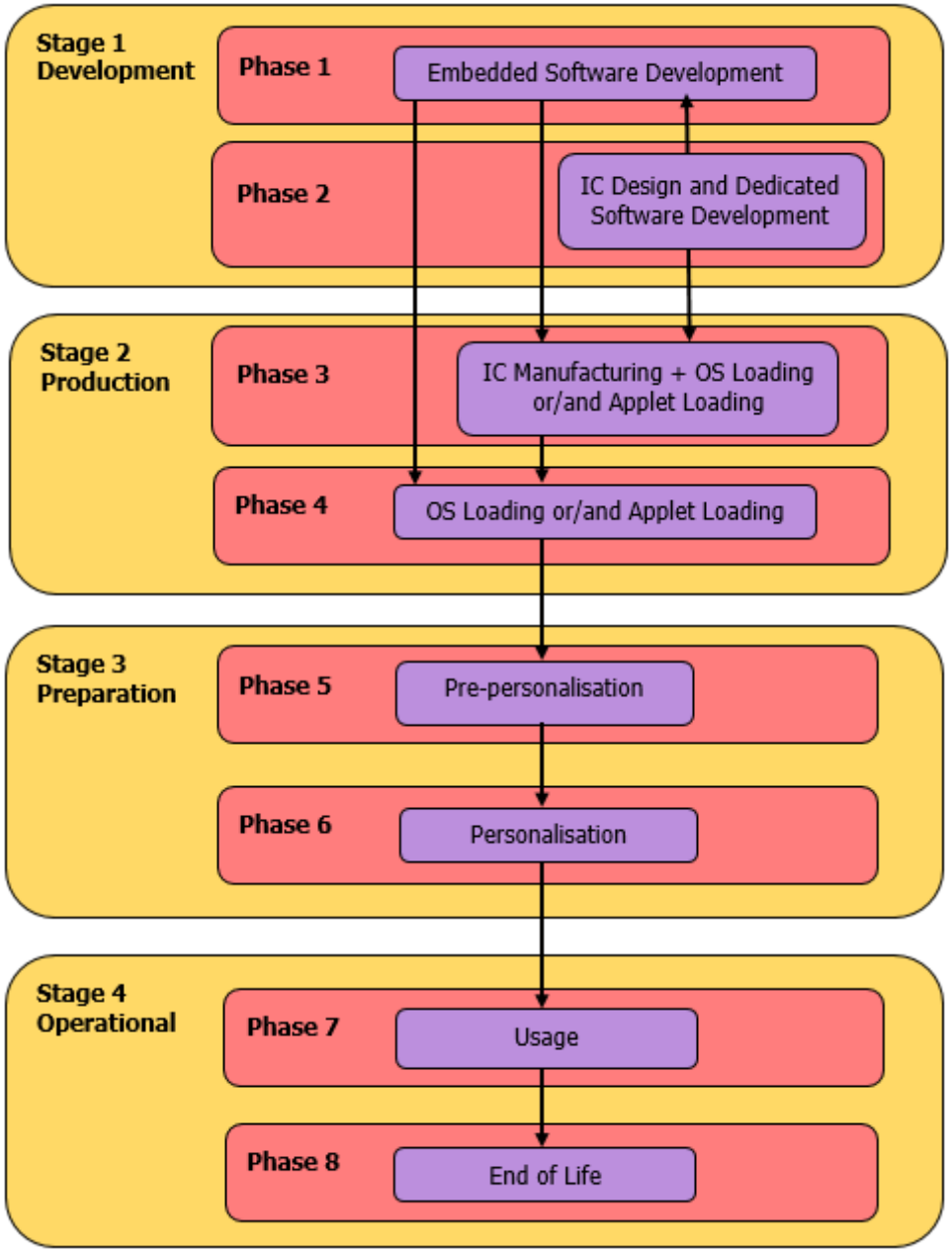


Figure 2 Life cycle Overview

4.1 Development Environment

In this environment, the following two phases take place:

- Phase 1: IC Embedded Software Development (Java Card Open Platform components and CombICAO Applet v3)
- Phase 2: IC Development

The IC Embedded Software Developer is in charge of the specification, development and validation of the software (Java Card Open Platform and CombICAO Applet v3).

The IC Developer designs the IC, develops the IC dedicated software and provides information, software or tools to the IC embedded software developer.

Roles, actors, sites and coverage for this environment of the product life-cycle are listed in the table below:

Role	Actor	Site	Covered by
CombICAO Applet v3 Developer	INSI	MANILA and COURBEVOIE R&D sites	ALC
Embedded Software Developer (Java Card Open Platform)	IDEMIA	Platform Developer Refer to [ST_PTF]	ALC
Redaction and Review of Documents	INSI	MANILA and COURBEVOIE R&D sites	ALC
IC Developer	INFINEON	IC Manufacturer Refer to [ST_PTF]	ALC

Table 2 : Development R&D Sites

4.2 Production Environment

In this environment, the following two phases take place:

- Phase 3: IC Manufacturing
- Phase 4: ID-One Cosmo X Platform loading and CombICAO Applet v3 loading

The CombICAO Applet v3 run time code is integrated in the FLASH memory of the chip.

Depending on the intention, the following different loading options are supported. Details on delivery methods for each option are provided in the **[AGD_PRE].**

INSI or IDEMIA CC Audited Production Sites are listed below:

INSI or IDEMIA CC Audited Production Sites/Plants	Country
Haarlem	Netherlands
Noida	India
Ostrava	Czech Republic
Shenzhen	China
Vitré	France

Table 3 : Audited Production Sites

(Option 1) Image Loading audited IC Manufacturer site

FLASH image containing both the "ID-One Cosmo X" Java Card Platform OS along with the CombICAO Applet v3 is securely delivered directly from the software developer (INSI or IDEMIA R&D Audited Site) to the **IC Manufacturer** (Infineon CC Audited Site) to be loaded into FLASH memory. The FLASH image is always encrypted.

TOE Delivery point (i.e. point in time where the TOE starts to exist):

- The TOE delivery point occurs in Phase 4, as soon as the loading of the image with ID-One Cosmo X Platform + CombICAO Applet v3 by the IC Manufacturer has been completed.

Package	Actor for FLASH image loading	Site For FLASH image loading	Covered by CC
FLASH image containing ID-One Cosmo X Platform + CombICAO Applet v3	IC Manufacturer	IC Manufacturer CC Audited Production Plants specified in [ST_PTF]	ALC

Table 4 Option 1: Both Platform and Applet packages are loaded at IC Manufacturer Site

(Option 2) Image loading at INSI or IDEMIA and External sites

FLASH image containing both ID-One Cosmo X Platform along with CombICAO Applet v3 is securely delivered directly from the software developer (INSI or IDEMIA R&D Audited Site) for loading to **CC Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

TOE Delivery point:

- If loading of ID-One Cosmo X Platform + CombICAO Applet v3 is performed in Audited INSI or IDEMIA Production Sites, then TOE delivery is considered at the end of Phase 4.

- If loading of ID-One Cosmo X Platform + CombICAO Applet v3 is performed in Non-Audited INSI or IDEMIA Production Sites or External Sites, then TOE delivery is considered after Phase 4.

Package	Actor for FLASH image loading	Site for FLASH image loading	Covered by CC
FLASH image containing the ID-One Cosmo X Platform + CombICAO Applet v3	INSI or IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited INSI or IDEMIA Sites or External Sites	AGD

Table 5 Option 2: Both Platform and Applet packages are loaded at CC Audited Sites

(Option 3) Platform loaded by IC Manufacturer, Applet loaded by INSI or 3rd party
Only the ID-One Cosmo X Platform is delivered to the IC Manufacturer (Infineon Audited Sites) to be loaded.

With the ID-One Cosmo X Platform already loaded (i.e. present) on the chip, the following options (**3a or 3b (i) or 3b (ii) or 3c**) can be chosen for loading the CombICAO Applet v3.

(Option 3a) Applet loading using GP CLFDB mechanism.

The CombICAO Applet v3 along with the TOE's guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

Loading of the CombICAO Applet v3 on top of the already present ID-One Cosmo X Platform GP Java Card OS in any of these sites is accomplished by using a GP CLFDB decryption Key.

TOE Delivery points:

- If loading of the CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform (as described below) is done in a CC Audited INSI or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of the CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited INSI or IDEMIA Production Sites or External Sites then, TOE delivery is considered after phase 4.

Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
CombICAO Applet v3 loaded through GP mechanism using CLFDB Key	INSI or IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited INSI or IDEMIA Sites or External Sites	AGD

Table 6 Option 3(a): Platform package is loaded at IC Manufacturer Site and Applet package is loaded at Audited INSI or IDEMIA Sites or Non-Audited INSI or IDEMIA Sites or External Sites through GP Mechanism

(Option 3b) Applet loading using the Resident Application

(i) CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

CombICAO Applet v3 package is securely loaded via LSK on top of the present ID-One Cosmo X Platform Java Card OS in any of these sites. This loading is accomplished by using the "Resident Application" of the ID-One Cosmo X Platform.

(ii) The DUMP package (including CombICAO Applet v3) with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

Loading of DUMP PACKAGES in any of these sites is done through Resident Application using DSK secret production key on top of the platform already loaded by IC Manufacturer (Infineon).

TOE Delivery points:

- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Audited INSI or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited INSI or IDEMIA Production Sites or External Sites then, TOE delivery after Phase 4.

Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
3b (i) CombICAO Applet v3 loaded through Resident Application using LSK format	INSI or IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited INSI or IDEMIA Sites or External Sites	AGD
3b (ii) DUMP PACKAGE Ciphered format [DSK Secret Live Key]	INSI or IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited INSI or IDEMIA Sites or External Sites	AGD

Table 7 Platform package is loaded at IC Manufacturer Site and Applet package is loaded through resident application using LSK format or DUMP Package in Ciphered format is loaded

(Option 3c) Applet loading in plain (unprotected) format using GP

CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **CC Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table).

Here, there is a provision for loading the applet in plain format in **Common Criteria Audited INSI or IDEMIA Sites only,** on top of the platform already loaded by IC Manufacturer (Infineon). This applet loading in plain format is not allowed in Non-Audited INSI or IDEMIA Sites or External Sites.

TOE Delivery points:

- The loading of CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform is done in plain (unprotected) format in Common Criteria Audited INSI or IDEMIA Production Sites. The TOE delivery is considered at the end of Phase 4.

Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
CombICAO Applet v3 in Plain Format	INSI Authorized Entity	Refer Audited Production Sites Table	ALC

Table 8 Option 3(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at Audited INSI Sites only

(Option 4) Platform and Applet loaded by INSI or IDEMIA or 3rd party
Only ID-One Cosmo X Platform is securely delivered directly from the software developer (INSI or IDEMIA R&D Audited Site) for loading to **CC Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

Note: Here, when the ID-One Cosmo X Platform package is loaded in Non-Audited INSI or IDEMIA Sites or External Sites, then the Platform is in self-protected mode by its secure functions

The following options (**4a or 4b (i) or 4b (ii) or 4c**) can be chosen for loading applets on top of the already loaded platform.

(Option 4a) Applet loading using GP CLFDB mechanism
CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

Loading of Applet in any of these sites is done through GP mechanism using CLFDB Key on top of the platform already loaded by **CC Audited INSI or IDEMIA Production Sites** or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

TOE Delivery points:

- If loading of the CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform (as described below) is done in CC Audited INSI or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of the CombICAO Applet v3 onto the already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited INSI or IDEMIA Production Sites or External Sites then, TOE delivery is considered after Phase 4.

Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	INSI or IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited INSI or IDEMIA Sites or External Sites	AGD
CombICAO Applet v3 loaded through GP mechanism using CLFDB Key	INSI or IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited INSI or IDEMIA Sites or External Sites	AGD

Table 9 Option 4(a): Platform package is loaded at Audited INSI or IDEMIA Sites or Non-Audited INSI or IDEMIA Sites or External Sites and Applet package is loaded at Audited INSI or IDEMIA Sites or Non-Audited INSI or IDEMIA Sites or External Sites through GP Mechanism

(Option 4b) Applet loading using the Resident Application

(i) CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

Secure loading of CombICAO Applet v3 is done via LSK on top of the present Cosmo X Java Card OS (already loaded by **Audited INSI or IDEMIA Production Sites** or **Non-Audited INSI or IDEMIA Sites** or **External Sites)** in any of these sites. This loading is accomplished by using the INSI or IDEMIA "Resident Application" of the ID-One Cosmo X Platform OS

(ii) DUMP package (including the CombICAO Applet v3) with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

Loading of DUMP PACKAGES in any of these sites is done through Resident Application using DSK secret production key on top of the platform already loaded by **Audited INSI or IDEMIA Production Sites** or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

TOE Delivery points:

- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Audited INSI or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited INSI or IDEMIA Production Sites or External Sites then, TOE delivery is considered after Phase 4.

Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	INSI or IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited INSI or IDEMIA Sites or External Sites	AGD
4b (i) CombICAO Applet v3 package loaded through Resident Application using LSK format	INSI or IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited INSI or IDEMIA Sites or External Sites	AGD
4b (ii) DUMP PACKAGE Ciphered format [DSK Secret Live Key]	INSI or IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited INSI or IDEMIA Sites or External Sites	AGD

Table 10 Platform package is loaded at Audited INSI or IDEMIA Sites or Non-Audited INSI or IDEMIA Sites or External Sites and Options and Applet package is loaded through Resident application using LSK format or DUMP Package in Ciphered format is loaded

(Option 4c) Applet loading in plain (unprotected) format using GP

CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table).

Here, there is a provision of loading the applet in plain format in Audited INSI or IDEMIA Sites **only,** on top of the platform already loaded by Audited INSI or IDEMIA Production Sites or Non-Audited INSI or IDEMIA Sites or External Sites. This applet loading in plain format is not allowed in Non-Audited INSI or IDEMIA Sites or External Sites.

TOE Delivery points:

- Here, since the loading of Applet package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Plain format in CC Audited INSI or IDEMIA Production Sites, so TOE delivery is considered at the end of Phase 4.

Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	INSI or IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited INSI or IDEMIA Sites or External Sites	AGD
CombICAO Applet v3 in Plain Format	INSI or IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC

Table 11 Option 4(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at CC Audited INSI Sites only

4.3 Preparation Environment

In this environment, the following two phases take place:

- Phase 5: Pre-personalisation of the applet
- Phase 6: Personalisation

The preparation environment may not necessarily take place in a manufacturing site, but may be performed anywhere. All along these two phases, the TOE is self-protected as it requires the authentication of the pre-personalisation agent or personalisation agent prior to any operation.

The CombICAO Applet v3 is pre-personalised and personalised according to [AGD_PRE].

These two phases are covered by [AGD_PRE] tasks of the TOE and Guidance tasks of [ST_PTF].

4.4 Operational Environment

Phase 7: Use Phase

The TOE is used as a travel document's chip by the traveller and the inspection systems in the "Operational Use" phase. The user data can be read according to the security policy of the issuing State or Organisation and can be used according to the security policy of the issuing State but they can never be modified for eMRTD application.
Note that applications can be loaded onto the ID-One Cosmo X platform during this phase.

During this phase, the TOE may be used as described in [AGD_OPE] of the TOE.

This phase is covered by [AGD_OPE] tasks of the TOE and Guidance tasks of [ST_PTF].

5 Conformance claims

5.1 Common Criteria Conformance Claim

This security target claims conformance to the Common Criteria version 3.1, revision 5 [CC2] and [CC3].

The conformance to the CC is claimed as follows:

CC	Conformance rationale
Part 2	Conformance with the extended[3] part: ▪ FCS_RND.1 "Quality metric for random numbers" ▪ FMT_LIM.1 "Limited capabilities" ▪ FMT_LIM.2 "Limited availability" ▪ FPT_EMS.1 "TOE Emanation" ▪ FIA_API.1[2] "Authentication Proof of Identity"
Part 3	Conformance to assurance package EAL 5, augmented with: ▪ AVA_VAN.5: "Advanced methodical vulnerability analysis" ▪ ALC_DVS.2: "Sufficiency of security measures" ▪ ALC_FLR.1: "Basic flaw remediation"

Table 12 Common Criteria conformance claim

Remark:

The Common Methodology for Information Technology Security Evaluation [CEM] has been taken into account.

5.2 Protection Profile Conformance Claim

This security target is strict compliant with the following PPs:

- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation" [PP-SSCD2].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 3: Device with key import" [PP-SSCD3].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 4: Extension for device with key generation and trusted communication with certificate generation application" [PP-SSCD4].

2 FIA_API.1 has been added to this security target for the needs of the Chip Authentication Protocol.

- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 5: Extension for device with key generation and trusted communication with signature creation application" [PP-SSCD5].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 6: Extension for device with key import and trusted communication with signature creation application" [PP-SSCD6].

5.3 Package Claim

The protection profiles require an assurance level of level EAL4 augmented with AVA_VAN.5. This security target considers an assurance level EAL5 augmented with AVA_VAN.5, ALC_FLR.1 and ALC_DVS.2, which still complies with the requirements of the protection profiles.

5.4 Conformance Rationale

[PP-SSCD4] and [PP-SSCD5] are strictly conforming to the core PP-SSCD2 [PP-SSCD2]. [PP-SSCD6] is strictly conforming to the core PP-SSCD3 [PP-SSCD3]. This ST is claimed to be conformant to the above mentioned PPs [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]. A detailed justification is given in the following:

1) The SPD of this ST contains the security problem definition [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]. The SPD for this ST is described by the same threats, organisational security policies and assumptions as for the TOE in the PPs.

2) The security objectives for the TOE in this ST include all the security objectives for the TOE of the core PPs [PP-SSCD2] and [PP-SSCD3] and add
   a. the security objectives OT.TOE_TC_VAD_Imp and OT.TOE_TC_DTBS_Imp from [PP-SSCD5] and [PP-SSCD6],
   b. the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp from [PP-SSCD4],

3) The assumptions in this ST include A.CSP from [PP-SSCD3] and [PP-SSCD6]. This assumption doesn't mitigate any threat and doesn't fulfil any OSP meant to be addressed by security objectives for the TOE in the other PPs.

4) The security objectives for the operational environment in this ST include all security objectives for the operational environment of the core PPs [PP-SSCD2] and [PP-SSCD3] except OE.HI_VAD, OE.DTBS_Protect and OE.SSCD_Prov_Service.
   - This ST adapts OE.HI_VAD and OE.DTBS_Protect to the support provided by the TOE by new security functionality (cf. OT.TOE_TC_VAD_Imp, OT.TOE_TC_DTBS_Imp) provided by the TOE and changes them into OE.HID_TC_VAD_Exp and OE.SCA_TC_DTBS_Exp ([PP-SSCD5] and [PP-SSCD6] for details).
   - OE.SSCD_Prov_Service is replaced by OE.Dev_Prov_Service from [PP-SCCD4].

   This ST also includes security objectives for the operational environment OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp from [PP-SSCD4]

5) The SFRs specified in this ST includes all security functional requirements (SFRs) specified in the core PPs [PP-SSCD2] and [PP-SSCD3]. Additional SFRs address :

a. trusted channel between the TOE and the SCA from [PP-SSCD5] and [PP-SSCD6]: FDP_UIT.1/DTBS, FTP_ITC.1/VAD and FTP_ITC.1/DTBS.
b. Trusted communication with CGA from [PP-SSCD4] : FIA_API.1 and FDP_DAU.2/SVD, FTP_ITC.1/SVD

6) This ST provides refinements for the SFR FIA_UAU.1 according to [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6].

7) The security assurance requirements (SARs) are originally taken from SARs of part 3 [CC3] according to the package conformance EAL 5 augmented with ALC_DVS.2, ALC_FLR.1 and AVA_VAN.5 (the Evaluation Assurance Level EAL5+ of the current ST exceeds the EAL4+ defined by [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]).

This security target is compliant with the SPD of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE SPDs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
Assumptions						
A.CGA	×		x	×		×
A.SCA	×		x	×		×
A.CSP		x			x	x
Threats						
T.SCD_Divulg	x	x	x	×	x	×
T.SCD_Derive	×	x	x	×	x	×
T.Hack_Phys	×	x	x	×	x	×
T.SVD_Forgery	×	x	x	×	x	×
T.SigF_Misuse	×	x	x	×	x	×
T.DTBS_Forgery	×	x	x	×	x	×
T.Sig_Forgery	×	x	x	×	x	×
Organisational Security Policies						

TOE SPDs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
P.CSP_QCert	×	x	x	×	x	×
P.QSign	×	x	x	×	x	×
P.Sigy_SSCD	×	x	x	×	x	×
P.Sig_Non-Repud	×	x	x	×	x	×

Table 13 PP SPDs vs. ST

This security target is compliant with the security objectives of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE Objectives	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
Objectives for the TOE						
OT.Lifecycle_Security	x	x	x	x	x	×
OT.SCD/SVD_Auth_Gen	x		x	x		×
OT.SCD_Unique	x		x	x		×
OT.SCD_SVD_Corresp	x		x	x		×
OT.SCD_Secrecy	x	x	x	x	x	×
OT.Sig_Secure	x	x	x	x	x	×
OT.Sigy_SigF	x	x	x	x	x	×
OT.DTBS_Integrity_TOE	x	x	x	x	x	×
OT.EMSEC_Design	x	x	x	x	x	×
OT.Tamper_ID	x	x	x	x	x	×
OT.Tamper_Resistance	x	x	x	x	x	×
OT.TOE_TC_VAD_Imp				×	x	×
OT.TOE_TC_DTBS_Imp				×	x	×
OT.TOE_SSCD_Auth			x			×
OT.TOE_TC_SVD_Exp			x			×
OT.SCD_Auth_Imp		x			x	x

Objectives for the Operational Environment						
OE.SVD_Auth	×	×	×	×	×	×
OE.CGA_QCert	×	×	×	×	×	×
OE.SSCD_Prov_Service	×	×		×	×	
OE.SCD/SVD_Auth_Gen		×			×	×
OE.SCD_Unique		×			×	×
OE.SCD_SVD_Corresp		×			×	×
OE.SCD_Secrecy		x			x	×
OE.HID_VAD	×	×	×			
OE.DTBS_Intend	×	×	×	×	x	×
OE.DTBS_Protect	×	×	×			
OE.Signatory	×	×	×	×	×	×
OE.HID_TC_VAD_Exp				×	×	×
OE.SCA_TC_DTBS_Exp				×	×	×
OE.Dev_Prov_Service			x			x
OE.CGA_SSCD_Auth			x			×
OE.CGA_TC_SVD_Imp			x			×

Table 14 PP Security Objectives vs. ST

This security target is compliant with the security functional requirements of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE SFRs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
FCS_CKM.1	×		×	×		×
FCS_CKM.4	×	×	×	×	×	×
FCS_COP.1	×	×	×	×	×	×
FDP_ACC.1/SCD/SVD_Generation	×		×	×		×
FDP_ACF.1/SCD/SVD_Generation	×		×	×		×
FDP_ACC.1/SVD_Transfer	×		×	×		×
FDP_ACF.1/SVD_Transfer	×		×	×		×
FDP_ACC.1/Signature_Creation	×	×	×	×	×	×
FDP_ACF.1/Signature_Creation	×	×	×	×	×	×
FDP_ACC.1/SCD_Import		×			×	×
FDP_ACF.1/SCD_Import		×			×	×
FDP_RIP.1	×	×	×	×	×	×
FDP_SDI.2/Persistent	×	×	×	×	×	×
FDP_SDI.2/DTBS	×	×	×	×	×	×

FIA_UID.1	×	×	×	×	×	×
FIA_UAU.1	×	×	×	×	×	×
FIA_AFL.1	×	×	×	×	×	×
FMT_SMR.1	×	×	×	×	×	×
FMT_SMF.1	×	×	×	×	×	×
FMT_MOF.1	×	×	×	×	×	×
FMT_MSA.1/Admin	×	×	×	×	×	×
FMT_MSA.1/Signatory	×	×	×	×	×	×
FMT_MSA.2	×	×	×	×	×	×
FMT_MSA.3	×	×	×	×	×	×
FMT_MSA.4	×	×	×	×	×	×
FMT_MTD.1/Admin	×	×	×	×	×	×
FMT_MTD.1/Signatory	×	×	×	×	×	×
FPT_EMS.1	×	×	×	×	×	×
FPT_FLS.1	×	×	×	×	×	×
FPT_PHP.1	×	×	×	×	×	×
FPT_PHP.3	×	×	×	×	×	×

FPT_TST.1	×	×	×	×	×	×
FIA_API.1			×			×
FTP_ITC.1/SVD			×			×
FDP_DAU.2/SVD			×			x
FDP_UIT.1/DTBS				×	×	×
FTP_ITC.1/VAD				×	×	×
FTP_ITC.1/DTBS				×	×	×
FDP_ITC.1/SCD		×				×
FDP_UCT.1/SCD		×				×
FTP_ITC.1/SCD		×				×
FCS_RNG.1						×

Table 15 PP SFRs vs. ST

8) The additional functionalities (PACE authentication, Chip Authentication Protocol Version 1 and Terminal Authentication Protocol Version 1) have been added to the TOE with: (i) additional security problem definition; (ii) additional security objectives; (iii) additional SFRs. All these additions are based on the [PP_EACwPACE].

   Notice that the added security objectives for the operational environment don't mitigate any threats of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] and don't fulfil any OSPs meant to be addressed by security objectives for the TOE in PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]. The objectives and SFRs related to the functionality are only valid in case the additional functionalities are configured for the TOE.

   The additions are mentioned in the below sections:

5.4.1 Additional Assets

The following additional Assets are identified:

- **Keys**
- **PIN/PUK**
- **VAD**
- **Session Keys**
- **Authenticity of the Electronic Documents Chip**
- **Tracing Data**
- **Sensitive User Data**

- **User Data stored on the TOE**
- **User Data transferred between the TOE and the Terminal**
- **Accessibility of TOE Functions and Data only for Authorized Subjects**
- **Genuineness of the TOE**
- **Electronic Document Communication Establishment Authorization Data**
- **Secret Document Holder Authentication Data**
- **TOE internal Non-Secret Cryptographic Material**

5.4.2 Additional Subjects

The following additional Subjects are identified:

- **Issuer Certification Authority (Issuer CA)**
- **Country Verifying Certification Authority (CVCA)**
- **eService Certification Authority**
- **Document Holder**
- **Electronic Document Presenter**
- **Basic Authentication Terminal (BAT)**
- **Authentication Terminal**
- **Administration Terminal**
- **Terminal**

5.4.3 Additional Threats

The following additional Threats are identified:

- **T.Key_Divulg**
- **T.Key_Derive**
- **T.TOE_PublicAuthKey_Forgery**
- **T.Authentication_Replay**
- **T.Counterfeit**
- **T.Sensitive_Data**
- **T.Abuse-Func**
- **T.Eavesdropping**
- **T.Forgery**
- **T.Information_Leakage**
- **T.Malfunction**
- **T.Phys-Tamper**
- **T.Skimming**
- **T.Tracing**
- **T.ADMIN_Configuration**
- **T.Key_Access**

5.4.4 Additional Organisational Security Policies

The following additional Organisational Security Policy is identified:

- **P.LinkSCD_QualifiedCertificate**
- **P.TOE_PublicAuthKey_Cert**
- **P.eServices**
- **P.EAC_Terminal**
- **P.Terminal_PKI**
- **P.Card_PKI**

- **P.Pre-Operational**
- **P.Terminal**
- **P.Trustworthy_PKI**
- **P.Manufact**

5.4.5 Additional Security Objectives

The following additional Security Objectives of the TOE are identified:

- **OT.Identification**
- **OT.Authentication_Secure**
- **OT.Key_Lifecycle_Security**
- **OT.Keys_Secrecy**
- **OT.TOE_AuthKey_Unique**
- **OT.Lifecycle_Management**
- **OT.eServices**
- **OT.AC_Pers_EAC**
- **OT.Tracing**
- **OT.ADMIN_Configuration**
- **OT.Key_Usage_Counter**

5.4.6 Additional Security Objectives for the Operational Environment

The following additional Security Objectives of the Operational Environment are identified:

- **OE.LinkSCD_QualifiedCertificate**
- **OE.AuthKey_Transfer**
- **OE.AuthKey_Unique**
- **OE.TOE_PublicKeyAuth_Transfer**
- **OE.Terminal_Authentication**
- **OE.Legislative_Compliance**
- **OE.Passive_Auth_Sign**
- **OE.Personalization**
- **OE.Terminal**
- **OE.Electronic_Document_Holder**

5.4.7 Additional Security Functional Requirements

The following additional Security Functional Requirements are identified:

- **FCS_RND.1**
- **FCS_CKM.1/DH_PACE**
- **FCS_CKM.1/Session Keys**
- **FCS_COP.1/GP Secret Data Protection**
- **FCS_COP.1/SM in Confidentiality**
- **FCS_COP.1/SM in Integrity**
- **FCS_COP.1/Digital Auth**
- **FCS_COP.1/Enc Key Decipherment**
- **FCS_COP.1/SIG_VER**
- **FDP_ACC.1/TRM**
- **FDP_ACF.1/TRM**
- **FDP_ACC.1/MNG_File**
- **FDP_ACF.1/MNG_File**

- **FDP_UCT.1/TRM**
- **FDP_UIT.1/TRM**
- **FIA_UID.1/PACE**
- **FIA_UAU.1/PACE**
- **FIA_UAU.4/PACE**
- **FIA_UAU.5/PACE**
- **FIA_UAU.6/PACE**
- **FIA_UAU.6/EAC**
- **FIA_AFL.1/AUTH**
- **FIA_API.1/TOE Authentication**
- **FMT_SMR.1/PACE**
- **FMT_MTD.1/CVCA_INI**
- **FMT_MTD.1/CVCA_UPD**
- **FMT_MTD.1/DATE**
- **FMT_MTD.1/CAPK**
- **FMT_MTD.1/KEY_READ**
- **FMT_MTD.1/Key_Usage_Counter**
- **FMT_MTD.1/Initialize_PIN**
- **FMT_MTD.1/Resume_PIN**
- **FMT_MTD.1/Change_PIN**
- **FMT_MTD.1/Unblock_PIN**
- **FMT_MTD.1/UnblockChange_RAD**
- **FMT_MTD.1/Erase_PIN**
- **FMT_MTD.1/Reinitialize_PIN**
- **FMT_MTD.1/UnblockChange_PUK**
- **FMT_MTD.1/TOE State**
- **FMT_MTD.3**
- **FMT_LIM.1**
- **FMT_LIM.2**
- **FPT_EMS.1/PIN-PUK-KEYS**
- **FTP_ITC.1/PACE**

6 Security Problem Definition

6.1 Assets

6.1.1 Assets from Protection Profiles

SCD

Signature Creation Data

Private key used to perform an electronic signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD shall be maintained.

SVD

Signature Verification Data

Public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported shall be maintained.

DTBS/R

Data to be signed or its unique Representation

Set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature shall be maintained.

6.1.2 Additional Assets

Keys

- Private or secret key(s) used to (1) authenticate an external user or entity, (2) perform authentication protocols, (3) perform digital authentication, (4) perform digital signature or (5) perform encryption key decipherment. Their integrity and confidentiality must be maintained.
- Public key(s) used as trust anchor to verify a certificate chain used in terminal authentication. Their integrity must be maintained.

PIN/PUK

The applet manages two types of PINs (PINSig called also RAD and PINAuth) for user authentication and one PUK for management purpose. They are used to authenticate natural persons. The PINs and PUK must be created and initialized first before they can be used for authentication. Furthermore, PINAuth can only be an Code PIN.

VAD

PIN code entered by the end user to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)

Session Keys

Keys computed for secure messaging and used to ensure confidentiality, authenticity and integrity of data.

Authenticity of the Electronic Documents Chip

The authenticity of the electronic document's chip, personalized by the issuing organization for the Document holder, is used by the electronic document presenter to prove his possession of a genuine electronic document.

Tracing Data

Technical information about the current and previous locations of the electronic document gathered unnoticeable by the Document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.

Sensitive User Data

User data, which have been classified as sensitive data by the electronic document issuer. Sensitive user data are a subset of all user data, and are protected by EAC.

User Data stored on the TOE

All data, with the exception of authentication data, that are stored in the context of the application(s) on the electronic document. These data are allowed to be accessed either by a BAT, or, in the case of sensitive data, by an Authentication Terminal with appropriate authorization level.

User Data transferred between the TOE and the Terminal

All data, with the exception of authentication data, that are transferred (both directions) during usage of the application(s) of the electronic document between the TOE and authenticated terminals.

Accessibility of TOE Functions and Data only for Authorized Subjects

Property of the TOE to restrict access to TSF and TSF-Data stored in the TOE to authorized subjects only.

Genuineness of the TOE

Property of the TOE to be authentic in order to provide claimed security functionality in a proper way.

Electronic Document Communication Establishment Authorization Data

Restricted-revealable authorization information for a human user used for verification of the authorization attempts as an authorized user (PACE password). These data are stored in the TOE and not send to it. Restricted-revealable here refers to the fact that if necessary, the Document holder may reveal her verification values of CAN and MRZ to an authorized person, or to a device that acts according to respective regulations and is considered trustworthy.

Secret Document Holder Authentication Data

Secret authentication information for the Document holder being used for verification of the authentication attempts as authorized Document holder (sent PACE passwords, e.g. PIN, PUK, MRZ or CAN).

TOE internal Non-Secret Cryptographic Material

Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material used by the TOE in order to enforce its security functionality.

6.2 Users / Subjects

6.2.1 Subjects from Protection Profiles

User

End user of the TOE who can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

Administrator

User who is in charge to perform the TOE initialization, TOE (pre-)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.

Application Note:

For all activities related to Personalization, the subject Administrator is also called Personalization Agent in the rest of the document.

For all activities related to Use Phase, the subject Administrator has following roles as defined below:

- Manage symmetric authentication using Administration Agent keys,
- Configure the size or value of the Chip Authentication key to be modified in USE phase,
- Change the key parameters during the key generation process,
- Read that Proof that a key has been on board generated,
- Create or Delete Files in Use Phase,
- Invalidate one of the Chip Authentication key in USE phase and to set the secondary key as being the primary key
- Unblock and Change the PUK
- Unblock and Change the PINSig
- Generate keypair Chip Authentication Key
- Generate keypair SCD/SVD

Signatory

User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

6.2.2 Threat agents

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.

6.2.3 Additional Subjects

Issuer Certification Authority (Issuer CA)

An organization enforcing the policy of the electronic document issuer, i. e. confirming correctness of user and TSF data that are stored within the electronic document. The Issuer CA represents both the (1) root and (2) intermediate sub-CAs of the public key infrastructure (PKI) used to issue the electronic document. The Issuer CA signs user and TSF data to create a digital seals that is stored in the electronic document to demonstrate their integrity and authenticity.

Country Verifying Certification Authority (CVCA)

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing state or organization, i. e. enforcing protection of sensitive user data that are stored in the electronic document. The CVCA represents the country specific root of the PKI of Authentication Terminals and eServices certification authorities, and creates eServices certification authorities certificates within this PKI. Updates of the public key of the CVCA are distributed as CVCA Link-Certificates, see [TR-03110-3].

eService Certification Authority

An organization issuing terminal certificates. The eService certification authority is a certificate authority, authorized by the corresponding CVCA to issue certificates for Authentication Terminals.

Document Holder

A person who the electronic document issuer has personalized the electronic document for. Personalization here refers to associating a person uniquely with a specific electronic document. Note that an Document holder can also be an attacker. The document holder is equivalent to the signatory and can use and manage the PINSig (called also the RAD), the PINAuth and the PUK.

Electronic Document Presenter

A person presenting the electronic document to a terminal and claiming the identity of the Document holder. Note that an electronic document presenter can also be an attacker.

Basic Authentication Terminal (BAT)

A BAT implements the terminal part of the PACE protocol and/or the VERIFY PIN command and authenticates itself to the electronic document using a shared password (CAN, MRZ, PIN, PUK). A BAT is not allowed to access sensitive user data.

Authentication Terminal

A terminal that has successfully passed Terminal Authentication is an Authentication Terminal. It is authorized by the electronic document issuer through the eServices certification authorities of the receiving branch (by issuing terminal certificates) to access a subset or all of the data stored on the electronic document.

Administration Terminal

A terminal that has successfully performed GP Authentication in phase 7 is an Administration Terminal. This terminal is linked to Administrator role in Use phase (phase 7).

Terminal

A terminal is any technical system communicating with the TOE through the contactless or contact-based interface. The role terminal is the default role for any terminal being recognized by the TOE that is neither a BAT nor an Authentication Terminal nor an Administration Terminal.

6.3 Threats

6.3.1 Threats drawn from the Protection Profiles

T.SCD_Divulg

Storing, copying and releasing of the signature creation data

An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature creation in the TOE.

T.SCD_Derive

Derive the signature creation data

An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

T.Hack_Phys

Physical attacks through the TOE interfaces

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

T.SVD_Forgery

Forgery of the signature verification data

An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

T.SigF_Misuse

Misuse of the signature creation function of the TOE

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

T.DTBS_Forgery

Forgery of the DTBS/R

An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign.

T.Sig_Forgery

Forgery of the electronic signature

An attacker forges a signed data object, maybe using an electronic signature that has been 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 created 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.

6.3.2 Additional Threats

T.Key_Divulg

Storing, copying, and releasing of a key stored in the TOE

An attacker can store and copy a key (other than SCD) stored in the TOE outside the TOE. An attacker can release a key during generation, storage and use in the TOE.

T.Key_Derive

Derive a key

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

T.TOE_PublicAuthKey_Forgery

Forgery of the public key of a TOE authentication key

An attacker forges the public key of a TOE authentication key presented by the TOE. This results in loss of the public key integrity in the authentication certificate of the TOE.

T.Authentication_Replay

Replay of an authentication of an external entity

An attacker retrieves by observation authentication data used by a third party during an authentication sequence. The attacker tries to replay this authentication sequence to grant access to the TOE.

T.Counterfeit

An attacker with high attack potential produces an unauthorized copy or reproduction of a chip of a genuine electronic document. This copy or reproduction can be used as a part of a counterfeit electronic document. This violates the authenticity of the electronic document's chip used for authentication of an electronic document presenter by possession of an electronic document. The attacker may generate a new data set or extract completely or partially the data from a genuine electronic document's chip and copy them to another appropriate chip to imitate the chip of the genuine electronic document.

Threat agent: having high attack potential, being in possession of one or more legitimate ID-Cards

T.Sensitive_Data

An attacker tries to gain access to sensitive user data through the communication interface (contact or contactless) of the electronic document's chip. The attack T.Sensitive_Data is similar to the threat T.Skimming from [PACEPP] w.r.t. the attack path (communication interface) and the motivation (to get data stored on the electronic document's chip) but differs from those in the asset under the attack, the opportunity (i.e. knowing the PACE Password or the PIN) and therefore the possible attack methods.

Threat agent: having high attack potential, knowing the PACE Password or the PIN, being in possession of a legitimate electronic document

T.Abuse-Func

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialization and Personalization in the operational phase after delivery to the holder.

T.Eavesdropping

An attacker is listening to the contactless communication between the electronic document and the BAT in order to gain the user data transferred between the TOE and the terminal connected.

T.Forgery

An attacker fraudulently alters the User Data or/and TSF-data stored on the electronic document or/and exchanged between the TOE and the terminal connected in order to outsmart the BAT by means of changed electronic document holder's related reference data. The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

T.Information_Leakage

An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the electronic document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

T.Malfunction

An attacker may cause a malfunction the electronic document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the electronic document outside the normal operating conditions, exploiting errors in the electronic document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

T.Phys-Tamper

An attacker may perform physical probing of the electronic document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the electronic document in order to alter (i) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the travel document.

T.Skimming

An attacker imitates a terminal in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless interface of the TOE.

T.Tracing

An attacker tries to gather TOE tracing data (i.e. to trace the movement of the electronic document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE.

T.ADMIN_Configuration

Adverse action: An attacker may access to the TOE at user phase (phase 7) to try to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the eDigitalIdentity document's embedded software or (iii) Create or Delete EF files without properly authenticating as Administrator.

Threat agent: having high attack potential, being in possession of one or more legitimate eDigitalIdentity document in Operational use phase.

Asset: authenticity of logical eDigitalIdentity document data and Accessibility of TOE Functions and Data only for Authorized Subjects

T.Key_Access

Adverse action: An attacker may access to the internal secret cryptographic keys of the TOE.

Threat agent: having high attack potential, knowing the key values, being in possession of a legitimate eDigitalIdentity document.

Asset: TOE internal secret cryptographic keys

6.4 Organizational Security Policies

6.4.1 Security Policies drawn from the Protection Profiles

P.CSP_QCert

Qualified certificate

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. previous [Directive], Article 2, clause 10 or new [eIDAS_Regulation], Article 3, clause 15) for the SVD generated by the SSCD. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

P.QSign

Qualified electronic signatures

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. the [Directive], Article 2, clause 2 or new [eIDAS_Regulation], Article 3, clause 11), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the [Directive], Article 2, clause 10 or new [eIDAS_Regulation], Article 3, clause 15). The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable

P.Sigy_SSCD

TOE as secure signature creation device

The TOE meets the requirements for an SSCD laid down in (Article 2, clause 6 of the [Directive] or new [eIDAS_Regulation], Article 3, clause 22/23). This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

P.Sig_Non-Repud

Non-repudiation of signatures

The lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

6.4.2 Additional Security Policies

P.LinkSCD_QualifiedCertificate

Link between a SCD stored in the TOE and the relevant qualified certificate

The Role in charge of creating and updating the SCD (Personalization Agent, R.Admin), or the trusted IT entity involved in the updating process (CSP) shall ensure an unambiguous link between the (qualified) certificate(s) and the corresponding SCD(s). This link might be figured out by a PKCS#15 structure, an XML structure, an identifier.linking the file

containing the (qualified) certificate or the URL hosting them to the SCD(s) stored in the TOE. In particular, it implies this link is updated, each time the SCD(s) is created, imported, erased or generated.

P.TOE_PublicAuthKey_Cert

Certificate for asymmetric TOE authentication keys

The TOE contains certificate(s) issued by a known entity ensuring its public key corresponding to the authentication private key is genuine.

P.eServices

Provision of eServices

The TOE provides the following mechanisms:

- decrypt encryption decipherment keys using asymmetric mechanisms;
- digital authentication: authentication of the TOE (on behalf of the TOE holder) using an asymmetric private key;

Moreover, the TOE ensures these keys remain genuine by enforcing an access control over the update of these keys, in order to ensure that only entitled entities can change them.

P.EAC_Terminal

Terminals that intent to be Authentication Terminals must implement the respective terminal part of the protocols required to execute EAC protocol, and store (static keys) or generate (temporary keys and nonces) the corresponding credentials.

P.Terminal_PKI

The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer.

P.Card_PKI

The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

- The electronic document Issuer shall establish a public key infrastructure to ensure the integrity and authenticity of the content of the electronic document, through the generation of digital seals protecting the data it contains. For this aim, it runs an Issuer CA.
- The Issuer CA shall securely generate, store and use the Issuer CA key pair. The Issuer CA shall keep the Issuer CA Private Key secret.

P.Pre-Operational

- The electronic document Issuer issues the electronic document and approves it using the terminals complying with all applicable laws and regulations.
- The electronic l document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE.
- The electronic document Issuer uses only such TOE's technical components (IC) which enable traceability of the electronic documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase,
- If the electronic document Issuer authorizes a Personalization Agent to personalize the electronic document for electronic document holders, the electronic document Issuer has to ensure that the Personalization Agent acts in accordance with the electronic document Issuer's policy.

P.Terminal

The BAT shall operate their terminals as follows:

- The related terminals shall be used by terminal operators and by electronic document holders.
- They shall implement the terminal parts of the PACE protocol and check the digital seal generated by the Issuer CA included in the electronic document and protecting its content. The BAT shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
- They shall also securely store the Issuer CA certificate in order to be able to verify the digital seals generated by the Issuer CA and included in the electronic document to protect its content (integrity and authenticity of the data stored in the electronic document).
- The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords or the PIN, integrity of PKI certificates, etc.).

P.Trustworthy_PKI

The Issuer CA shall ensure that it issues its certificates exclusively to the rightful organizations and that they create exclusively correct digital seals to be stored on the electronic document.

P.Manufact

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The electronic document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.

6.5 Assumptions

6.5.1 All SSCD parts

A.CGA

Trustworthy certificate generation application

The CGA protects the authenticity of the signatory's name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

A.SCA

Trustworthy signature creation application

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of data the signatory wishes to sign in a form appropriate for signing by the TOE.

6.5.2 Parts 3 and 6 only

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 authorised 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.

7 Security Objectives

7.1 Security Objectives for the TOE

7.1.1 All SSCD parts

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 the signatory.

OT.SCD_Secrecy

Secrecy of the signature creation data

The secrecy of the SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential.

OT.Sig_Secure

Cryptographic security of the electronic signature

The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.Sigy_SigF

Signature creation function for the legitimate signatory only

The TOE shall provide the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

OT.DTBS_Integrity_TOE

DTBS/R integrity inside the TOE

The TOE shall not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation.

OT.EMSEC_Design

Provide physical emanations security

The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

OT.Tamper_ID

Tamper detection

The TOE shall provide system features that detect physical tampering of its components, and uses those features to limit security breaches.

OT.Tamper_Resistance

Tamper resistance

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

7.1.2 SSCD parts 2, 4 and 5 only

OT.SCD/SVD_Auth_Gen

Authorised SCD/SVD generation

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

OT.SCD_Unique

Uniqueness of the signature creation data

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation shall practically occur only once and shall not be reconstructable from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible.

OT.SCD_SVD_Corresp

Correspondence between SVD and SCD

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD.

7.1.3 SSCD parts 3 and 6 only

OT.SCD_Auth_Imp

Authorised SCD import

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

7.1.4 SSCD part 4 only

OT.TOE_SSCD_Auth

Authentication proof as SSCD

The TOE shall hold unique identity and authentication data as SSCD and provide security mechanisms to identify and to authenticate itself as SSCD.

OT.TOE_TC_SVD_Exp

TOE trusted channel for SVD export

The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the TOE.

7.1.5 SSCD parts 5 and 6 only

OT.TOE_TC_VAD_Imp

Trusted channel of TOE for VAD import

The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed.

Application Note:

This security objective for the TOE is partly covering OE.HID_VAD from the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.HID_VAD in the core PP requires only the operational environment to protect VAD, this ST 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 this ST re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

OT.TOE_TC_DTBS_Imp

Trusted channel of TOE for DTBS import

The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE shall not generate electronic signatures with the SCD for altered DTBS.

7.1.6 Additional Security Objectives for the TOE

OT.Identification

Identification of the TOE

The TOE must provide means to store Initialisation36 and Pre-Personalisation Data in its non volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the electronic document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

OT.Authentication_Secure

Secure authentication mechanisms

The TOE provides strong mechanism to authenticate external users/entity and mechanisms to establish a strong trusted channel with an external IT entity. The authentication protocols rely on cryptographic schemes that are based on either symmetric or asymmetric cryptography. The TOE uses freshly generated random number in the authentication mechanism in order to avoid replay attacks. The authentication protocols ensure that the cryptogram cannot be forged without the knowledge of the authentication key, and that they cannot be reconstructed from the authentication cryptograms. The trusted channel

ensures integrity, authenticity, and confidentiality of the data using strong encryption techniques. The trusted channel ensures protection against deletion, and modification of commands. Moreover, the TOE ensures the key its uses are genuine by enforcing an access control over the authentication keys update, in order to ensure that only entitled entities can change key values.These mechanisms provided by the electronic document's chip are protected against attacks with high attack potential.

Note: The natural person may authenticate itself to the TOE via the VERIFY PIN command.

Protection against Abuse of Functionality:

The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

Protection against Information Leakage:

The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

Protection against Malfunctions:

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature. The following TOE security objectives address the aspects of identified threats to be countered involving TOE's environment.

Protection against Physical Tampering:

The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the electronic document's Embedded Software by means of

- measuring through galvanic contacts representing a direct physical probing on the chip's surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis),
- manipulation of the hardware and its security functionality, as well as
- controlled manipulation of memory contents (User Data, TSF-data)with a prior
- reverse-engineering to understand the design and its properties and functionality.

OT.Key_Lifecycle_Security

Life cycle security of the keys stored in the TOE

The TOE shall detect flaws during the initialization, Personalization and operational usage. The TOE shall provide safe destruction techniques for the keys (other than the SCD) it stores in case of erasure, re-import or re-generation.

OT.Keys_Secrecy

Secrecy of Keys

The secrecy of the keys (other than the SCD) stored in the TOE is reasonably assured against attacks with a high attack potential.

OT.TOE_AuthKey_Unique

Uniqueness of the TOE authentication key(s)

The TOE shall ensure the cryptographic quality of the asymmetric authentication key pair used for the TOE authentication. The private key used for TOE authentication can practically occur only once and cannot be reconstructed from the public key. In that context 'practically occur once' means that the probability of equal TOE authentication key is negligible low.

OT.Lifecycle_Management

Management of the life cycle

The TOE provides a life cycle management enabling to separate its life cycle in two main phases. The first one (phase 6) is the one during which the TOE is under the sole control of the Personalization Agent. The following operation may be realized:

- The SCD, SVD and keys may be created, generated, imported or erased
- The PINs/PUK (s) may be created and loaded
- SVD and public keys may be exported Once performed, the Personalization Agent switches the TOE in phase 7. This transition is irreversible leaving the TOE under the sole control of the R.Sigy and R.Admin according to the TOE specification and security rules set by the Personalization Agent.

OT.eServices

Provision of eServices

The TOE provides the following mechanisms:

- decrypt encryption decipherment keys using asymmetric mechanisms;
- digital authentication: authentication of the TOE (on behalf of the TOE holder) using an asymmetric private key;

Moreover, the TOE ensures these keys remain genuine by enforcing an access control over the update of these keys, in order to ensure that only entitled entities can change them.

These mechanisms provided by the electronic document's chip are protected against attacks with high attack potential.

OT.AC_Pers_EAC

Personalization of the Electronic Document

The TOE must ensure that user data and TSF-Data that are permanently stored in the TOE can be written by authorized personalization agents only, with the following exception: an Authentication Terminal may also write or modify user data according to its effective authorization. The effective authorization is determined by the electronic document during Terminal Authentication.

OT.Tracing

Tracing electronic document

The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the electronic document remotely through establishing or listening to a communication via the contactless interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

OT.ADMIN_Configuration

Protection of the TOE administration

In user phase, the TOE must ensure the administration actions are only authorized for Administrator. The TOE must control the access to its sensitive information and its functions and must provide the means to secure exchanges using cryptographic functions. The TOE must also ensure that any subject who is being authenticated as Administrator is only allowed Create or Delete Files in Use Phase.

OT.Key_Usage_Counter

Configuration of Key Usage Counter

The TOE must protect the key usage through OT.Key_Usage_Counter that support a Key Usage Counter which should be decremented by one each time the key is used. Once the counter is depleted, the key should become unusable.

7.2 Security Objectives for the Operational Environment

7.2.1 All SSCD parts

OE.SVD_Auth

Authenticity of the SVD The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

OE.CGA_QCert

Generation of qualified certificates

The CGA shall generate a qualified certificate that includes (amongst others): a the name of the signatory controlling the TOE; b the SVD matching the SCD stored in the TOE and being under sole control of the signatory; c the advanced signature of the CSP.

The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a SSCD.

OE.DTBS_Intend

SCA sends data intended to be signed

The signatory shall use a trustworthy SCA that:

- generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE;
- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE;

- attaches the signature produced by the TOE to the data or provides it separately.

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.

7.2.2 SSCD parts 2, 3 and 4 only

OE.HID_VAD

Protection of the VAD

If an external device provides the human interface for user authentication, this device shall ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface. In particular, if the TOE requires a trusted channel for import of the VAD, the HID shall support usage of this trusted channel.

OE.DTBS_Protect

SCA protects the data intended to be signed

The operational environment shall ensure that the DTBS/R cannot be altered in transit between the SCA and the TOE. In particular, if the TOE requires a trusted channel for import of the DTBS/R, the SCA shall support usage of this trusted channel.

7.2.3 SSCD parts 2, 3, 5 and 6 only

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.

7.2.4 SSCD parts 3 and 6 only

OE.SCD/SVD_Auth_Gen

Authorised SCD/SVD generation

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

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.

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.

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 sent to the CGA and the SCD exported to the TOE of the signatory identified in the SVD certificate.

7.2.5 SSCD part 4 only

OE.Dev_Prov_Service

Authentic SSCD provided by SSCD Provisioning Service

The SSCD Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, personalizes the TOE for the legitimate user as signatory, links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the signatory.

OE.CGA_TC_SVD_Imp

CGA trusted channel for SVD import

The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the SSCD.

OE.CGA_SSCD_Auth

Pre-initialization of the TOE for SSCD authentication

The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSCD, successfully proved this identity as SSCD to the CGA, and whether this identity is linked to the legitimate holder of the device as applicant for the certificate.

7.2.6 SSCD parts 5 and 6 only

OE.HID_TC_VAD_Exp

Trusted channel of HID for VAD export

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.

Application Note:

This security objective for the TOE is partly covering OE.HID_VAD from the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.HID_VAD in the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI) requires only the operational environment to protect VAD, this

ST 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 this ST 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.

OE.SCA_TC_DTBS_Exp

Trusted channel of SCA for DTBS export

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

Application Note:

This security objective for the TOE is partly covering OE.DTBS_Protect from the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.DTBS_Protect in the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI) requires only the operational environment to protect DTBS, this ST 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 this ST 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.

7.2.7 Additional Security Objectives for the Operational Environment

OE.LinkSCD_QualifiedCertificate

Link between SCD stored in the TOE and the relevant qualified certificate

The Role in charge of creating and updating the SCD (Personalization Agent, R.Admin), or the trusted IT entity involved in the updating process (CSP) shall ensure an unambiguous link between the (qualified) certificate(s) and the corresponding SCD(s). This link might be figured out by a PKCS#15 structure, an XML structure, an identifier linking the file containing the (qualified) certificate or the URL hosting them to the SCD(s) stored in the TOE. In particular, it implies this link is updated, each time the SCD(s) is created, imported, erased or generated.

OE.AuthKey_Transfer

Secure transfer of authentication key(s) to the TOE

The entity in charge of generating the authentication keys to be loaded in the TOE shall ensure the confidentiality of the key(s) transferred to the TOE.

OE.AuthKey_Unique

Uniqueness of the authentication key(s)

The entity in charge of generating the authentication keys to be loaded in the TOE shall ensure the cryptographic quality of the authentication key(s). The authentication key used for authentication can practically occur only once and, in case of a TOE authentication key

cannot be reconstructed from its public portion. In that context 'practically occur once' means that the probability of equal keys is negligible low.

OE.TOE_PublicKeyAuth_Transfer

Secure transfer of public authentication key(s) of the TOE

The entity in charge of generating the authentication certificate from the TOE's authentication public key generated in the TOE shall ensure the authenticity of this data when transferred from the TOE. This may be achieved through operational measures.

OE.Terminal_Authentication

AuthenticationKey pairs needed for Terminal Authentication

The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer.

OE.Legislative_Compliance

Issuing of the electronic document

The electronic document Issuer must issue the electronic document and approve it using the terminals complying with all applicable laws and regulations.

OE.Passive_Auth_Sign

Authentication of electronic document by Signature

The electronic document Issuer has to establish the necessary public key infrastructure as follows: the Issuer CA acting on behalf and according to the policy of the electronic document Issuer must (i) generate a cryptographically secure Issuer CA Key Pair, (ii) ensure the secrecy of the Issuer CA Private Key and issue certificate for its Sub-CA in a secure operational environment (if needed), and (iii) publish its certificate. Hereby authenticity and integrity of these certificates are being maintained. An Issuer CA acting in accordance with the Issuer CA policy must generate digital seals protecting the content of electronic document in a secure operational environment only.

The Issuer CA must issue its certificates exclusively to the rightful organizations (and must sign exclusively correct digital seals to be stored on electronic document).

OE.Personalization

Personalization of electronic document

The electronic document Issuer must ensure that the Personalization Agents acting on his behalf (i) store the corresponding data in the electronic document (electronic Personalization) for the electronic document holder, (ii) write the document details data, (iii) write the initial TSF data, (iv) sign the digital seal protecting the content of the electronic document.

OE.Terminal

Terminal operating

The terminal operators must operate their terminals as follows:

- The related terminals are used by terminal operators and by electronic document holders.
- The related terminals implement the terminal parts of the PACE protocol and check the digital seal generated by the Issuer CA included in the electronic document and protecting its content. The BAT shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
- The related terminals securely store the Issuer CA certificate in order to be able to verify the digital seals generated by the Issuer CA and included in the electronic document to protect its content (integrity and authenticity of the data stored in the electronic document).
- The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords or the PIN, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE.

OE.Electronic_Document_Holder

Electronic document holder Obligations

The electronic document holder may reveal, if necessary, his or her verification values of the PACE password or the PIN to an authorized person or device who definitely act according to respective regulations and are trustworthy.

7.3 Security Objectives Rationale

7.3.1 Threats

7.3.1.1 Threats drawn from the Protection Profiles

T.SCD_Divulg addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the [Directive], bullet (18). 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 authorised SCD generation in the environment is possible, and OT.SCD_Auth_Imp, which ensures that only authorised SCD import is possible.

T.SCD_Derive 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.

- OT.SCD/SVD_Auth_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD pair.

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

T.Hack_Phys 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 resisting tampering attacks. OT.Keys_Secrecy preserves the secrecy of all the authentication and eServices keys stored in the TOE.

T.SVD_Forgery deals with the forgery of the SVD exported by the TOE to the CGA for certificate generation. T.SVD_Forgery is addressed by

- OT.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and
- OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA.
- OE.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD.
- Additionally T.SVD_Forgery is addressed by OT.TOE_TC_SVD_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA_TC_SVD_Imp, which provides verification of SVD authenticity by the CGA.

T.SigF_Misuse 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 by ([Directive], Annex III, paragraph 1, bullet (c) or new [eIDAS_Regulation], Article 26, bullet (a)). OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialization, personalization 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 and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and 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_VAD (Protection of the VAD) provides confidentiality and integrity of the VAD as needed by the authentication method employed. OE.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 ensures also that the signatory keeps their VAD confidential. OT.Lifecycle_Management ensures that when the TOE is under the Personalization Agent control, it cannot be misused to sign on behalf of the legitimate Signatory.

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 from the SCA to 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).

T.DTBS_Forgery addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment 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, and by means of OE.DTBS_Protect, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R inside the TOE.

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.

T.Sig_Forgery deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique and OE.CGA_QCert address this threat in general. OT.Sig_Secure (Cryptographic security of the electronic signature) ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. OT.SCD_Unique 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. 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.

7.3.1.2 Additional Threats

T.Key_Divulg addresses the threat against the (1) authentication key of the TOE, (2) the authentication keys of entities and (3) the eServices keys stored in the TOE due to storage and copying of key(s) outside the TOE. This threat is countered by OT.Keys_Secrecy which assures the secrecy of the keys stored and used by the TOE. OE.AuthKey_Transfer ensures the confidentiality of the authentication keys transferred to the TOE. OT.Key_Lifecycle_Security (Lifecycle security) ensures the secrecy of the keys stored in the TOE during the whole life of the TOE.

T.Key_Derive deals with attacks on authentication and eServices keys via public known data produced or received by the TOE (public key, authentication cryptogram,…). This threat is countered by OE.AuthKey_Unique (in case of import) and OT.TOE_AuthKey_Unique (in case

of TOE's authentication key generation) that provides cryptographic secure generation of the keys. OT.Authentication_Secure ensures secure authentication cryptograms.

T.TOE_PublicAuthKey_Forgery deals with the forgery of the TOE's public key used for authentication exported by the TOE to an entitled entity for the generation of the certificate. This is addressed by OE.TOE_PublicKeyAuth_Transfer which ensures the authenticity of the TOE's public key for authentication.

T.Authentication_Replay deals with the threats when an attacker retrieves an authentication cryptogram presented to the TOE by an entity and presents it again to the TOE in order to grant some rights and gain access to some data on the TOE. This threat is addressed by OT.Authentication_Secure that ensures the authentication cryptogram can not be replayed as they rely on random data internally generated by the TOE.

T.Counterfeit addresses the attack of an unauthorized copy or reproduction of the genuine electronic document. This attack is countered by the proof of the chip's authenticity, as aimed by OT.Authentication_Secure using a Chip Authentication key pair that is generated within the issuing PKI branch, as aimed by OE.AuthKey_Transfer, OE.AuthKey_Unique, OE.TOE_PublicKeyAuth_Transfer.

T.Sensitive_Data is countered by the TOE-Objective OT.Authentication_Secure, that requires that read access to sensitive user data is only granted to Authentication Terminals with corresponding access rights. Furthermore, it is required that the confidentiality of the data is ensured during contactless transmission. The objective OE.Terminal_Authentication requires the electronic document issuer to provide the public key infrastructure (PKI) to generate and distribute the card verifiable certificates needed by the electronic document to securely authenticate the Authentication Terminal.

T.Abuse-Func addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the soft-coded security functionality. The security objective OT.Authentication_Secure ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

T.Eavesdropping addresses listening to the contactless communication between the TOE and a BAT or an Authentication Terminal in order to gain access to transferred user data. This threat is countered by the security objective OT.Authentication_Secure through a trusted channel based on PACE or EAC Authentication

T.Forgery addresses the fraudulent, complete or partial alteration of user data and/or TSF-Data stored on the TOE, and/or exchanged between the TOE and the terminal. The threat T.Forgery addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. The security objective OT.AC_Pers_EAC requires the TOE to limit the write access for the travel document to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objective OT.Authentication_Secure. This objective contribute also to protecting integrity of the User Data or/and TSF-data stored on the TOE. A terminal

operator operating his terminals according to OE.Terminal and performing the digital seal verification as aimed by OE.Passive_Auth_Sign will be able to effectively verify integrity and authenticity of the data received from the TOE.

T.Information_Leakage is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Authentication_Secure.

T.Malfunction is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Authentication_Secure.

T.Phys-Tamper is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Authentication_Secure.

T.Skimming addresses accessing the user data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless interface. This threat is countered by the security objective OT.Authentication_Secure through the PACE authentication. The objective OE.Electronic_Document_Holder ensures that a PACE session can only be established either by the travel document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker. Additionally, the threat is also addressed by OT.Authentication_Secure that demands a trusted channel based on Chip Authentication, and requires that read access to sensitive user data is only granted to Authentication Terminals with corresponding access rights. Moreover, OE.Terminal_Authentication requires the electronic document issuer to provide the corresponding PKI.

T.Tracing addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE, whereby the attacker does not a priori know the correct values of the PACE password. This threat is directly countered by security objectives OT.Tracing (no gathering TOE tracing data) and OE.Electronic_Document_Holder (the attacker does not a priori know the correct values of the shared passwords).

T.ADMIN_Configuration The threat T.ADMIN_Configuration "Tampering attempt of the TOE during administration" addresses attacks in Operational use phase. The attacker trying to access to unauthorized TOE functions, trying to access or to modify sensitive information exchanged between the TOE and the Administartion system or trying to Create or Delete EF files in Use Phase. Protection of the TOE during this phases is directly addressed by OT.ADMIN_Configuration "Protection of the TOE administration".

T.Key_Access The threat T.Key_Access addresses the threat of access to the internal secret cryptographic keys of the TOE. The TOE protects the key usage through OT.Key_Usage_Counter "Configuration of Key Usage Counter" that support a Key Usage Counter that is decremented by one each time the key is used. Once the counter is depleted,

the key becomes unusable. In the case of CA key, the Key Usage Counter will be reset to the maximum usage if the CA key is re-generated in USE phase.

7.3.2 Organizational Security Policies

7.3.2.1 Security Policies drawn from the Protection Profiles

P.CSP_QCert 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. P.CSP_QCert is addressed by

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialization, personalization and operational usage;
- OT.SCD_SVD_Corresp, which requires to ensure the correspondence between the SVD and the SCD during their generation;
- OE.SCD/SVD_Auth_Gen, which ensures that the SCD/SVD generation can be invoked by authorised users only;
- OT.SCD_Auth_Imp which ensures that authorised users only may invoke the import of the SCD;
- OE.SCD_SVD_Corresp, which requires the CSP to ensure the correspondence between the SVD and the SCD during their generation, and
- OE.CGA_QCert for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory. According to OT.TOE_SSCD_Auth the copies of the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD to prove this identity as SSCD to the CGA. The OE.CGA_SSCD_Auth ensures that the SP checks the proof of the device presented of the applicant that it is a SSCD.

P.QSign 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 requires the TOE to meet (Annex III of the [Directive] or Article 26 of new [eIDAS_Regulation]). This is ensured as follows:

- OE.SCD_Unique meets the (paragraph 1 bullet (a) of the [Directive], Annex III or bullet (a) of new [eIDAS_Regulation], Article 26), by the requirements that the SCD used for signature creation can practically occur only once;
- OT.SCD_Unique meets Annex III, by the requirements that the SCD used for signature creation can practically occur only once;

- OT.SCD_Unique, OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in Annex III by the requirements to ensure secrecy of the SCD;
- OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of the SCD against specific attacks;
- OT.SCD_Auth_Imp, which limits SCD import to authorised users only;
- OE.SCD_Secrecy, which ensures the confidentiality of the SCD during generation and export to the TOE, and deletes the SCD after export to the TOE. The CSP does not use the SCD for signature creation;
- OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in in paragraph 1(b) of Annex III by the requiements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE; — OT.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only, and
- OT.Sigy_SigF meets the requirement in Annex III by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others;
- OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of Annex III as the TOE shall not alter the DTBS/R. Annex III requires that a SSCD does not prevent the data to be signed from being presented to the signatory prior to the signature process is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the signatory and send it to the SSCD for signing. The usage of SCD under sole control of the signatory is ensured by
- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialization, personalization and operational usage;
- OE.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only;
- 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 SSCD from an SSCD-provisioning service.
- OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialized and personalized TOE from an SSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD In the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA_SSCD_Auth and the received SVD is sent by this SSCD as required by OE.CGA_TC_SVD_Imp. Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

P.Sig_Non-Repud 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 created with the TOE. 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. 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 provides that the signatory's SCD can practically occur just once. OE.SCD_SVD_Corresp 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. OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. OT.SCD_Unique provides that the signatory's SCD can practically occur just once. OE.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 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.DTBS_Intend, OE.DTBS_Protect 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. The robust cryptographic techniques required by OT.Sig_Secure 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. The TOE security feature addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp supported by OE.Dev_Prov_Service enables the verification whether the device presented by the applicant is a SSCD as required by OE.CGA_SSCD_Auth and the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA_TC_SVD_Imp. OE.DTBS_Intend (SCA sends data intended to be signed), OE.DTBS_Protect OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure 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. OT.LifeCycle_Management ensures that when the TOE is under the Personalization Agent control, it can not be misused to sign on behalf of the legitimate Signatory. OE.LinkSCD_QualifiedCertificate ensure the SCA always uses the SCD it intends to, in order to create a digital signature. OE.LinkSCD_QualifiedCertificate ensures that the SCA can unambiguously sort out within

the TOE file structure the SCD matching any (qualified) certificate it has chosen and intends to use.

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

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

7.3.2.2 Additional Security Policies

P.LinkSCD_QualifiedCertificate ensures that the SCA can unambiguously find within the TOE File structure the SCD matching a (qualified) certificate it has chosen to perform an electronic signature. It is addressed by OE.LinkSCD_QualifiedCertificate that ensures an unambiguous link between each (qualified) certificate and the matching SCD loaded in the TOE.

P.TOE_PublicAuthKey_Cert ensures that each private key(s) of the TOE for authentication matches the public key stored within the relevant certificate issued by an entitled entity. The authentication public key is exported thanks to OE.TOE_PublicKeyAuth_Transfer.

P.eServices ensures that the TOE provides secure eServices functionalities. It is addressed by OT.eServices.

P.EAC_Terminal addresses the requirement for Authentication Terminals to implement the terminal parts of the protocols needed to executed EAC according to its specification in [TR-03110-1] and [TR-03110-3], and to store (static keys) or generate (temporary keys and nonces) the needed related credentials. This is enforced by OE.AuthKey_Transfer, OE.AuthKey_Unique and OE.TOE_PublicKeyAuth_Transfer which require Chip Authentication and Restricted Identity keys to be correctly generated and stored, by OE.Terminal_Authentication for the PKI needed for Terminal Authentication, and by OE.Terminal which covers the PACE protocol and the digital seal verification.

P.Terminal_PKI is enforced by establishing the receiving PKI branch as aimed by the objective OE.Terminal_Authentication

P.Card_PKI is enforced by establishing the issuing PKI branch as aimed by the objective OE.Passive_Auth_Sign (for the digital seal verification).

P.Pre-Operational is enforced by the following security objectives: OT.Identification is affine to the OSP's property 'traceability before the operational phase'; OT.AC_Pers_EAC and OE.Personalization together enforce the OSP's properties 'correctness of the User- and the

TSF-data stored' and 'authorisation of Personalisation Agents'; OE.Legislative_Compliance is affine to the OSP's property 'compliance with laws and regulations'.

P.Terminal is obviously enforced by the objective OE.Terminal, whereby the one-to-one mapping between the related properties is applicable

P.Trustworthy_PKI is enforced by OE.Passive_Auth_Sign (for Issuer CA, issuing PKI branch).

P.Manufact The OSP P.Manufact "Manufacturing of the electronic document's chip" requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalisation Data as being fulfilled by OT.Identification.

7.3.3 Assumptions

7.3.3.1 All SSCD parts

A.CGA 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.SCA 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.

7.3.3.2 Parts 3 and 6 only

A.CSP establishes several security aspects concerning handling of SCD and SVD by the CSP. That the SCD/SVD generation device can only be used by authorised users is addressed by OE.SCD/SVD_Auth_Gen (Authorised SCD/SVD Generation), that the generated SCD is unique and cannot be derived by the SVD is addressed by OE.SCD_Unique (Uniqueness of the signature creation data), that SCD and SVD correspond to each other is addressed by OE.SCD_SVD_Corresp (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are deleted in the environment once exported to the TOE is addressed by OE.SCD_Secrecy (SCD Secrecy).

7.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.SCD_Divulg	OT.SCD_Secrecy, OT.SCD_Auth_Imp, OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy	Section 7.3.1

T.SCD_Derive	OT.SCD/SVD_Auth_Gen, OT.Sig_Secure, OE.SCD_Unique	Section 7.3.1
T.Hack_Phys	OT.SCD_Secrecy, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, OT.Keys_Secrecy	Section 7.3.1
T.SVD_Forgery	OT.SCD_SVD_Corresp, OE.SVD_Auth, OE.SCD_SVD_Corresp, OT.TOE_TC_SVD_Exp, OE.CGA_TC_SVD_Imp	Section 7.3.1
T.SigF_Misuse	OT.Lifecycle_Security, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OE.Signatory, OE.DTBS_Intend, OE.HID_VAD, OE.DTBS_Protect, OT.Lifecycle_Management, OT.TOE_TC_VAD_Imp, OT.TOE_TC_DTBS_Imp, OE.HID_TC_VAD_Exp, OE.SCA_TC_DTBS_Exp	Section 7.3.1
T.DTBS_Forgery	OT.DTBS_Integrity_TOE, OE.DTBS_Intend, OE.DTBS_Protect, OT.TOE_TC_DTBS_Imp, OE.SCA_TC_DTBS_Exp	Section 7.3.1
T.Sig_Forgery	OT.SCD_Unique, OT.Sig_Secure, OE.CGA_QCert, OE.SCD_Unique	Section 7.3.1
T.Key_Divulg	OT.Key_Lifecycle_Security, OT.Keys_Secrecy, OE.AuthKey_Transfer	Section 7.3.1
T.Key_Derive	OT.Authentication_Secure, OT.TOE_AuthKey_Unique, OE.AuthKey_Unique	Section 7.3.1
T.TOE_PublicAuthKey_Forgery	OE.TOE_PublicKeyAuth_Transfer	Section 7.3.1
T.Authentication_Replay	OT.Authentication_Secure	Section 7.3.1
T.Counterfeit	OT.Authentication_Secure, OE.AuthKey_Transfer, OE.AuthKey_Unique, OE.TOE_PublicKeyAuth_Transfer	Section 7.3.1
T.Sensitive_Data	OT.Authentication_Secure, OE.Terminal_Authentication	Section 7.3.1
T.Abuse-Func	OT.Authentication_Secure	Section 7.3.1
T.Eavesdropping	OT.Authentication_Secure	Section 7.3.1
T.Forgery	OT.Authentication_Secure, OT.AC_Pers_EAC, OE.Passive_Auth_Sign, OE.Personalization, OE.Terminal	Section 7.3.1
T.Information_Leakage	OT.Authentication_Secure	Section 7.3.1
T.Malfunction	OT.Authentication_Secure	Section 7.3.1

T.Phys-Tamper	OT.Authentication_Secure	Section 7.3.1
T.Skimming	OT.Authentication_Secure, OE.Terminal_Authentication, OE.Electronic_Document_Holder	Section 7.3.1
T.Tracing	OT.Tracing, OE.Electronic_Document_Holder	Section 7.3.1
T.ADMIN_Configuration	OT.ADMIN_Configuration	Section 7.3.1
T.Key_Access	OT.Key_Usage_Counter	Section 7.3.1

Table 16 Threats and Security Objectives - Coverage

Security Objectives	Threats
OT.Lifecycle_Security	T.SigF_Misuse
OT.SCD_Secrecy	T.SCD_Divulg, T.Hack_Phys
OT.Sig_Secure	T.SCD_Derive, T.Sig_Forgery
OT.Sigy_SigF	T.SigF_Misuse
OT.DTBS_Integrity_TOE	T.SigF_Misuse, T.DTBS_Forgery
OT.EMSEC_Design	T.Hack_Phys
OT.Tamper_ID	T.Hack_Phys
OT.Tamper_Resistance	T.Hack_Phys
OT.SCD/SVD_Auth_Gen	T.SCD_Derive
OT.SCD_Unique	T.Sig_Forgery
OT.SCD_SVD_Corresp	T.SVD_Forgery
OT.SCD_Auth_Imp	T.SCD_Divulg
OT.TOE_SSCD_Auth	
OT.TOE_TC_SVD_Exp	T.SVD_Forgery
OT.TOE_TC_VAD_Imp	T.SigF_Misuse
OT.TOE_TC_DTBS_Imp	T.SigF_Misuse, T.DTBS_Forgery
OT.Identification	
OT.Authentication_Secure	T.Key_Derive, T.Authentication_Replay, T.Counterfeit, T.Sensitive_Data, T.Abuse-Func, T.Eavesdropping, T.Forgery, T.Information_Leakage, T.Malfunction, T.Phys-Tamper, T.Skimming
OT.Key_Lifecycle_Security	T.Key_Divulg
OT.Keys_Secrecy	T.Hack_Phys, T.Key_Divulg
OT.TOE_AuthKey_Unique	T.Key_Derive

OT.Lifecycle_Management	T.SigF_Misuse
OT.eServices	
OT.AC_Pers_EAC	T.Forgery
OT.Tracing	T.Tracing
OT.ADMIN_Configuration	T.ADMIN_Configuration
OT.Key_Usage_Counter	T.Key_Access
OE.SVD_Auth	T.SVD_Forgery
OE.CGA_QCert	T.Sig_Forgery
OE.DTBS_Intend	T.SigF_Misuse, T.DTBS_Forgery
OE.Signatory	T.SigF_Misuse
OE.HID_VAD	T.SigF_Misuse
OE.DTBS_Protect	T.SigF_Misuse, T.DTBS_Forgery
OE.SSCD_Prov_Service	
OE.SCD/SVD_Auth_Gen	T.SCD_Divulg
OE.SCD_Secrecy	T.SCD_Divulg
OE.SCD_Unique	T.SCD_Derive, T.Sig_Forgery
OE.SCD_SVD_Corresp	T.SVD_Forgery
OE.Dev_Prov_Service	
OE.CGA_TC_SVD_Imp	T.SVD_Forgery
OE.CGA_SSCD_Auth	
OE.HID_TC_VAD_Exp	T.SigF_Misuse
OE.SCA_TC_DTBS_Exp	T.SigF_Misuse, T.DTBS_Forgery
OE.LinkSCD_QualifiedCertificate	
OE.AuthKey_Transfer	T.Key_Divulg, T.Counterfeit
OE.AuthKey_Unique	T.Key_Derive, T.Counterfeit
OE.TOE_PublicKeyAuth_Transfer	T.TOE_PublicAuthKey_Forgery, T.Counterfeit
OE.Terminal_Authentication	T.Sensitive_Data, T.Skimming
OE.Legislative_Compliance	
OE.Passive_Auth_Sign	T.Forgery
OE.Personalization	T.Forgery
OE.Terminal	T.Forgery
OE.Electronic_Document_Holder	T.Skimming, T.Tracing

Table 17 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.CSP_QCert	OT.Lifecycle_Security, OT.SCD_SVD_Corresp, OE.CGA_QCert, OT.SCD_Auth_Imp, OE.SCD/SVD_Auth_Gen, OE.SCD_SVD_Corresp, OT.TOE_SSCD_Auth, OE.CGA_SSCD_Auth	Section 7.3.2
P.QSign	OT.Sig_Secure, OT.Sigy_SigF, OE.CGA_QCert, OE.DTBS_Intend	Section 7.3.2
P.Sigy_SSCD	OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen, OT.SCD_Unique, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_Resistance, OT.SCD_Auth_Imp, OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OT.TOE_SSCD_Auth, OT.TOE_TC_SVD_Exp, OE.Dev_Prov_Service, OE.CGA_TC_SVD_Imp, OE.CGA_SSCD_Auth, OE.SSCD_Prov_Service	Section 7.3.2
P.Sig_Non-Repud	OT.Lifecycle_Security, OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, OE.CGA_QCert, OE.SVD_Auth, OE.DTBS_Intend, OE.Signatory, OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OE.SCD_SVD_Corresp, OT.TOE_SSCD_Auth, OT.TOE_TC_SVD_Exp, OE.Dev_Prov_Service, OE.CGA_TC_SVD_Imp, OE.CGA_SSCD_Auth, OE.DTBS_Protect, OE.LinkSCD_QualifiedCertificate, OT.TOE_TC_VAD_Imp,	Section 7.3.2

	OT.TOE_TC_DTBS_Imp, OE.HID_TC_VAD_Exp, OE.SCA_TC_DTBS_Exp, OE.SSCD_Prov_Service	
P.LinkSCD_QualifiedCertificate	OE.LinkSCD_QualifiedCertificate	Section 7.3.2
P.TOE_PublicAuthKey_Cert	OE.TOE_PublicKeyAuth_Transfer	Section 7.3.2
P.eServices	OT.eServices	Section 7.3.2
P.EAC_Terminal	OE.Terminal, OE.Terminal_Authentication, OE.AuthKey_Transfer, OE.AuthKey_Unique, OE.TOE_PublicKeyAuth_Transfer	Section 7.3.2
P.Terminal_PKI	OE.Terminal_Authentication	Section 7.3.2
P.Card_PKI	OE.Passive_Auth_Sign	Section 7.3.2
P.Pre-Operational	OT.AC_Pers_EAC, OE.Personalization, OE.Legislative_Compliance, OT.Identification	Section 7.3.2
P.Terminal	OE.Terminal	Section 7.3.2
P.Trustworthy_PKI	OE.Passive_Auth_Sign	Section 7.3.2
P.Manufact	OT.Identification	Section 7.3.2

Table 18 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
OT.Lifecycle_Security	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud
OT.SCD_Secrecy	P.Sigy_SSCD, P.Sig_Non-Repud
OT.Sig_Secure	P.QSign, P.Sigy_SSCD, P.Sig_Non-Repud
OT.Sigy_SigF	P.QSign, P.Sigy_SSCD, P.Sig_Non-Repud
OT.DTBS_Integrity_TOE	P.Sigy_SSCD, P.Sig_Non-Repud
OT.EMSEC_Design	P.Sigy_SSCD, P.Sig_Non-Repud
OT.Tamper_ID	P.Sig_Non-Repud
OT.Tamper_Resistance	P.Sigy_SSCD, P.Sig_Non-Repud
OT.SCD/SVD_Auth_Gen	P.Sigy_SSCD
OT.SCD_Unique	P.Sigy_SSCD, P.Sig_Non-Repud
OT.SCD_SVD_Corresp	P.CSP_QCert, P.Sig_Non-Repud
OT.SCD_Auth_Imp	P.CSP_QCert, P.Sigy_SSCD

OT.TOE_SSCD_Auth	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud
OT.TOE_TC_SVD_Exp	P.Sigy_SSCD, P.Sig_Non-Repud
OT.TOE_TC_VAD_Imp	P.Sig_Non-Repud
OT.TOE_TC_DTBS_Imp	P.Sig_Non-Repud
OT.Identification	P.Pre-Operational, P.Manufact
OT.Authentication_Secure	
OT.Key_Lifecycle_Security	
OT.Keys_Secrecy	
OT.TOE_AuthKey_Unique	
OT.Lifecycle_Management	
OT.eServices	P.eServices
OT.AC_Pers_EAC	P.Pre-Operational
OT.Tracing	
OT.ADMIN_Configuration	
OT.Key_Usage_Counter	
OE.SVD_Auth	P.Sig_Non-Repud
OE.CGA_QCert	P.CSP_QCert, P.QSign, P.Sig_Non-Repud
OE.DTBS_Intend	P.QSign, P.Sig_Non-Repud
OE.Signatory	P.Sig_Non-Repud
OE.HID_VAD	
OE.DTBS_Protect	P.Sig_Non-Repud
OE.SSCD_Prov_Service	P.Sigy_SSCD, P.Sig_Non-Repud
OE.SCD/SVD_Auth_Gen	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud
OE.SCD_Secrecy	P.Sigy_SSCD, P.Sig_Non-Repud
OE.SCD_Unique	P.Sigy_SSCD, P.Sig_Non-Repud
OE.SCD_SVD_Corresp	P.CSP_QCert, P.Sig_Non-Repud
OE.Dev_Prov_Service	P.Sigy_SSCD, P.Sig_Non-Repud
OE.CGA_TC_SVD_Imp	P.Sigy_SSCD, P.Sig_Non-Repud
OE.CGA_SSCD_Auth	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud
OE.HID_TC_VAD_Exp	P.Sig_Non-Repud
OE.SCA_TC_DTBS_Exp	P.Sig_Non-Repud

OE.LinkSCD_QualifiedCertificate	P.Sig_Non-Repud, P.LinkSCD_QualifiedCertificate
OE.AuthKey_Transfer	P.EAC_Terminal
OE.AuthKey_Unique	P.EAC_Terminal
OE.TOE_PublicKeyAuth_Transfer	P.TOE_PublicAuthKey_Cert, P.EAC_Terminal
OE.Terminal_Authentication	P.EAC_Terminal, P.Terminal_PKI
OE.Legislative_Compliance	P.Pre-Operational
OE.Passive_Auth_Sign	P.Card_PKI, P.Trustworthy_PKI
OE.Personalization	P.Pre-Operational
OE.Terminal	P.EAC_Terminal, P.Terminal
OE.Electronic_Document_Holder	

Table 19 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.CGA	OE.CGA_QCert, OE.SVD_Auth	Section 7.3.3
A.SCA	OE.DTBS_Intend	Section 7.3.3
A.CSP	OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OE.SCD_SVD_Corresp	Section 7.3.3

Table 20 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions
OE.SVD_Auth	A.CGA
OE.CGA_QCert	A.CGA
OE.DTBS_Intend	A.SCA
OE.Signatory	
OE.HID_VAD	
OE.DTBS_Protect	
OE.SSCD_Prov_Service	
OE.SCD/SVD_Auth_Gen	A.CSP
OE.SCD_Secrecy	A.CSP
OE.SCD_Unique	A.CSP
OE.SCD_SVD_Corresp	A.CSP
OE.Dev_Prov_Service	

OE.CGA_TC_SVD_Imp	
OE.CGA_SSCD_Auth	
OE.HID_TC_VAD_Exp	
OE.SCA_TC_DTBS_Exp	
OE.LinkSCD_QualifiedCertificate	
OE.AuthKey_Transfer	
OE.AuthKey_Unique	
OE.TOE_PublicKeyAuth_Transfer	
OE.Terminal_Authentication	
OE.Legislative_Compliance	
OE.Passive_Auth_Sign	
OE.Personalization	
OE.Terminal	
OE.Electronic_Document_Holder	

Table 21 Security Objectives for the Operational Environment and Assumptions - Coverage

8 Extended Requirements

8.1 Extended Families

8.1.1 Extended Family FPT_EMS - TOE Emanation

8.1.1.1 Description

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 TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, 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.

8.1.1.2 Extended Components

Extended Component FPT_EMS.1

Family behavior:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS TOE Emanation	1

FPT_EMS.1 TOE Emanation has two constituents:

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

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

Definition

FPT_EMS.1 TOE Emanation

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

8.1.2 Extended Family FMT_LIM - Limited capabilities

8.1.2.1 Description

The family FMT_LIM describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing abuse of functions by limiting the capabilities of the functions and by limiting their availability.

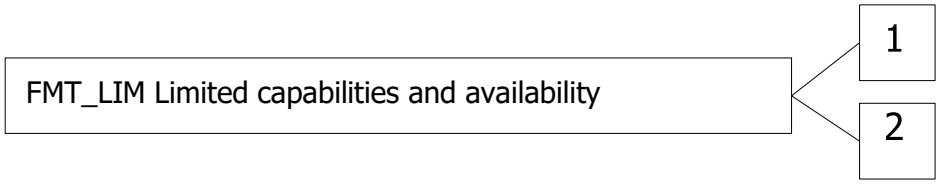
8.1.2.2 Extended Components

Extended Component FMT_LIM.1

Family behavior:

This family defines requirements that limit the capabilities and availability of functions in acombined manner. Note, that FDP_ACF restricts access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuinepurpose.

FMT_LIM.2	Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.
Management:	FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.
Audit:	FMT_LIM.1, FMT_LIM.2 There are no actions defined to be auditable.

Definition

FMT_LIM.1 Limited capabilities

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced [assignment: Limited capability and availability policy]

Hierarchical to: No other components

Dependencies: FMT_LIM.2 Limited availability.

Extended Component FMT_LIM.2

Definition

FMT_LIM.2 Limited availability

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced [assignment: Limited capability and availability policy]

Hierarchical to: No other components

Dependencies: FMT_LIM.1 Limited availability.

8.1.3 Extended Family FIA_API - Authentication Proof of Identity

8.1.3.1 Description

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

Application note 10: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter 'Explicitly stated IT security requirements (APE_SRE)') from a TOE point of view.

8.1.3.2 Extended Components

Extended Component FIA_API.1

Family behavior:

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

Component levelling:

FIA_API Authentication Proof of Identity	1

Management FIA_API.1

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

Audit: FIA_API.1
There are no actions defined to be auditable.

Definition

FIA_API.1 Authentication Proof of Identity

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

Hierarchical to: No other components

Dependencies: No dependencies.

8.1.4 Extended Family FCS_RND - Generation of random numbers

8.1.4.1 Description

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

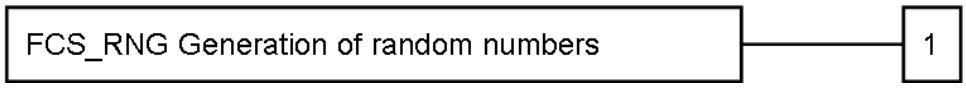
8.1.4.2 Extended Components

Extended Component FCS_RND.1

Family behavior:

This family defines requirements for the generation random number where the random numbers are intended to be used for cryptographic purposes.

Component levelling:



Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

Definition

FCS_RND.1 Quality metric for random numbers

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

Hierarchical to: No other components.

Dependencies: No dependencies.

9 Security Requirements

9.1 Security Functional Requirements

This section describes the requirements imposed on the TOE in order to achieve the security objectives laid down in the previous chapter. In some of the functional requirements below, the [Editorially Refined] tag has been used to signify a small change in the requirement, to adhere to proper English grammar, or to make it more understandable to the reader.

9.1.1 Security Attributes

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

Subject or object the security attribute is associated with	Security Attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	Authorized, Not authorized
SCD	SCD Operational	Yes, No
SCD	SCD Identifier	Arbitrary value

9.1.1.1 SCD/SVD Management

In phase 6

S.Admin is the personalization agent, and as such always has the attribute "SCD/SVD Management" set to "Authorized". Furthermore in that phase, the TOE allows the SCD to be imported or generated.

In phase 7

In this phase, the TOE only supports SCD/SVD generation. The access condition for SCD/SVD generation is granted if the User is successfully authenticated as S.Admin. If this condition is fulfilled, the attribute "SCD/SVD management" is set to "authorized", otherwise it is set to "not authorized".

9.1.1.2 SCD Operational

In phase 6

The attribute "SCD operational" is always set to "No".

In phase 7

The attribute "SCD operational" is set to "yes" as soon as the subject is authenticated as S.Signatory, using the RAD.

9.1.2 All SSCD parts

9.1.2.1 Protection of the TSF (FPT)

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **side channel emissions** in excess of **limits specified by the state-of-the-art attacks on smart card IC** enabling access to **SCD** and **RAD**.

FPT_EMS.1.2 The TSF shall ensure **all users** are unable to use the following interface **external contact emanations** to gain access to **RAD** and **SCD**.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- **self-test according to FPT_TST fails**
- **security violation detected by [ST_PTF] with FAU_ARP.1**.

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **physical manipulation and physical probing** to the **TSF** by responding automatically such that the SFRs are always enforced.

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up** to demonstrate the correct operation of **the TSF**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of **TSF**.

9.1.2.2 Security management (FMT)

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **R.Admin and R.Sigy**.

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

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- **Creation and modification of RAD,**
- **Enabling the signature creation function,**
- **Modification of the security attribute SCD/SVD management, SCD operational,**
- **Change the default value of the security attribute SCD Identifier,**
- **SCD/SVD Generation,**
- **SCD import,**
- **Unblock of RAD,**
- **Initialisation, change, resume, and unblock of PIN and PUK,**
- **Erase of PIN and RAD,**
- **Reinitialisation of PIN,**
- **Create and Delete File in Use Phase**.

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **enable** the functions **signature creation function** to **R.Sigy**.

FMT_MSA.1/Admin Management of security attributes

FMT_MSA.1.1/Admin The TSF shall enforce the **SCD/SVD Generation SFP and SCD Import SFP** to restrict the ability to **modify** the security attributes **SCD/SVD management** to **R.Admin**.

FMT_MSA.1/Signatory Management of security attributes

FMT_MSA.1.1/Signatory The TSF shall enforce the **Signature Creation SFP** to restrict the ability to **modify** the security attributes **SCD operational** to **R.Sigy**.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for

- **SCD/SVD Management**
- **SCD operational**.

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **SCD/SVD Generation SFP, SVD Transfer SFP, SCD Import SFP and Signature Creation SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **authorized identified role** to specify alternative initial values to override the default values when an object or information is created.

Application Note:

The authorized identified roles are defined in the following table depending on the TOE lifecycle phase

Security attribute	**Phase**	**Authorized identified roles**
SCD/SVD Management	6&7	R.Admin
SCD Operational	7	R.Sigy

FMT_MSA.4 Security attribute value inheritance

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes:

- **If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation**
- **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" after import of the SCD as a single operation.**
- **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**

Application Note:

Third point doesn't apply as SCD import is only possible in phase 6 where the role R.Sigy doesn't exist

FMT_MTD.1/Admin Management of TSF data

FMT_MTD.1.1/Admin The TSF shall restrict the ability to **[Operation]** the **[TSF Data]** to **Admin**

Operation	TSF Data
Create	**RAD, File in Use Phase**
Modify	**The Chip Authentication key parameters to be used during key generation in USE phase**
Read	**The Chip Authentication key parameters to be used during key generation in USE phase, Proof that a key has been on board generated**
Delete	**File in Use Phase**
Invalidate	**Invalidate one of the Chip Authentication key in USE phase or set the secondary key as being the primary key**

FMT_MTD.1/Signatory Management of TSF data

FMT_MTD.1.1/Signatory The TSF shall restrict the ability to **modify and none** the **RAD** to **R.Sigy**.

Application Note:

This requirement applies only to the RAD belonging to S.Sigy.

9.1.2.3 Identification and authentication (FIA)

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

- **self-test according to FPT_TST.1,**
- **establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD,**
- **establishing a trusted channel between the CSP and the TOE by means of TSF required by FTP_ITC.1/SCD**

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.

FIA_AFL.1/RAD Authentication failure handling

FIA_AFL.1.1/RAD The TSF shall detect when **an administrator configurable positive integer within 1 and 15** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.

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

Application Note:

These SFRs apply to R.Sigy and R.Admin using the PUK to authenticate itself.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

a) self-test according to FPT_TST.1,

b) identification of the user by means of TSF required by FIA_UID.1,

c) establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD

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

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

9.1.2.4 User data protection (FDP)

FDP_SDI.2/DTBS Stored data integrity monitoring and action

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

FDP_SDI.2.2/DTBS Upon detection of a data integrity error, the TSF shall

- **prohibit the use of the altered data**
- **inform the S.Sigy about integrity error**.

Application Note:

The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data".

FDP_SDI.2/Persistent Stored data integrity monitoring and action

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

FDP_SDI.2.2/Persistent Upon detection of a data integrity error, the TSF shall

- **prohibit the use of the altered data**
- **inform the S.Sigy about integrity error**.

Application Note:

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

- SCD
- RAD
- Keys

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **SCD, RAD, VAD, Keys, PIN, PUK, Session keys and related data**.

FDP_ACC.1/Signature_Creation Subset access control

FDP_ACC.1.1/Signature_Creation The TSF shall enforce the **Signature Creation SFP** on

- **subjects: S.User,**
- **objects: DTBS/R, SCD,**
- **operations: signature creation**.

FDP_ACF.1/Signature_Creation Security attribute based access control

FDP_ACF.1.1/Signature_Creation The TSF shall enforce the **Signature Creation SFP** to objects based on the following:

- **the user S.User is associated with the security attribute "Role" and**
- **the SCD with the security attribute "SCD Operational"**.

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"**.

FDP_ACF.1.3/Signature_Creation The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

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"**.

9.1.2.5 Cryptographic support (FCS)

FCS_COP.1/Sign Cryptographic operation

FCS_COP.1.1/Sign The TSF shall perform **Signature Computation** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithms	Key size(s)	Standard
Signature Computation with Off-Card Hashing: RSA and ECDSA	**RSA-1024, 1536, 2048, 3072 and 4096 bits with PKCS#1 v1.5 and PKCS#1-PSS EC-DSA over elliptic curves of size of- 192, 224, 256, 320, 384, 512 and 521 bits SHA-1, 224, 256, 384 and 512**	**[PKCS#1], [ANSIX9.62]**
Signature Computation with On-Card Hashing: ECDSA only	**EC-DSA over elliptic curves of size of 192, 224, 256, 320, 384, 512 and 521 SHA-1, 256 and 384**	**[ANSIX9.62]**

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the buffer containing the key with zero** that meets the following: **none**.

Application Note:

This SFR applies to all keys, whether it is the SCD, the SVD or another one. The cryptographic key SCD will be destroyed before the SCD is re-imported of re-generated into the TOE.

9.1.3 SSCD parts 2, 4 and 5 only

9.1.3.1 Cryptographic support (FCS)

FCS_CKM.1/SCD/SVD_Generation Cryptographic key generation

FCS_CKM.1.1/SCD/SVD_Generation [Editorially Refined] The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[cryptographic key sizes]** that meet the following: **[list of standards]**

The assignments of the cryptographic operations are described in the table below:

key generation algorithm	key sizes	list of standards
Key pair over Elliptic Curve	Any elliptic curve from 192 bits up to 521 with prime field p	[IEEE]
RSA Key generation	1024, 1536, 2048, 3072 and 4096 bits	[ANSIX9.31]

9.1.3.2 User data protection (FDP)

FDP_ACC.1/SVD_Transfer Subset access control

FDP_ACC.1.1/SVD_Transfer The TSF shall enforce the **SVD Transfer SFP** on

- **subjects: S.User;**
- **objects: SVD;**
- **operations: export**.

Application Note:

Note that here S.User can be either R.Sigy or R.Admin depending on the personalization done.

FDP_ACF.1/SVD_Transfer Security attribute based access control

FDP_ACF.1.1/SVD_Transfer The TSF shall enforce the **SVD Transfer SFP** to objects based on the following:

- **the S.User is associated with the security attribute Role,**
- **the SVD**.

FDP_ACF.1.2/SVD_Transfer The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **R.Admin is allowed to export SVD**.

FDP_ACF.1.3/SVD_Transfer The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/SVD_Transfer The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

Application Note:

For this operation, S.User is S.Admin.

In phase 6, S.Admin is the "personalization agent" and is always allowed to export the SVD.

In phase 7, S.Admin is the subject allowed to export the SVD.

FDP_ACC.1/SCD/SVD_Generation Subset access control

FDP_ACC.1.1/SCD/SVD_Generation The TSF shall enforce the **SCD/SVD Generation SFP** on

- **subjects: S.User,**
- **objects: SCD, SVD,**
- **operations: generation of SCD/SVD pair**.

FDP_ACF.1/SCD/SVD_Generation Security attribute based access control

FDP_ACF.1.1/SCD/SVD_Generation The TSF shall enforce the **SCD/SVD Generation SFP** to objects based on the following: **the user S.User is associated with the security attribute "SCD/SVD Management"**.

FDP_ACF.1.2/SCD/SVD_Generation The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to generate SCD/SVD pair**.

FDP_ACF.1.3/SCD/SVD_Generation The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/SCD/SVD_Generation The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair**.

Application Note:

In phase 7, the S.user can become S.admin after authentication as S.Signatory combined with an Authentication Terminal (TA_CMT)or Administration Terminal.

9.1.4 SSCD parts 3 and 6 only

9.1.4.1 Trusted path/channels (FTP)

FTP_ITC.1/SCD Inter-TSF trusted channel

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** to initiate communication via the trusted channel.

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

- **Data exchange integrity according to FDP_UCT.1/SCD**
- **None**.

9.1.4.2 User data protection (FDP)

FDP_UCT.1/SCD Basic data exchange confidentiality

FDP_UCT.1.1/SCD [Editorially Refined] The TSF shall enforce the **SCD Import SFP** to **receive SCD** in a manner protected from unauthorised disclosure.

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

FDP_ITC.1.1/SCD The TSF shall enforce the **SCD Import SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/SCD [Editorially Refined] The TSF shall ignore any security attributes associated with the **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: **SCD shall be sent by an authorized CSP**.

Application Note:

This SFR only applies in phase 6.

The TOE interacts with a CSP through a SCD/SVD generation application to import the SCD. Authorized CSP is able to establish a trusted channel with the TOE for SCD transfer as required by FTP_ITC.1.3/SCD.

The authorized CSP is the «Personalization Agent».

FDP_ACC.1/SCD_Import Subset access control

FDP_ACC.1.1/SCD_Import The TSF shall enforce the **SCD Import SFP** on

- **subjects: S.User,**
- **objects: SCD,**
- **operations: import of SCD**.

FDP_ACF.1/SCD_Import Security attribute based access control

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

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 "authorised" is allowed to import SCD**.

FDP_ACF.1.3/SCD_Import The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

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 authorised" is not allowed to import SCD**.

Application Note:

For this operation, S.User is S.Admin.

In phase 6, S.Admin is the "Personalization Agent" and always has the security attribute "SCD/SVD Management" set to "authorized".

In phase 7, SCD import is not allowed.

9.1.5 SSCD part 4 only

9.1.5.1 Trusted path/channels (FTP)

FTP_ITC.1/SVD Inter-TSF trusted channel

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

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

FTP_ITC.1.3/SVD [Editorially Refined] The TSF **or the CGA shall** initiate communication via the trusted channel for

- **data Authentication with Identity of Guarantor according to FIA_API.1 and FDP_DAU.2/SVD**
- **None**.

9.1.5.2 User data protection (FDP)

FDP_DAU.2/SVD Data Authentication with Identity of Guarantor

FDP_DAU.2.1/SVD The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **SVD**.

FDP_DAU.2.2/SVD The TSF shall provide **CGA** with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

9.1.5.3 Identification and authentication (FIA)

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide an **authentication mechanism** to prove the identity of the **SSCD**.

Application Note:

The authentication mechanism is achieved as follows:

- In phase 6: GP authentication

- In phase 6 & 7: an outgoing MAC

9.1.6 SSCD parts 5 and 6 only

9.1.6.1 User data protection (FDP)

FDP_UIT.1/DTBS Data exchange integrity

FDP_UIT.1.1/DTBS The TSF shall enforce the **Signature Creation SFP** to **receive** user data in a manner protected from **modification and insertion** errors.

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

9.1.6.2 Trusted path/channels (FTP)

FTP_ITC.1/VAD Inter-TSF trusted channel

FTP_ITC.1.1/VAD [Editorially Refined] 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 [Editorially Refined] The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/VAD [Editorially Refined] The TSF **or the HID** shall initiate communication via the trusted channel for:

- **User authentication according to FIA_UAU.1**
- **Assignment: None**

FTP_ITC.1/DTBS Inter-TSF trusted channel

FTP_ITC.1.1/DTBS [Editorially Refined] 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 [Editorially Refined] The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/DTBS [Editorially Refined] The TSF **or the SCA** shall initiate communication via the trusted channel for

- **signature creation**
- **Assignment: None**.

9.1.7 Additional SFRs

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **FCS_RNG.1 Quality metric for random numbers of [ST_PTF]**.

FCS_CKM.1/DH_PACE Cryptographic key generation

FCS_CKM.1.1/DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[cryptographic key sizes]** that meet the following: **[standard]**

Cryptographic Key Generation Algorithm	**Cryptographic Key Sizes**	**Standard**
ECDH compliant to [ISO_15946]	**192 bits to 521 bits**	**Based on ECDH protocol compliant to [TR-03111]**

FCS_CKM.1/Session Keys Cryptographic key generation

FCS_CKM.1.1/Session Keys [Editorially Refined] The TSF shall generate session keys in accordance with a specified cryptographic key generation algorithm **key derivation function** and specified cryptographic key sizes

- **DES keys of 112 bits**
- **AES keys of 128, 192 and 256 bits**

that meet the following: **[TR-03110-3], [GP2.3], [SCP03]**.

FCS_COP.1/GP Secret Data Protection Cryptographic operation

FCS_COP.1.1/GP Secret Data Protection The TSF shall perform **GP secret data encryption** in accordance with a specified cryptographic algorithm

- **SCP02**
- **SCP03 using AES**

and cryptographic key sizes

- **128 bits**
- **128, 192 and 256 bits**

that meet the following:

- **[GP2.3]**
- **[SCP03]**.

Application Note:

The type of algorithm used by the TOE depends on the configuration set during the javacard open platform Personalization (For more details see [AGD_PRE_PLT]). The applet provides this service via the platform, it doesn't own and cannot access the keys used to protect secret data. Their import/generation and destruction are managed by the platform.

FCS_COP.1/SM in Confidentiality Cryptographic operation

FCS_COP.1.1/SM in Confidentiality The TSF shall perform **Secure messaging in confidentiality** in accordance with a specified cryptographic algorithm

- **Encryption with TDES EDE in CBC mode**
- **Encryption with AES in CBC mode**

and cryptographic key sizes

- **128 bits**
- **128 bits, 192 bits and 256 bits**

that meet the following:

- **[GP2.3] and [TR-03110-3]**
- **[SCP03] and [TR-03110-3]**.

Application Note:

This algorithm is used during secure Messaging to ensure confidentiality of incoming and outgoing data.

FCS_COP.1/SM in Integrity Cryptographic operation

FCS_COP.1.1/SM in Integrity The TSF shall perform **Secure messaging in integrity and authenticity** in accordance with a specified cryptographic algorithm

- **Retail MAC: MAC algorithm 3 with padding method 2 and DES block Cipher**
- **CMAC**

and cryptographic key sizes

- **128 bits**
- **128 bits, 192 bits and 256 bits**

that meet the following:

- **[GP2.3] and, [TR-03110-3]**
- **[SCP03] and [TR-03110-3]**.

Application Note:

This algorithm is used during secure Messaging to ensure integrity and authenticity of incoming and outgoing data.

FCS_COP.1/Digital Auth Cryptographic operation

FCS_COP.1.1/Digital Auth The TSF shall perform **Digital Authentication** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	Key Size(s)	Standard
Digital authentication with Off-Card Hashing: RSA and ECDSA	**RSA-1024, 1536, 2048, 3072 and 4096 bits with PKCS#1 v1.5 and PKCS#1-PSS EC-DSA over elliptic curves of size of-192, 224, 256, 320, 384, 512 and 521 bits SHA-1, 224, 256, 384 and 512**	**[PKCS#1], [ANSIX9.62]**
Digital authentication with On-Card Hashing: ECDSA only	**EC-DSA over elliptic curves of size of 192, 224, 256, 320, 384, 512 and 521 SHA-1, 256 and 384**	**[ANSIX9.62]**

FCS_COP.1/Enc Key Decipherment Cryptographic operation

FCS_COP.1.1/Enc Key Decipherment The TSF shall perform **Encryption Key Decipherment** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	Key Size(s)	Standard
Encryption key decipherment: RSA	**RSA-1024, 1536, 2048, 3072 and 4096 bits with PKCS#1 OAEP, using SHA-1, 224, 256, 384 and 512**	**[PKCS#1]**
Encryption key decipherment: EC-DH	**EC-DH over elliptic curves of size of 192, 224, 256, 320, 384, 512 and 521, using SHA-1, 224, 256, 384 and 512**	**[ANSIX9.62]**

FCS_COP.1/SIG_VER Cryptographic operation

FCS_COP.1.1/SIG_VER The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	Key Size(s)	Standard
EC-DSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	**Elliptic curves of size of 192 to 512 bits**	**[TR-03110-3]**
RSA PKCS#1 v1.5 & v2.1 PSS with SHA-1, SHA-256,SHA-512	**1024, 1536, 2048, 3072 and 4096 bits**	**[TR-03110-3]**

FDP_ACC.1/TRM Subset access control

FDP_ACC.1.1/TRM The TSF shall enforce the **Access Control SFP** on **terminals gaining access User data stored in the TOE (including sensitive user data)**.

FDP_ACF.1/TRM Security attribute based access control

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

- **Subjects: Terminal, BAT, Authentication Terminal.**
- **Objects: User data stored in the TOE (including sensitive user data),**

- **Security attributes: Terminal Authorization**.

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 BAT is allowed to read data objects (except sensitive user data) specified in FDP_ACF.1.1/TRM after successful authentication, as required by FIA_UAU.1/PACE.**
- **Reading, modifying, writing, or using sensitive user data protected by CAv1 and TAv1 (objects specified in FDP_ACF.1.1/TRM) is only allowed to Authentication Terminals using the following mechanism: The TOE applies the EAC protocol (cf. FIA_UAU.5) to determine effective authorizations of the terminal. To determine the effective authorization of a terminal, the chip must calculate a bitwise Boolean 'and' of the relative authorization contained in the CHAT of the Terminal Certificate, the referenced eService certification authority Certificate. Based on the terminal type drawn from the CHAT of the Terminal Certificate, the TOE shall grant the right to read, modify or write sensitive user data, or perform operations using these sensitive user data**.

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

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

- **Any terminal not being a BAT or an Authentication Terminal is not allowed to read, to write, to modify, or to use any user data specified in FDP_ACF.1.1/TRM.**
- **In contactless, terminals not using secure messaging are not allowed to read, write, modify, or use any user data specified in FDP_ACF.1.1/TRM**.

FDP_ACC.1/MNG_File Subset access control

FDP_ACC.1.1/MNG_File The TSF shall enforce the **Create and Delete_FILE access Control SFP** on **administrator gaining access to create and delete EF file(s)**.

FDP_ACF.1/MNG_File Security attribute based access control

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

- **Subjects: Administrator**
- **Objects: EF Files**
- **Security attributes: Create File or Delete File ADMIN Access condition**.

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

- **The Administrator successfully authenticated following FDP_ACC.1/MNG_File can create or delete any transparent EF under any ADF whose Create File or Delete File access condition is set to ADMIN**.

FDP_ACF.1.3/MNG_File The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

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

- **Any subject not being authenticated as Administrator is not allowed:**
  - **To Create RAD,**
  - **Configure the size or value of the Chip Authentication key to be modified in USE phase,**
  - **Read that Proof that a key has been on board generated,**
  - **Create or Delete Files in Use Phase or**
  - **Invalidate one of the Chip Authentication key in USE phase**.

FDP_UCT.1/TRM Basic data exchange confidentiality

FDP_UCT.1.1/TRM The TSF shall enforce the **Access Control SFP** to **receive and transmit** user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/TRM Data exchange integrity

FDP_UIT.1.1/TRM The TSF shall enforce the **Access Control SFP** to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors.

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

FIA_UID.1/PACE Timing of identification

FIA_UID.1.1/PACE The TSF shall allow

- **to establish the communication channel**
- **to carry out the PACE Protocol (PIN, PUK, MRZ or CAN) according to [TR-03110-2] and [TR-03110-3] and/or the VERIFY PIN command**
- **to read the Initialization Data if it is not disable by TSF**

- **to carry out the Chip Authentication Protocol v.1 according to [TR-03110-3]**
- **to carry out the Terminal Authentication Protocol v.1 according to [TR-03110-3]**

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

FIA_UID.1.2/PACE The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/PACE Timing of authentication

FIA_UAU.1.1/PACE The TSF shall allow

- **to establish the communication channel**
- **to carry out the PACE Protocol (PIN, PUK, MRZ or CAN) according to [TR-03110-2] and [TR-03110-3] and/or the VERIFY PIN command**
- **to read the Initialization Data if it is not disable by TSF**
- **to identify themselves by selection of the authentication key**
- **to carry out the Chip Authentication Protocol v.1 according to [TR-03110-3]**
- **to carry out the Terminal Authentication Protocol v.1 according to [TR-03110-3]**

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

FIA_UAU.1.2/PACE The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4/PACE Single-use authentication mechanisms

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

- **PACE Protocol (PIN, PUK, MRZ or CAN) according to [TR-03110-2] and [TR-03110-3].**
- **Authentication Mechanisms based on Triple-DES or AES**
- **Terminal Authentication Protocol v.1 according to [TR-03110-3]**.

Application Note:

The Authentication Mechanisms based on Triple-DES or AES is the authentication process performed in phases 5 and 6.

FIA_UAU.5/PACE Multiple authentication mechanisms

FIA_UAU.5.1/PACE The TSF shall provide

- **PACE Protocol (PIN, PUK, MRZ or CAN) according to [TR-03110-2] and [TR-03110-3] and/or VERIFY PIN command**
- **Mean to verify the integrity and authenticity of the Chip authentication public key**
- **Secure messaging in MAC-ENC mode according to [TR-03110-3]**
- **Symmetric Authentication Mechanism based on Triple-DES or AES**
- **Terminal Authentication Protocol v.1 according to [TR-03110-3]**

to support user authentication.

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

- **Having successfully run the PACE protocol (PIN, PUK, MRZ or CAN), 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.**
- **The establishment of the secure messaging with the PACE protocol is not mandatory in contact mode unless compliance to PP-SSCD5 and/or PP-SSCD6 is required, then establishment of the secure messaging with the PACE protocol becomes mandatory in both contact and contactless mode.**
- **The TOE accepts the authentication attempt as Personalization Agent by the Authentication Mechanism with Personalization Agent Key(s).**
- **After run of the Chip Authentication Protocol Version 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.**
- **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**
- **The TOE accepts the authentication attempt as Administrator by the Authentication Mechanism with Administrator Key(s)**.

FIA_UAU.6/PACE Re-authenticating

FIA_UAU.6.1/PACE The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the BAT**.

FIA_UAU.6/EAC Re-authenticating

FIA_UAU.6.1/EAC The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System**.

FIA_AFL.1/AUTH Authentication failure handling

FIA_AFL.1.1/AUTH The TSF shall detect when **[selection]** unsuccessful authentication attempts occur related to **[list of authentication events]**.

FIA_AFL.1.2/AUTH When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **[list of actions]**

Selection	List of Authentication Events	List of Actions
Positive integer number set to 0x0A	**Authentication attempt involving MRZ or CAN as shared password for PACE**	**Wait for an increasing time between receiving of the terminal challenge and sending of the TSF response during the PACE authentication attempts**
An administrator configurable positive integer linked to the PIN or PUK (respectively)	**Consecutive failed authentication attempts using the PIN or PUK leaving a single authentication attempt**	**Suspend the PIN or the PUK**
'1'	**Consecutive failed authentication attempts using the suspended PIN or PUK**	**Block the PIN or the PUK**
'1'	**Personalization agent authentication attempt**	**slow down exponentially the next authentication**

FIA_API.1/TOE Authentication Authentication Proof of Identity

FIA_API.1.1/TOE Authentication The TSF shall provide an **authentication mechanism** to prove the identity of the **document holder**.

Application Note:

The TOE acts as a substitute for the Document holder, to authenticate digitally on its behalf. The authentication mechanism is triggered by the Document holder itself by presenting its PIN to the TOE.

FMT_SMR.1/PACE Security roles

FMT_SMR.1.1/PACE The TSF shall maintain the roles

- **Personalization Agent,**
- **Terminal,**
- **BAT,**
- **Country Verifying Certification Authority,**
- **eService certification authority,**
- **Authentication Terminal,**
- **Document holder**.

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

FMT_MTD.1/CVCA_INI Management of TSF data

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to **write** the

- **initial Country Verifying Certification Authority Public Key,**
- **initial Country Verifying Certification Authority Certificate,**
- **initial Current Date**

to **the personalization agent**.

FMT_MTD.1/CVCA_UPD Management of TSF data

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to **update** the

- **Country Verifying Certification Authority Public Key,**
- **Country Verifying Certification Authority Certificate,**

to **Country Verifying Certification Authority**.

FMT_MTD.1/DATE Management of TSF data

FMT_MTD.1.1/DATE The TSF shall restrict the ability to **modify** the **current date** to

- **Country Verifying Certification Authority,**
- **eService certification authority,**

- **Authentication Terminal**.

FMT_MTD.1/CAPK Management of TSF data

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to **load or generate** the **Chip Authentication Private Key selected in Access Control SFP** to **the Personalization Agent**.

FMT_MTD.1/KEY_READ Management of TSF data

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to **read** the

- **PACE passwords,**
- **Personalization Agent Keys,**
- **Chip Authentication Private Key,**
- **Administrator Key(s)**

to **none**.

FMT_MTD.1/Key_Usage_Counter Management of TSF data

FMT_MTD.1.1/Key_Usage_Counter The TSF shall restrict the ability to **configure** the **Key Usage Counter** to **Personalization Agent**.

FMT_MTD.1/Initialize_PIN Management of TSF data

FMT_MTD.1.1/Initialize_PIN The TSF shall restrict the ability to **write** the **PIN, PUK, MRZ and CAN, selected in Access Control SFP** to **the personalization agent**.

FMT_MTD.1/Resume_PIN Management of TSF data

FMT_MTD.1.1/Resume_PIN The TSF shall restrict the ability to **resume** the **suspended PIN or PUK selected in Access Control SFP** to **the electronic document presenter**.

FMT_MTD.1/Change_PIN Management of TSF data

FMT_MTD.1.1/Change_PIN The TSF shall restrict the ability to **change** the **PIN selected in Access Control SFP** to **the document holder (using the PUK for unblocking)**.

FMT_MTD.1/Unblock_PIN Management of TSF data

FMT_MTD.1.1/Unblock_PIN The TSF shall restrict the ability to **unblock** the **PIN selected in Access Control SFP** to **the document holder (using the PUK for unblocking)**.

FMT_MTD.1/UnblockChange_RAD Management of TSF data

FMT_MTD.1.1/UnblockChange_RAD The TSF shall restrict the ability to **unblock and optionally change** the **RAD selected in Access Control SFP** to

- **If change is required, the document holder (using the PUK for unblocking) and an Authentication Terminal (TA_PMT) or Administration Terminal in accordance with FMT_MTD.1/Signatory;**
- **Otherwise if only unblock is required, the document holder (using the PUK for unblocking)**.

FMT_MTD.1/Erase_PIN Management of TSF data

FMT_MTD.1.1/Erase_PIN The TSF shall restrict the ability to **erase** the **PIN or RAD selected in Access Control SFP** to **an Authentication Terminal (TA_PMT) or Administration Terminal**.

FMT_MTD.1/Reinitialize_PIN Management of TSF data

FMT_MTD.1.1/Reinitialize_PIN The TSF shall restrict the ability to **(re)initialize** the **PIN selected in Access Control SFP** to **the document holder (using the PUK)**.

FMT_MTD.1/UnblockChange_PUK Management of TSF data

FMT_MTD.1.1/UnblockChange_PUK The TSF shall restrict the ability to **unblock and change** the **PUK selected in Access Control SFP** to **an Authentication Terminal (TA_PMT)or Administration Terminal**.

FMT_MTD.1/TOE State Management of TSF data

FMT_MTD.1.1/TOE State The TSF shall restrict the ability to **switch** the **TOE from phase 6 to phase 7** to **personalization agent**.

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for **TSF data of the Terminal Authentication Protocol v1 and the Access Control SFP**.

FMT_MTD.1/INI_ENA Management of TSF data

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to **write** the **Initialisation Data and the Pre-personalisation Data** to **the Manufacturer**.

FMT_MTD.1/INI_DIS Management of TSF data

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to **read out** the **Initialisation Data and the Pre-personalisation Data** to **the Personalisation Agent**.

FMT_LIM.1 Limited capabilities

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced **Deploying Test Features after TOE Delivery does not allow**

- **User Data to be disclosed and manipulated,**
- **TSF data to be disclosed or manipulated,**
- **software to be reconstructed and,**
- **substantial information about construction of TSF to be gathered which may enable other attacks**

FMT_LIM.2 Limited availability

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced **Deploying Test Features after TOE Delivery does not allow**

- **User Data to be disclosed and manipulated,**

- **TSF data to be disclosed or manipulated,**
- **software to be reconstructed and,**
- **substantial information about construction of TSF to be gathered which may enable other attacks**

FPT_EMS.1/PIN-PUK-KEYS TOE Emanation

FPT_EMS.1.1/PIN-PUK-KEYS The TOE shall not emit **side channel emission** in excess of **limits specified by the state of the art attacks on smart card IC** enabling access to **PIN, PUK, Keys** and **none**.

FPT_EMS.1.2/PIN-PUK-KEYS The TSF shall ensure **all users** are unable to use the following interface **external contacts emanations** to gain access to **PIN, PUK, Keys** and **none**.

FTP_ITC.1/PACE Inter-TSF trusted channel

FTP_ITC.1.1/PACE [Editorially Refined] The TSF shall provide a communication channel between itself and a **BAT** 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. **The trusted channel shall be established by performing the PACE protocol according to [TR-03110-3].**

FTP_ITC.1.2/PACE [Editorially Refined] The TSF shall permit **the BAT** to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE The TSF shall initiate communication via the trusted channel for **any data exchange between the TOE and a BAT after PACE**.

9.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL5 augmented with AVA_VAN.5, ALC_FLR.1 and ALC_DVS.2.

9.2.1 ADV Development

9.2.1.1 ADV_ARC Security Architecture

ADV_ARC.1 Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.1.2 ADV_FSP Functional specification

ADV_FSP.5 Complete semi-formal functional specification with additional error information

ADV_FSP.5.1D The developer shall provide a functional specification.

ADV_FSP.5.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.5.1C The functional specification shall completely represent the TSF.

ADV_FSP.5.2C The functional specification shall describe the TSFI using a semi-formal style.

ADV_FSP.5.3C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.5.4C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.5.5C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.5.6C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.5.7C The functional specification shall describe all error messages that do not result from an invocation of a TSFI.

ADV_FSP.5.8C The functional specification shall provide a rationale for each error message contained in the TSF implementation yet does not result from an invocation of a TSFI.

ADV_FSP.5.9C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.5.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

9.2.1.3 ADV_IMP Implementation representation

ADV_IMP.1 Implementation representation of the TSF

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

9.2.1.4 ADV_TDS TOE design

ADV_TDS.4 Semiformal modular design

ADV_TDS.4.1D The developer shall provide the design of the TOE.

ADV_TDS.4.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.4.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.4.2C The design shall describe the TSF in terms of modules, designating each module as SFR-enforcing, SFR-supporting, or SFR-non-interfering.

ADV_TDS.4.3C The design shall identify all subsystems of the TSF.

ADV_TDS.4.4C The design shall provide a semiformal description of each subsystem of the TSF, supported by informal, explanatory text where appropriate.

ADV_TDS.4.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.4.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.4.7C The design shall describe each SFR-enforcing and SFR-supporting module in terms of its purpose and relationship with other modules.

ADV_TDS.4.8C The design shall describe each SFR-enforcing and SFR-supporting module in terms of its SFR-related interfaces, return values from those interfaces, interaction with

other modules and called SFR-related interfaces to other SFR-enforcing or SFR-supporting modules.

ADV_TDS.4.9C The design shall describe each SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.4.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

ADV_TDS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.4.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

9.2.1.5 ADV_INT TSF internals

ADV_INT.2 Well-structured internals

ADV_INT.2.1D The developer shall design and implement the entire TSF such that it has well-structured internals.

ADV_INT.2.2D The developer shall provide an internals description and justification.

ADV_INT.2.1C The justification shall describe the characteristics used to judge the meaning of ``well-structured''.

ADV_INT.2.2C The TSF internals description shall demonstrate that the entire TSF is well-structured.

ADV_INT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_INT.2.2E The evaluator shall perform an internals analysis on the TSF.

9.2.2 AGD Guidance documents

9.2.2.1 AGD_OPE Operational user guidance

AGD_OPE.1 Operational user guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.2.2 AGD_PRE Preparative procedures

AGD_PRE.1 Preparative procedures

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

9.2.3 ALC Life-cycle support

9.2.3.1 ALC_CMC CM capabilities

ALC_CMC.4 Production support, acceptance procedures and automation

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.2 ALC_CMS CM scope

ALC_CMS.5 Development tools CM coverage

ALC_CMS.5.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.5.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.

ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.5.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.3 ALC_DEL Delivery

ALC_DEL.1 Delivery procedures

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.4 ALC_DVS Development security

ALC_DVS.2 Sufficiency of security measures

ALC_DVS.2.1D The developer shall produce and provide development security documentation.

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the

confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_DVS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

9.2.3.5 ALC_FLR Flaw remediation

ALC_FLR.1 Basic flaw remediation

ALC_FLR.1.1D The developer shall document and provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective action to TOE users.

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.6 ALC_LCD Life-cycle definition

ALC_LCD.1 Developer defined life-cycle model

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.7 ALC_TAT Tools and techniques

ALC_TAT.2 Compliance with implementation standards

ALC_TAT.2.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

ALC_TAT.2.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

ALC_TAT.2.3D The developer shall describe and provide the implementation standards that are being applied by the developer.

ALC_TAT.2.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.2.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.2.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.2.2E The evaluator shall confirm that the implementation standards have been applied.

9.2.4 ASE Security Target evaluation

9.2.4.1 ASE_CCL Conformance claims

ASE_CCL.1 Conformance claims

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.2 ASE_ECD Extended components definition

ASE_ECD.1 Extended components definition

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

9.2.4.3 ASE_INT ST introduction

ASE_INT.1 ST introduction

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

9.2.4.4 ASE_OBJ Security objectives

ASE_OBJ.2 Security objectives

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.5 ASE_REQ Security requirements

ASE_REQ.2 Derived security requirements

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.6 ASE_SPD Security problem definition

ASE_SPD.1 Security problem definition

ASE_APD.1.1D The developer shall provide a security problem definition.

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.7 ASE_TSS TOE summary specification

ASE_TSS.1 TOE summary specification

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

9.2.5 ATE Tests

9.2.5.1 ATE_COV Coverage

ATE_COV.2 Analysis of coverage

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.5.2 ATE_DPT Depth

ATE_DPT.3 Testing: modular design

ATE_DPT.3.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.3.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and modules in the TOE design.

ATE_DPT.3.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.3.3C The analysis of the depth of testing shall demonstrate that all TSF modules in the TOE design have been tested.

ATE_DPT.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.5.3 ATE_FUN Functional tests

ATE_FUN.1 Functional testing

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.5.4 ATE_IND Independent testing

ATE_IND.2 Independent testing - sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

9.2.6 AVA Vulnerability assessment

9.2.6.1 AVA_VAN Vulnerability analysis

AVA_VAN.5 Advanced methodical vulnerability analysis

AVA_VAN.5.1D The developer shall provide the TOE for testing.

AVA_VAN.5.1C The TOE shall be suitable for testing.

AVA_VAN.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.5.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.5.3E The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.5.4E The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

9.3 Security Requirements Rationale

9.3.1 Objectives

9.3.1.1 Security Objectives for the TOE

All SSCD parts

OT.Lifecycle_Security is provided by the SFR as follows. 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 import according to FDP_UCT.1/SCD in the trusted channel FTP_ITC.1/SCD. Secure SCD/SVD generation is ensured by FCS_CKM.1/SCD/SVD_Generation. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer. The secure SCD usage is ensured cryptographically according to FCS_COP.1/Sign.The SCD usage is controlled by access control FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_MTD.1/UnblockChange_RAD, FMT_MTD.1/Erase_PIN, FMT_SMF.1 and FMT_SMR.1. The test functions FPT_TST.1 provides failure detection throughout the lifecycle. The SFR FCS_CKM.4, ensures a secure SCD desctruction.

OT.SCD_Secrecy is provided by the security functions specified by the following SFR. FDP_UCT.1/SCD and FTP_ITC.1/SCD ensures the confidentiality for SCD import. FCS_CKM.1/SCD/SVD_Generation ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information. The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA). SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

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

OT.Sigy_SigF is provided by an SFR for identification authentication and access control. FIA_UAU.1 and FIA_UID.1 ensure that no signature creation function can be invoked before

the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. SFR FIA_AFL.1/RAD provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS. The security functions specified by FDP_ACC.1/Signature_Creation and FDP_ACF.1/Signature_Creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory. FMT_MOF.1 restricts the ability to enable the signature creation function to the signatory. FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory. Furthermore, FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process) and ensures that no attacker can get hold of the SCD (to create signatures outside the TOE) once SCD has been deleted by the legitimate signatory. FMT_MTD.1/Unblock_PIN and FMT_MTD.1/UnblockChange_RAD ensure the unblocking of the PIN (including the RAD) is made under the sole control of the administrator. In phase 6, the RAD may be loaded on the TOE by the Personalization Agent as defined in FMT_SMF.1. The Personalization Agent is authenticated with a mutual authentication performed with FCS_RND.1 and FCS_COP.1/GP, and is authenticated with FMT_SMR.1. During the mutual authentication, a session encryption key is agreed between the TOE and the Personalization Agent and used by the TOE to decrypt the RAD using FCS_COP.1/GP Secret Data Protection, ensuring the confidentiality of the RAD during its transfer in phase 6. In phase 6, FMT_MSA.1/ Signatory guarantees that the Personalization Agent cannot sign on behalf of the signatory, ensuring the signature creation features remains under the sole control of the signatory.

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

OT.EMSEC_Design covers that no intelligible information is emanated. This is provided by FPT_EMS.1.1 and FPT_EMS.1/PIN-PUK-KEYS.

OT.Tamper_ID is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

OT.Tamper_Resistance is provided by FPT_PHP.3 to resist physical attacks.

SSCD parts 2, 4 and 5 only

OT.SCD/SVD_Auth_Gen addresses that generation of a SCD/SVD pair requires proper user authentication. FIA_UAU.1 and FIA_UID.1 provide user identification and user authentication prior to enabling access to authorized functions. The SFR FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute

initialization. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute "SCD operational" of the SCD.

OT.SCD_Unique implements the requirement of practically unique SCD as laid down in Annex III, paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1/SCD/SVD_Generation.

OT.SCD_SVD_Corresp addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1/SCD/SVD_Generation to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT_SMF.1 and by FMT_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

SSCD parts 3 and 6 only

OT.SCD_Auth_Imp is provided by the security functions specified by the following SFR. FIA_UID.1 and FIA_UAU.1 ensure that the user is identified and authenticated before SCD can be imported. FDP_ACC.1/SCD_Import and FDP_ACF.1/SCD_Import ensure that only authorised users can import SCD.

SSCD part 4 only

OT.TOE_SSCD_Auth requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by FIA_API.1 (Authentication proof of identity). The SFR FIA_UAU.1 allows establishment of the trusted channel before (human) user is authenticated.

OT.TOE_TC_SVD_Exp requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA, which is directly provided by

- The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer
- FDP_DAU.2/SVD (Data authentication with identity of guarantor), which requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.
- FTP_ITC.1/SVD (inter-TSF trusted channel), which requires the TOE to provide a trusted channel to the CGA.

SSCD parts 5 and 6 only

OT.TOE_TC_VAD_Imp is provided by FTP_ITC.1/VAD to provide a trusted channel to protect the VAD provided by the HID to the TOE.

OT.TOE_TC_DTBS_Imp is provided by FTP_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by FDP_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS.

Additional Security Objectives for the TOE

OT.Identification The security objective OT.Identification addresses the storage of Initialisation and Pre-Personalisation Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialisation and Pre-personalisation Data (including the Personalisation Agent key). The SFR FMT_MTD.1/INI_DIS requires the Personalisation Agent to disable access to Initialisation and Pre-personalisation Data in the life cycle phase 'operational use'.The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and the roles related.

OT.Authentication_Secure is provided by FCS_RND.1 and FCS_COP.1/GP for the authentication of the Personalization agent. The use of a challenge freshly generated by the TOE with FCS_RND.1 in theses authentication protocols ensures a protection against replay attacks when authenticating external entities. The security function specified by FPT_TST.1 ensures that the security functions are performed correctly and FDP_SDI.2/Persistent guarantees the integrity of the authentication key(s) used by the TOE. FMT_SMR.1 and FMT_SMF.1 ensure the TOE can distinguish between external entities successfully authenticated (R.Admin) and can grant them dedicated rights. In case of authentication protocols involving the import of ephemeral public key on the TOE (using Card verifiable certificates), FDP_RIP.1 ensures that the key value is not kept by the TOE after usage and then can not be reused for a replay attack. This objective ensures as well the establishment of a trusted channel following a successful mutual authentication. This trusted channel ensures authenticity, integrity and confidentiality of communication. FCS_CKM.1/Session Keys generate session keys for the secure communication from a common secret agreed between the TOE and the external entity during the mutual authentication procedure. Any incoming command shall contain a MAC computed by the issuer with the session key agreed during the mutual authentication, so that any unauthenticated or non integer command is detected by the MAC verification performed by the TOE using FCS_COP.1/SM in Integrity. The data exchanged through this trusted channel are also protected in confidentiality thanks to FCS_COP.1/SM in Confidentiality, ensuring they can only be disclosed to the parties authenticated during the mutual authentication step. The encryption key is ephemeral as it is generated during the mutual authentication using a challenge freshly generated by the TOE using FCS_RND.1, which ensures that dictionary attacks cannot be performed on encrypted data. When an integrity error is detected, or if the MAC is wrong (wrong authentication of the command issuer), the session keys (for integrity and confidentiality) are erased thanks to FCS_CKM.4 so that they cannot be reused anymore, causing the trusted channel to be irreversibly lost. In particular, it ensures that encrypted data that may be caught by an attacker cannot be reused anymore to masquerade the TOE. In phase 6, the integrity and confidentiality of data is ensured by

FCS_COP.1/GP Secret Data Protection. The SSCD provides a proof of identity with FIA_API.1. This objective ensures as well that any authentication key is loaded in the TOE by an authenticated user, so that only genuine keys associated to genuine users are declared to the TOE. The key import defined by FMT_SMF.1 is protected by access control. It is protected by the proper Agent(s) authentication that cannot be bypassed to access these functions with the TSF specified by FIA_UID.1 and FIA_UAU.1. The agent entitled to load the authentication key is (are) authenticated with FMT_SMR.1. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1/RAD. This objective ensures the verification of the authenticity of the TOE as a whole device. This objective is mainly achieved by FIA_API.1/TOE Authentication using FCS_CKM.1/DH_PACE. CA provides an evidence of possessing the Chip Authentication Private Key (CAPK). FMT_MTD.1/CAPK governs creating/loading CAPK, whereas FMT_MTD.1/KEY_READ requires making this key unreadable by users. Hence, its value remains confidential. FDP_RIP.1 requires erasing the values of CAPK and the session keys, here for CMAC. The authentication token is calculated using FCS_COP.1/SM in Integrity. The TOE holder provides a proof of identity with FIA_API.1/TOE Authentication. This objective aims to explicitly protect sensitive (as opposed to common) user and TSF-Data. This is mainly achieved by enforcing (FDP_UCT.1/TRM and FDP_UIT.1/TRM) the access control SFPs FDP_ACC.1/TRM and FDP_ACF.1/TRM. A specific authorization level is achieved by terminal identification/authentication as required by the SFRs FIA_UID.1/PACE, FIA_UAU.1/PACE supported by FCS_COP.1/SIG_VER. The TA protocol uses the result of the PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE, confidentiality of the PACE passwords is ensured by FMT_MTD.1/KEY_READ) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA_AFL.1/AUTH, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/UnblockChange_RAD, FMT_MTD.1/Erase_PIN, FMT_MTD.1/Reinitialize_PIN, FMT_MTD.1/UnblockChange_PUK) also support to achieve this objective. FDP_RIP.1 requires erasing the temporal values of the PIN and PUK. FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE and FCS_CKM.4 represent some specific properties of the used protocols. To allow for a verification of the certificate chain as required in FMT_MTD.3, the CVCA's public key and certificate as well as the current date are written or updated by authorized identified role as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. In contactless, this objective for the data exchanged is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/SM in Confidentiality. A prerequisite for establishing this trusted channel is a successful Chip Authentication, cf. FIA_API.1/TOE Authentication using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, and FIA_UAU.6/EAC. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA_UID.1/PACE, FIA_UAU.1/PACE and FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE. CA provides an evidence of possessing the Chip Authentication Private Key (CAPK). FMT_MTD.1/CAPK governs creating/loading CAPK, FMT_MTD.1/KEY_READ requires making this key unreadable by users. Thus its value remains confidential. FDP_RIP.1 requires erasing the values of CAPK and session keys, here for KENC. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles. This objective ensures also the authenticity of user- and TSF-Data (after Terminal- and the Chip Authentication) by enabling its verification on both the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by FTP_ITC.1/PACE in contactless using FCS_COP.1/SM in Integrity. A prerequisite for establishing this trusted channel is a successful Chip Authentication, cf. FIA_API.1/TOE Authentication using

FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, and FIA_UAU.6/EAC. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA_UID.1/PACE, FIA_UAU.1/PACE and FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE. CA provides an evidence of possessing the Chip Authentication Private Key (CAPK). FMT_MTD.1/CAPK governs creating/loading CAPK, FMT_MTD.1/KEY_READ requires to make this key unreadable by users. Hence its value remains confidential. FDP_RIP.1 requires to erase the values of CAPK and session keys, here for KMAC. A prerequisite for successful CA is an accomplished TA as required by FIA_UID.1/PACE, FIA_UAU.1/PACE supported by FCS_COP.1/SIG_VER. The TA protocol uses the result of the PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA_AFL.1/AUTH, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/UnblockChange_RAD, FMT_MTD.1/Erase_PIN, FMT_MTD.1/Reinitialize_PIN, FMT_MTD.1/UnblockChange_PUK) also support achieving this objective. FDP_RIP.1 requires to erase the temporal values of the PIN and PUK. FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC and FCS_CKM.4 represent some specific required properties of the used protocols.To allow for a verification of the certificate chain as required in FMT_MTD.3, the CVCA's public key and certificate, as well as the current date, are written or updated by authorized identified roles as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles. This objective ensures the confidentiality of the user- and TSF-Data stored and, after Terminal- and Chip Authentication, of their exchange. This objective for the data stored is mainly achieved by FDP_ACC.1/TRM and FDP_ACF.1/TRM. Enforcement of the two previous in a protected manner is ensured by FDP_UCT.1/TRM and FDP_UIT.1/TRM. A specific authorization level is achieved by terminal identification/authentication as required by the SFRs FIA_UID.1/PACE, FIA_UAU.1/PACE supported by FCS_COP.1/SIG_VER. The TA protocol uses the result of the PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE, confidentiality of the PACE passwords is ensured by FMT_MTD.1/KEY_READ) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA_AFL.1/AUTH, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/UnblockChange_RAD, FMT_MTD.1/Erase_PIN, FMT_MTD.1/Reinitialize_PIN, FMT_MTD.1/UnblockChange_PUK) also support to achieve this objective. FDP_RIP.1 requires erasing the temporal values of the PIN and PUK.FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE and FCS_CKM.4 represent some specific properties of the used protocols.To allow for a verification of the certificate chain as required in FMT_MTD.3, the CVCA's public key and certificate as well as the current date are written or updated by authorized identified role as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. This objective for the data exchanged is mainly achieved in contactless by FTP_ITC.1/PACE using FCS_COP.1/SM in Confidentiality. A prerequisite for establishing this trusted channel is a successful Chip Authentication, cf. FIA_API.1/TOE Authentication using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, and FIA_UAU.6/EAC. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA_UID.1/PACE, FIA_UAU.1/PACE and FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE. CA provides an evidence of possessing the Chip Authentication Private Key (CAPK). FMT_MTD.1/CAPK governs creating/loading CAPK, FMT_MTD.1/KEY_READ requires making this key unreadable by users. Thus its value

remains confidential. FDP_RIP.1 requires erasing the values of CAPK and session keys, here for KENC. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles. This objective ensures the integrity of stored user- and TSF-Data and, after Terminal- and Chip Authentication, of these data exchanged (physical manipulation and unauthorized modifying). Physical manipulation is addressed by FPT_PHP.3.Unauthorized modifying of the stored data is addressed by FDP_ACC.1/TRM and FDP_ACF.1/TRM. Enforcement of the two previous in a protected manner is ensured by FDP_UCT.1/TRM and FDP_UIT.1/TRM. A specific authorization level is achieved by terminal identification/ authentication as required by the SFRs FIA_UID.1/PACE, FIA_UAU.1/PACE supported by FCS_COP.1/SIG_VER. The TA protocol uses the result of PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) being, in turn, supported by FCS_CKM.1.1/DH_PACE. Since PACE can use the PIN as the shared secret, using and management of PIN (FIA_AFL.1/AUTH, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN FMT_MTD.1/Initialize_PIN, FMT_MTD.1/UnblockChange_RAD, FMT_MTD.1/Erase_PIN, FMT_MTD.1/Reinitialize_PIN, FMT_MTD.1/UnblockChange_PUK) also support achievement of this objective. FDP_RIP.1 requires erasing the temporal values of PIN, PUK. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the used protocols. To allow for a verification of the certificate chain as required in FMT_MTD.3, the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. Unauthorized modifying of the exchanged data is addressed by FTP_ITC.1/PACE in contactless using FCS_COP.1/SM in integrity. A prerequisite for establishing this trusted channel is a successful Chip Authentication, cf. FIA_API.1/TOE Authentication using FCS_CKM.1/DH_PACE possessing the special properties FIA_UAU.5/PACE and FIA_UAU.6/EAC. As a prerequisite of this trusted channel a trusted channel established with the PACE protocol using FIA_UID.1/PACE, FIA_UAU.1/PACE and FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE. CA provides an evidence of possessing the Chip Authentication Private Key (CAPK). FMT_MTD.1/CAPK governs creating/loading CAPK, and FMT_MTD.1/KEY_READ requires CAPK to be unreadable by users; thus its value remains confidential. FDP_RIP.1 requires erasing the values of CAPK and session keys (here: for KMAC). The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support related functions and roles. This objective prevents TOE's functions being not intended to be used in the operational phase from manipulating and disclosing the User- and TSF-data. This objective is achieved by FMT_LIM.1 and FMT_LIM.2 preventing misuse of test and other functionality of the TOE having not to be used in the TOE's operational life cycle phase. This objective protects against disclosure of confidential User- or/and TSF-data stored on / processed by the TOE. This objective is achieved

- by FPT_EMS.1 and FPT_EMS.1/PIN-PUK-KEYS for measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- by FPT_FLS.1 and FPT_TST.1 for forcing a malfunction of the TOE, and
- by FPT_PHP.3 for a physical manipulation of the TOE. This objective ensures a correct operation of the TOE by preventing its operation outside the normal operating conditions. This objective is covered by FPT_TST.1 requiring self tests to demonstrate the correct operation of the TOE and tests of authorised users to verify the integrity of the TSF-data and the embedded software (TSF code) as well as by FPT_FLS.1 requiring entering a secure state of the TOE in case of detected failure or operating conditions possibly causing a malfunction. This objective protects of the confidentiality and integrity of the User- and TSF-data as well as embedded

software stored in the TOE. This objective is completely covered by FPT_PHP.3 in an obvious way.

OT.Key_Lifecycle_Security Secure Keys generation is ensured by FCS_CKM.1/SCD/SVD_Generation. The secure keys usage is ensured cryptographically according to FCS_COP.1/Digital Auth, FCS_COP.1/Enc Key Decipherment. Keys usage is based on the security attribute secure TSF management according to FMT_MSA.2, FMT_MSA.3, FMT_SMF.1 and FMT_SMR.1. The test functions FPT_TST.1 provides failure detection throughout the lifecycle. The SFR FCS_CKM.4 ensures a secure keys destruction.

OT.Keys_Secrecy is provided by the security functions specified by the following SFR. FCS_CKM.1/SCD/SVD_Generation ensure the use of secure cryptographic algorithms for keys generation. Cryptographic quality of the asymmetric key pair(s) shall prevent disclosure of the TOE's private authentication key(s) and eServices key(s) by cryptographic attacks using the publicly known public key. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on a key(s) is destroyed after a key has been used for authentication (verification or proof) or an eServices keys has been used and that destruction of key(s) 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 authentication key. 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). FPT_EMS.1/PIN-PUK-KEYS and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the key(s).

OT.TOE_AuthKey_Unique implements the requirement of practically unique TOE's authentication private key, which is provided by the cryptographic algorithms specified by FCS_CKM.1/SCD/SVD_Generation.

OT.Lifecycle_Management ensures a correct separation of the TOE life cycle between phase 6 and 7. In phase 6, FMT_MTD.1/TOE State ensures the TOE irreversibly switches from phase 6 to phase 7 under the sole control of the Personalization Agent. The Personalization Agent is authenticated with a mutual authentication performed with FCS_RND.1 and FCS_COP.1/GP Secret Data Protection and is authenticated with FMT_SMR.1. In phase 7, FDP_ACC.1/Signature_Creation, FDP_ACC.1/SVD_Transfer, FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/SCD_Import, FDP_ACF.1/Signature_Creation, FDP_ACF.1/SVD_Transfer, FDP_ACF.1/SCD/SVD_Generation, FDP_ACF.1/SCD_Import, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/UnblockChange_RAD, FMT_MTD.1/Erase_PIN, FMT_MOF.1, FMT_MTD.1/Admin, FMT_MTD.1/Signatory ensures the Personalization Agent does not control the TOE anymore. In phase 6, the Personalization Agent has complete control over the administrative functions of the TOE. It may import, erase, generate SCD/SVD, export SVD, manage Keys, create RAD and manage the configuration of the TOE as mandated in FMT_SMF.1, according to the security policies defined in FDP_ACC.1/SVD transfer, FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/SCD import, FDP_ACF.1/SVD transfer, FDP_ACF.1/SCD/SVD_Generation, FDP_ACF.1/SCD import, It may as well change TOE State (FMT_MTD.1/TOE State). These functions are protected by the Personalization Agent authentication that cannot be bypassed to access these functions with the TSF specified by

FIA_UID.1 and FIA_UAU.1. FMT_MSA.1/Admin, FMT_MSA.2, FMT_MSA.3 ensure that the sole Personalization Agent can realize these functions.

OT.eServices is provided by the cryptographic mechanisms specified by (1) FCS_COP.1/Digital Auth, (2) FCS_COP.1/Enc Key Decipherment. These requirements ensure the cryptographic robustness of these eServices. The eServices keys may be loaded, generated, and the matching public key may be exported as required by FMT_SMF.1 and FMT_SMR.1. These functions are protected by the proper Agent(s) authentication that cannot be bypassed to access these functions with the TSF specified by FIA_UID.1/PACE and FIA_UAU.1/PACE. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1/RAD.

OT.AC_Pers_EAC ensures that only the personalization agent can write user- and TSF-Data into the TOE, and that some of this data cannot be altered after personalization. This property is covered by FDP_ACC.1/TRM and FDP_ACF.1/TRM requiring, amongst other, an appropriate authorization level of an Authentication Terminal. This authorization level can be achieved by terminal identification/authentication as required by the SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles. Since only an Authentication Terminal can reach the necessary authorization level, using and managing the PIN (the related SFRs are FIA_AFL.1/AUTH, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/UnblockChange_RAD, FMT_MTD.1/Erase_PIN, FMT_MTD.1/Reinitialize_PIN, FMT_MTD.1/UnblockChange_PUK) also support the achievement of this objective.The justification for the SFRs FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the pre-personalisation data. FDP_RIP.1 requires erasing the temporal values PIN and PUK. Finally, FMT_MTD.1/KEY_READ ensures that cryptographic keys for EAC cannot be read by users.

OT.Tracing ensures that the TOE prevents gathering TOE tracing data by means of unambiguously identifying the electronic document remotely through establishing or listening to communication via the contactless-based interface of the TOE without a priori knowledge of the correct values of shared passwords (MRZ,CAN, PIN, PUK). This objective is achieved by FIA_AFL.1/AUTH and FTP_ITC.1/PACE

OT.ADMIN_Configuration The security objective OT.ADMIN_Configuration "Protection of the TOE administration" addresses management of the Data Configuration with key size management for the Chip Authentication of the TOE. ADMIN keys are created during pre-personalization. FMT_MTD.1/KEY_READ restricts the ability to read the Administrator Keys to none. FPT_EMS.1 protects the confidentially of Administrator Agent keys. The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related. Symmetric authentication is managed through FCS_COP.1/GP Secret Data Protection, FCS_COP.1/SM in Confidentiality and FCS_COP.1/SM in Integrity. The administration TSF data manipulation are supported by FMT_MTD.1/Admin. It is now allowed to configure the Chip Authentication key parameters to be used during key generation in USE phase. The minimum key size that the user can generate in USE phase is controlled by the "ADMIN" role. It is also possible to change the key parameters during the key generation process. For example changing the domain parameters of an elliptic curve key. It is also possible to invalidate one of the Chip Authentication key in USE phase and to set the secondary key as being the primary key. It

is also possible to craete and delete EF files in Use Phase through proper File acees condition been met as defined in FDP_ACC.1/MNG_File and FDP_ACF.1/MNG_File. Note: after such process, the "freed" CA key set is available for a future CA key generation.

OT.Key_Usage_Counter The security objective OT.Key_Usage_Counter is covered by FMT_MTD.1/Key_Usage_Counter.

9.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.Lifecycle_Security	FCS_CKM.1/SCD/SVD_Generation, FCS_CKM.4, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/Signature_Creation, FDP_ACC.1/Signature_Creation, FDP_ACF.1/SVD_Transfer, 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_SMR.1, FMT_SMF.1, FPT_TST.1, FCS_COP.1/Sign, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FDP_ITC.1/SCD, FDP_UCT.1/SCD, FTP_ITC.1/SCD, FMT_MTD.1/Erase_PIN, FMT_MTD.1/UnblockChange_RAD	Section 9.3.1
OT.SCD_Secrecy	FCS_CKM.1/SCD/SVD_Generation, FCS_CKM.4, FDP_RIP.1, FDP_SDI.2/Persistent, FPT_FLS.1, FPT_PHP.3, FPT_TST.1, FDP_UCT.1/SCD, FTP_ITC.1/SCD, FPT_EMS.1	Section 9.3.1
OT.Sig_Secure	FDP_SDI.2/Persistent, FPT_TST.1, FCS_COP.1/Sign	Section 9.3.1
OT.Sigy_SigF	FDP_ACF.1/Signature_Creation, FDP_ACC.1/Signature_Creation, FDP_RIP.1, FDP_SDI.2/DTBS, FIA_AFL.1/RAD, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMR.1, FMT_SMF.1, FCS_COP.1/GP Secret Data Protection, FCS_RND.1, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/UnblockChange_RAD	Section 9.3.1
OT.DTBS_Integrity_TOE	FDP_SDI.2/DTBS	Section 9.3.1
OT.EMSEC_Design	FPT_EMS.1/PIN-PUK-KEYS, FPT_EMS.1	Section 9.3.1
OT.Tamper_ID	FPT_PHP.1	Section 9.3.1

OT.Tamper_Resistance	FPT_PHP.3	Section 9.3.1
OT.SCD/SVD_Auth_Gen	FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FIA_UAU.1, FIA_UID.1, FMT_MSA.1/Admin, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4	Section 9.3.1
OT.SCD_Unique	FCS_CKM.1/SCD/SVD_Generation	Section 9.3.1
OT.SCD_SVD_Corresp	FCS_CKM.1/SCD/SVD_Generation, FDP_SDI.2/Persistent, FMT_MSA.4, FMT_SMF.1	Section 9.3.1
OT.SCD_Auth_Imp	FIA_UID.1, FIA_UAU.1, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import	Section 9.3.1
OT.TOE_SSCD_Auth	FIA_UAU.1, FIA_API.1	Section 9.3.1
OT.TOE_TC_SVD_Exp	FDP_ACF.1/SVD_Transfer, FDP_ACC.1/SVD_Transfer, FDP_DAU.2/SVD, FTP_ITC.1/SVD	Section 9.3.1
OT.TOE_TC_VAD_Imp	FTP_ITC.1/VAD	Section 9.3.1
OT.TOE_TC_DTBS_Imp	FDP_UIT.1/DTBS, FTP_ITC.1/DTBS	Section 9.3.1
OT.Identification	FMT_SMF.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_SMR.1/PACE	Section 9.3.1
OT.Authentication_Secure	FCS_CKM.1/Session Keys, FCS_CKM.1/DH_PACE, FCS_COP.1/GP Secret Data Protection, FCS_COP.1/SM in Confidentiality, FCS_COP.1/SM in Integrity, FCS_COP.1/SIG_VER, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/EAC, FIA_AFL.1/AUTH, FIA_API.1/TOE Authentication, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FTP_ITC.1/PACE, FMT_SMR.1/PACE, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/UnblockChange_RAD, FMT_MTD.1/Erase_PIN, FMT_MTD.1/Reinitialize_PIN, FMT_MTD.1/UnblockChange_PUK, FMT_MTD.3, FMT_LIM.1, FMT_LIM.2, FPT_EMS.1/PIN-PUK-KEYS, FCS_CKM.4, FDP_RIP.1, FDP_SDI.2/Persistent, FIA_UID.1, FIA_UAU.1,	Section 9.3.1

	FIA_API.1, FMT_SMR.1, FMT_SMF.1, FPT_EMS.1, FPT_FLS.1, FPT_PHP.3, FPT_TST.1, FIA_AFL.1/RAD	
OT.Key_Lifecycle_Security	FCS_COP.1/Digital Auth, FCS_COP.1/Enc Key Decipherment, FCS_CKM.1/SCD/SVD_Generation, FCS_CKM.4, FMT_SMR.1, FMT_SMF.1, FMT_MSA.2, FMT_MSA.3, FPT_TST.1	Section 9.3.1
OT.Keys_Secrecy	FPT_EMS.1/PIN-PUK-KEYS, FCS_CKM.1/SCD/SVD_Generation, FCS_CKM.4, FDP_RIP.1, FDP_SDI.2/Persistent, FPT_FLS.1, FPT_PHP.3, FPT_TST.1	Section 9.3.1
OT.TOE_AuthKey_Unique	FCS_CKM.1/SCD/SVD_Generation	Section 9.3.1
OT.Lifecycle_Management	FCS_COP.1/GP Secret Data Protection, FCS_RND.1, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/UnblockChange_RAD, FMT_MTD.1/Erase_PIN, FMT_MTD.1/TOE State, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FIA_UID.1, FIA_UAU.1, FMT_SMR.1, FMT_SMF.1, FMT_MSA.1/Admin, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1/Admin, FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, FMT_MOF.1, FMT_MTD.1/Signatory	Section 9.3.1
OT.eServices	FCS_COP.1/Digital Auth, FCS_COP.1/Enc Key Decipherment, FIA_UID.1/PACE, FIA_UAU.1/PACE, FMT_SMR.1, FMT_SMF.1, FIA_AFL.1/RAD	Section 9.3.1
OT.AC_Pers_EAC	FDP_ACF.1/TRM, FDP_RIP.1, FDP_ACC.1/TRM, FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/KEY_READ, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_AFL.1/AUTH, FMT_MTD.1/UnblockChange_RAD, FMT_MTD.1/Erase_PIN, FMT_MTD.1/Reinitialize_PIN, FMT_MTD.1/UnblockChange_PUK, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS	Section 9.3.1

OT.Tracing	FIA_AFL.1/AUTH, FTP_ITC.1/PACE	Section 9.3.1
OT.ADMIN_Configuration	FMT_MTD.1/KEY_READ, FMT_MTD.1/Admin, FMT_SMF.1, FMT_SMR.1, FPT_EMS.1, FDP_ACC.1/MNG_File, FDP_ACF.1/MNG_File, FCS_COP.1/GP Secret Data Protection, FCS_COP.1/SM in Confidentiality, FCS_COP.1/SM in Integrity	Section 9.3.1
OT.Key_Usage_Counter	FMT_MTD.1/Key_Usage_Counter	Section 9.3.1

Table 22 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FPT_EMS.1	OT.SCD_Secrecy, OT.EMSEC_Design, OT.Authentication_Secure, OT.ADMIN_Configuration
FPT_FLS.1	OT.SCD_Secrecy, OT.Authentication_Secure, OT.Keys_Secrecy
FPT_PHP.1	OT.Tamper_ID
FPT_PHP.3	OT.SCD_Secrecy, OT.Tamper_Resistance, OT.Authentication_Secure, OT.Keys_Secrecy
FPT_TST.1	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure, OT.Authentication_Secure, OT.Key_Lifecycle_Security, OT.Keys_Secrecy
FMT_SMR.1	OT.Lifecycle_Security, OT.Sigy_SigF, OT.Authentication_Secure, OT.Key_Lifecycle_Security, OT.Lifecycle_Management, OT.eServices, OT.ADMIN_Configuration
FMT_SMF.1	OT.Lifecycle_Security, OT.Sigy_SigF, OT.SCD_SVD_Corresp, OT.Identification, OT.Authentication_Secure, OT.Key_Lifecycle_Security, OT.Lifecycle_Management, OT.eServices, OT.AC_Pers_EAC, OT.ADMIN_Configuration
FMT_MOF.1	OT.Lifecycle_Security, OT.Sigy_SigF, OT.Lifecycle_Management
FMT_MSA.1/Admin	OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen, OT.Lifecycle_Management

FMT_MSA.1/Signatory	OT.Lifecycle_Security, OT.Sigy_SigF
FMT_MSA.2	OT.Lifecycle_Security, OT.Sigy_SigF, OT.SCD/SVD_Auth_Gen, OT.Key_Lifecycle_Security, OT.Lifecycle_Management
FMT_MSA.3	OT.Lifecycle_Security, OT.Sigy_SigF, OT.SCD/SVD_Auth_Gen, OT.Key_Lifecycle_Security, OT.Lifecycle_Management
FMT_MSA.4	OT.Lifecycle_Security, OT.Sigy_SigF, OT.SCD/SVD_Auth_Gen, OT.SCD_SVD_Corresp
FMT_MTD.1/Admin	OT.Lifecycle_Security, OT.Sigy_SigF, OT.Lifecycle_Management, OT.ADMIN_Configuration
FMT_MTD.1/Signatory	OT.Lifecycle_Security, OT.Sigy_SigF, OT.Lifecycle_Management
FIA_UID.1	OT.Sigy_SigF, OT.SCD/SVD_Auth_Gen, OT.SCD_Auth_Imp, OT.Authentication_Secure, OT.Lifecycle_Management
FIA_AFL.1/RAD	OT.Sigy_SigF, OT.Authentication_Secure, OT.eServices
FIA_UAU.1	OT.Sigy_SigF, OT.SCD/SVD_Auth_Gen, OT.SCD_Auth_Imp, OT.TOE_SSCD_Auth, OT.Authentication_Secure, OT.Lifecycle_Management
FDP_SDI.2/DTBS	OT.Sigy_SigF, OT.DTBS_Integrity_TOE
FDP_SDI.2/Persistent	OT.SCD_Secrecy, OT.Sig_Secure, OT.SCD_SVD_Corresp, OT.Authentication_Secure, OT.Keys_Secrecy
FDP_RIP.1	OT.SCD_Secrecy, OT.Sigy_SigF, OT.Authentication_Secure, OT.Keys_Secrecy, OT.AC_Pers_EAC
FDP_ACC.1/Signature_Creation	OT.Lifecycle_Security, OT.Sigy_SigF, OT.Lifecycle_Management
FDP_ACF.1/Signature_Creation	OT.Lifecycle_Security, OT.Sigy_SigF, OT.Lifecycle_Management
FCS_COP.1/Sign	OT.Lifecycle_Security, OT.Sig_Secure
FCS_CKM.4	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Authentication_Secure,

	OT.Key_Lifecycle_Security, OT.Keys_Secrecy
FCS_CKM.1/SCD/SVD_Generation	OT.Lifecycle_Security, OT.SCD_Secrecy, OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.Key_Lifecycle_Security, OT.Keys_Secrecy, OT.TOE_AuthKey_Unique
FDP_ACC.1/SVD_Transfer	OT.Lifecycle_Security, OT.TOE_TC_SVD_Exp, OT.Lifecycle_Management
FDP_ACF.1/SVD_Transfer	OT.Lifecycle_Security, OT.TOE_TC_SVD_Exp, OT.Lifecycle_Management
FDP_ACC.1/SCD/SVD_Generation	OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen, OT.Lifecycle_Management
FDP_ACF.1/SCD/SVD_Generation	OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen, OT.Lifecycle_Management
FTP_ITC.1/SCD	OT.Lifecycle_Security, OT.SCD_Secrecy
FDP_UCT.1/SCD	OT.Lifecycle_Security, OT.SCD_Secrecy
FDP_ITC.1/SCD	OT.Lifecycle_Security
FDP_ACC.1/SCD_Import	OT.Lifecycle_Security, OT.SCD_Auth_Imp, OT.Lifecycle_Management
FDP_ACF.1/SCD_Import	OT.Lifecycle_Security, OT.SCD_Auth_Imp, OT.Lifecycle_Management
FTP_ITC.1/SVD	OT.TOE_TC_SVD_Exp
FDP_DAU.2/SVD	OT.TOE_TC_SVD_Exp
FIA_API.1	OT.TOE_SSCD_Auth, OT.Authentication_Secure
FDP_UIT.1/DTBS	OT.TOE_TC_DTBS_Imp
FTP_ITC.1/VAD	OT.TOE_TC_VAD_Imp
FTP_ITC.1/DTBS	OT.TOE_TC_DTBS_Imp
FCS_RND.1	OT.Sigy_SigF, OT.Authentication_Secure, OT.Lifecycle_Management
FCS_CKM.1/DH_PACE	OT.Authentication_Secure
FCS_CKM.1/Session Keys	OT.Authentication_Secure
FCS_COP.1/GP Secret Data Protection	OT.Sigy_SigF, OT.Authentication_Secure, OT.Lifecycle_Management, OT.ADMIN_Configuration

FCS_COP.1/SM in Confidentiality	OT.Authentication_Secure, OT.ADMIN_Configuration
FCS_COP.1/SM in Integrity	OT.Authentication_Secure, OT.ADMIN_Configuration
FCS_COP.1/Digital Auth	OT.Key_Lifecycle_Security, OT.eServices
FCS_COP.1/Enc Key Decipherment	OT.Key_Lifecycle_Security, OT.eServices
FCS_COP.1/SIG_VER	OT.Authentication_Secure
FDP_ACC.1/TRM	OT.Authentication_Secure, OT.AC_Pers_EAC
FDP_ACF.1/TRM	OT.Authentication_Secure, OT.AC_Pers_EAC
FDP_ACC.1/MNG_File	OT.ADMIN_Configuration
FDP_ACF.1/MNG_File	OT.ADMIN_Configuration
FDP_UCT.1/TRM	OT.Authentication_Secure
FDP_UIT.1/TRM	OT.Authentication_Secure
FIA_UID.1/PACE	OT.Authentication_Secure, OT.eServices, OT.AC_Pers_EAC
FIA_UAU.1/PACE	OT.Authentication_Secure, OT.eServices, OT.AC_Pers_EAC
FIA_UAU.4/PACE	OT.Authentication_Secure
FIA_UAU.5/PACE	OT.Authentication_Secure
FIA_UAU.6/PACE	OT.Authentication_Secure
FIA_UAU.6/EAC	OT.Authentication_Secure
FIA_AFL.1/AUTH	OT.Authentication_Secure, OT.AC_Pers_EAC, OT.Tracing
FIA_API.1/TOE Authentication	OT.Authentication_Secure
FMT_SMR.1/PACE	OT.Identification, OT.Authentication_Secure, OT.AC_Pers_EAC
FMT_MTD.1/CVCA_INI	OT.Authentication_Secure
FMT_MTD.1/CVCA_UPD	OT.Authentication_Secure
FMT_MTD.1/DATE	OT.Authentication_Secure
FMT_MTD.1/CAPK	OT.Authentication_Secure
FMT_MTD.1/KEY_READ	OT.Authentication_Secure, OT.AC_Pers_EAC, OT.ADMIN_Configuration
FMT_MTD.1/Key_Usage_Counter	OT.Key_Usage_Counter

FMT_MTD.1/Initialize_PIN	OT.Authentication_Secure, OT.AC_Pers_EAC
FMT_MTD.1/Resume_PIN	OT.Authentication_Secure, OT.AC_Pers_EAC
FMT_MTD.1/Change_PIN	OT.Authentication_Secure, OT.AC_Pers_EAC
FMT_MTD.1/Unblock_PIN	OT.Sigy_SigF, OT.Authentication_Secure, OT.Lifecycle_Management, OT.AC_Pers_EAC
FMT_MTD.1/UnblockChange_RAD	OT.Lifecycle_Security, OT.Sigy_SigF, OT.Authentication_Secure, OT.Lifecycle_Management, OT.AC_Pers_EAC
FMT_MTD.1/Erase_PIN	OT.Lifecycle_Security, OT.Authentication_Secure, OT.Lifecycle_Management, OT.AC_Pers_EAC
FMT_MTD.1/Reinitialize_PIN	OT.Authentication_Secure, OT.AC_Pers_EAC
FMT_MTD.1/UnblockChange_PUK	OT.Authentication_Secure, OT.AC_Pers_EAC
FMT_MTD.1/TOE State	OT.Lifecycle_Management
FMT_MTD.3	OT.Authentication_Secure
FMT_MTD.1/INI_ENA	OT.Identification, OT.AC_Pers_EAC
FMT_MTD.1/INI_DIS	OT.Identification, OT.AC_Pers_EAC
FMT_LIM.1	OT.Authentication_Secure
FMT_LIM.2	OT.Authentication_Secure
FPT_EMS.1/PIN-PUK-KEYS	OT.EMSEC_Design, OT.Authentication_Secure, OT.Keys_Secrecy
FTP_ITC.1/PACE	OT.Authentication_Secure, OT.Tracing

Table 23 SFRs and Security Objectives

9.3.3 Dependencies

9.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCS_RND.1	No Dependencies	

FCS_CKM.1/DH_PACE	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/SM in Confidentiality, FCS_COP.1/SM in Integrity, FCS_CKM.4
FCS_CKM.1/Session Keys	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/SM in Confidentiality, FCS_COP.1/SM in Integrity, FCS_CKM.4
FCS_COP.1/GP Secret Data Protection	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/Session Keys, FCS_CKM.4
FCS_COP.1/SM in Confidentiality	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/Session Keys, FCS_CKM.4
FCS_COP.1/SM in Integrity	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/Session Keys, FCS_CKM.4
FCS_COP.1/Digital Auth	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/SCD/SVD_Generation
FCS_COP.1/Enc Key Decipherment	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/SCD/SVD_Generation
FCS_COP.1/SIG_VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/SCD/SVD_Generation
FDP_ACC.1/TRM	(FDP_ACF.1)	FDP_ACF.1/TRM
FDP_ACF.1/TRM	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/TRM, FMT_MSA.3
FDP_ACC.1/MNG_File	(FDP_ACF.1)	FDP_ACF.1/TRM
FDP_ACF.1/MNG_File	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/TRM, FMT_MSA.3
FDP_UCT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/TRM, FTP_ITC.1/PACE
FDP_UIT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and	FDP_ACC.1/TRM, FTP_ITC.1/PACE

	(FTP_ITC.1 or FTP_TRP.1)	
FIA_UID.1/PACE	No Dependencies	
FIA_UAU.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FIA_UAU.4/PACE	No Dependencies	
FIA_UAU.5/PACE	No Dependencies	
FIA_UAU.6/PACE	No Dependencies	
FIA_UAU.6/EAC	No Dependencies	
FIA_AFL.1/AUTH	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_API.1/TOE Authentication	No Dependencies	
FMT_SMR.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FMT_MTD.1/CVCA_INI	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/CVCA_UPD	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/DATE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/CAPK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/Key_Usage_Counter	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/Initialize_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/Resume_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/Change_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/Unblock_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/UnblockChange_RAD	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/Erase_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/Reinitialize_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1

FMT_MTD.1/UnblockChange_PUK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.1/TOE State	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE, FMT_SMF.1
FMT_MTD.3	(FMT_MTD.1)	FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE
FMT_MTD.1/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_LIM.1	(FMT_LIM.2)	FMT_LIM.2
FMT_LIM.2	(FMT_LIM.1)	FMT_LIM.1
FPT_EMS.1/PIN-PUK-KEYS	No Dependencies	
FTP_ITC.1/PACE	No Dependencies	
FPT_EMS.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_PHP.1	No Dependencies	
FPT_PHP.3	No Dependencies	
FPT_TST.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FMT_SMF.1	No Dependencies	
FMT_MOF.1	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1, FDP_ACC.1/Signature_Creation, FDP_ACC.1/SVD_Transfer, FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/SCD_Import
FMT_MSA.1/Signatory	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1, FDP_ACC.1/Signature_Creation
FMT_MSA.2	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD/SVD_Generation
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory

FMT_MSA.4	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD/SVD_Generation
FMT_MTD.1/Admin	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FIA_UID.1	No Dependencies	
FIA_AFL.1/RAD	(FIA_UAU.1)	FIA_UAU.1
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FDP_SDI.2/DTBS	No Dependencies	
FDP_SDI.2/Persistent	No Dependencies	
FDP_RIP.1	No Dependencies	
FDP_ACC.1/Signature_Creation	(FDP_ACF.1)	FDP_ACF.1/Signature_Creation
FDP_ACF.1/Signature_Creation	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/Signature_Creation
FCS_COP.1/Sign	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/SCD/SVD_Generation, FDP_ITC.1/SCD
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/SCD/SVD_Generation, FDP_ITC.1/SCD
FCS_CKM.1/SCD/SVD_Generation	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/Sign, FCS_CKM.4
FDP_ACC.1/SVD_Transfer	(FDP_ACF.1)	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SVD_Transfer	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SVD_Transfer
FDP_ACC.1/SCD/SVD_Generation	(FDP_ACF.1)	FDP_ACF.1/SCD/SVD_Generation
FDP_ACF.1/SCD/SVD_Generation	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SCD/SVD_Generation
FTP_ITC.1/SCD	No Dependencies	
FDP_UCT.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FTP_ITC.1/SCD, FDP_ACC.1/SCD_Import
FDP_ITC.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SCD_Import

FDP_ACC.1/SCD_Import	(FDP_ACF.1)	FDP_ACF.1/SCD_Import
FDP_ACF.1/SCD_Import	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SCD_Import
FTP_ITC.1/SVD	No Dependencies	
FDP_DAU.2/SVD	(FIA_UID.1)	FIA_UID.1
FIA_API.1	No Dependencies	
FDP_UIT.1/DTBS	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FTP_ITC.1/VAD	No Dependencies	
FTP_ITC.1/DTBS	No Dependencies	

Table 24 SFRs Dependencies

9.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	(ADV_IMP.1) and (ADV_TDS.1)	ADV_IMP.1, ADV_TDS.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	(ADV_FSP.5)	ADV_FSP.5
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.5
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.5, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_FLR.1	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.2	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	

ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	(ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3

Table 25 SARs Dependencies

9.3.4 Rationale for the Security Assurance Requirements

The assurance level for this Security Traget is EAL5 augmented. EAL5 allows a developer to attain a reasonably high assurance level without the need for highly specialised 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. Augmentation results from the selection of:

AVA_VAN.5 Advanced methodical vulnerability analysis ALC_DVS.2 Sufficiency of security measures ALC_FLR.1 Basic flaw remediation

9.3.5 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 applications, i.e. the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. Insecure states shall be easy to detect and the TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF, OT.Sig_Secure and OT.Keys_Secrecy. This assurance requirement is achieved by the AVA_VAN.5 component. Independent vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication.

9.3.6 ALC_DVS.2 Sufficiency of security measures

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

9.3.7 ALC_FLR.1 Basic flaw remediation

The flaw remediation assurance improves a rigourous management for updating the TOE in the context of sensible market.

10 TOE Summary Specification

10.1 TOE Summary Specification

This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The summary is structured in security functions. The security functionalities concerning the IC and the JC Platform are described in [ST_PTF] and are not redefined in this security target, although they must be considered for the TOE.

The TOE inherits all the security functions provided by the underlying javacard open platform [ST_PTF]. On top of these, it adds some supplemental security functions that are described hereafter.

SF.PIN_MGT

This security function is involved in the management of the PINs (PIN, PUK and RAD). PINs are secret data used so that a natural person can authenticate itself to the TOE. This security function:

- Provides all management operations on these PINs (verification, change, unblocking, unblocking and change, initialization, re-initialization) and
- Enforces the access control policies over these operations. The natural person can authenticate itself to the TOE via the PACE protocol and/or the VERIFY PIN command. Take note that the usage of PACE protocol is mandatory only for contactless mode unless compliance to PP-SSCD5 and/or PP-SSCD6 is required, then usage of PACE protocol becomes mandatory for both contact and contactless mode. The verification process uses a velocity checking mechanism, thus a remaining try counter and a maximum error counter are defined for each PIN. If the verification fails, the try counter is decremented by one and an error status that contains the remaining attempts is returned by the application. When all available tries have failed, the PIN is suspended or blocked and can no longer be used. Note that a successful verification of the PIN resets its remaining try counter to the maximum error counter.

SF.SIG

This security function manages the signature creation service.

It enforces access control over the signature creation service:

- In phase 6, it ensures the signature computation function is not accessible, and in particular that the personalization agent cannot sign on behalf of the Signatory.
- In phase 7, it ensures the signature creation feature is activated only by the signatory. Also it enforces the integrity of DTBS, and ensures that R.Sigy is successfully authenticated before creating the signature.

The security function ensures the data hashing (if hash on card, or partial hashing is used), and the secure signature computation using the private key (SCD), either with RSA or EC-DSA cryptography. This security function relies on SF.PIN_MGT to authenticate the Signatory.

SF.AUTH

This security function manages the authentication protocols supported by the TOE. This security function supports the authentication with the personalization agent in phase 6. This authentication relies on a mutual authentication protocol authenticating

- the TOE to the personalization agent, and
- the personalization agent to the TOE. It relies on symmetric master key sets shared by the TOE and the personalization agent that may be DES or AES symmetric keys (depending on the type of Secure Channel Protocol – SCP). Upon successful completion of the authentication, both parties (TOE and personalization agent) generate session keys that may be used to establish a secure channel thanks to SF.SM. This secure channel allows protecting the communication between them in integrity, authenticity and confidentiality. Each symmetric master key sets is associated to an error counter, which aims at ensuring its protecting against brute force attacks. Upon each wrong authentication attempt, the authentication processing time is slowed down (exponentially). Once a successful authentication takes place, the slow down mechanisms is cancelled. In phase 7, this security function also supports the PACE protocol. This protocol is a human to machine authentication protocol allowing to
- authenticate a natural person to the TOE by using a PIN or
- prove the holder has the TOE in hand (using MRZ or CAN) and
- creating a secure channel between the TOE and a device used to initiate the communication. This protocol is designed to protect the secrecy of the PIN in the course of the authentication so that it can't be intercepted during the communication, or deduced through crypto analysis. Upon successful completion of PACE authentication, session keys used to establish a secure channel thanks to SF.SM are generated. This secure function also manage error counter on the credentials used to perform the authentication.
- Upon failure, the error counter of the credentials used to initiate the PACE authentication is decreased until it is blocked.
- Once blocked, a secret credential (PINs) can't be used anymore to perform a PACE protocol, while for MRZ or CAN, the PACE protocol is slowed down.
- Upon successful PACE authentication, the error counter of the credentials used to initiate the PACE authentication is reset to its maximum value; Last but not least, this security function also handles the suspension mechanisms protecting the PINs against Denial Of services attacks (not applicable to MRZ and CAN). When the remaining number of tries is set to '1', any attempt to perform a PACE authentication using a PIN credential will require it to be made through a secure channel generated using PACE authentication performed using the CAN.

The PACE protocol is used to establish a trusted channel with the SCA.

In phase 7, this security function also supports authentication of a natural person to the TOE by using a PIN through the VERIFY command.

In phase 7, this security function also supports the Extended Access Control protocol (EAC) made up with Chip authentication (CA) and Terminal Authentication (TA). This protocol allows

- a mutual authentication between the TOE and a remote terminal, and
- the generation of session keys used to establish a secure channel thanks to SF.SM. This secure channel protects the communication between them in integrity,

authenticity and confidentiality. This authentication is based on PKI scheme: each party (TOE and remote terminal) uses

- an authentication private key and
- digital certificates containing the corresponding authentication public key and linking it to the root of trust known by the other party, to authenticate itself to the other party. This security function manages the verification and processing of the certificates received from the remote terminal (that have a specific format named Card Verifiable Certificate – CVC). In particular, this security function computes the effective authorization of the remote terminal. The Extended Access Control (EAC) protocol or GP Authentication is used to establish a trusted channel with the CGA prior to SCD/SVD generation. In phase 7, this security function also provides mechanisms to authenticate the SSCD and prove its identity (thanks to the Chip Authentication mechanism described above).

SF.SM

This security function ensures the protection of communication between the TOE and an external entity. As such, this security function maintains a trusted channel between the TOE and an external entity. This security function requires the TOE and the external entity to establish first a trusted channel using an authentication supported by SF.AUTH. This security function ensures the following properties:

- In phase 6, it ensures the confidentiality, integrity and authenticity of the private keys (including the SCD), and the PINs (including the RAD);
- In phase 6, it ensures the integrity and authenticity of the asymmetric public key (including the SVD) when being exported to the outside
- In phase 7, it ensures the confidentiality, integrity and authenticity of communication between the TOE and the external entity with which an authentication was performed; In phase 6, the confidentiality, integrity and authenticity of communication is ensured by symmetric cryptography. Sensitive data (such as SCD or PINs) are encrypted using a dedicated symmetric session keys for data encryption generated from the seed agreed during the authentication with the personalization agent (see SF.AUTH). On top of that, data are encrypted and signed using symmetric session keys generated from the seed agreed during the authentication with the personalization agent (see SF.AUTH). In phase 7, the confidentiality, integrity and authenticity of communication is ensured by symmetric cryptography. Data are encrypted and signed using symmetric session keys generated from the seed agreed during the Extended Access Control (EAC) or PACE protocol (see SF.AUTH). Moreover, the protection against replay attacks is ensured by the Message Authentication Code (MAC) which is computed using a dynamic ICV, incremented at each new command. This security function is also in charge of:
- generating the session keys from the seed computed by SF.AUTH. These session keys are ephemeral and unique, as the seed is computed from random numbers generated by the TOE and the external entity.
- destroying the session keys in case an error is detected (data not authentic or not integer), or when a command in plain text is sent.
- providing CGA the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence. This security function supports SF.AUTH to prove the identity of the SSCD and the TOE holder.

SF.KEY_MGT

This security function is involved in the management of the asymmetric keys (including SCDs and SVDs). It enforces access control over any management operation on the keys:

- In phase 6, it only allows the key (including the SCD) to be loaded, generated and exported (for the public keys) by the personalization agent. It also requires the private keys to be encrypted in order to ensure their confidentiality. This security function ensures the personalization agent (1) can't use the keys it has loaded or generated. and (2) can't impersonate the associated role (in case of authentication keys), or create a signature with the SCD;
- In phase 7, it allows managing all the keys (including the SCD) by providing generation and export of the corresponding public key. It also enforces access control policies on these operations.

This security function also ensures that after update or generation, the former key (including SCD and SVD) is securely destroyed.

SF.CONF

This security function manages the configuration of the TOE in phase 6. For instance it allows the modification of the TOE State in phase 6. This security function ensures an access control over these operations. Only the successfully authenticated Personalization Agent can modify these attributes. This security function relies on SF.AUTH to authenticate the personalization agent.

SF.ESERVICE

This security function enables to perform digital authentication and electronic services. It is active in phase 7. This security function offers the following services:

- Digital authentication;
- Decryption key decipherment; This security function relies on SF.KEY_MGT which provides management of the keys on which these services rely.

SF.SAFESTATE_MGT

This security function ensures the TOE is always in a safe state. It monitors the integrity of the TOE, its assets and the TSF data by performing self-tests. When an unexpected event occurs (loss of power, loss of integrity, tearing,…), it ensures

- the TOE returns in a safe state
- all sensitive data are erased
- the TOE returns in a restrictive secure state When a major issue is detected, the security function ensures the destruction of the TOE, so that the assets are not accessible anymore.

SF.PHYS

This security function protects the TOE against physical attacks, so that the integrity and confidentiality of the TOE is ensured, including keys, user data, CPLC data, configuration data and TOE life cycle. It detects physical tampering, responds automatically and also controls the emanations sent out by the TOE. It furthermore prevents deploying test features after TOE delivery.

SF.ADMIN

This security functionality ensures that the TOE, when delivered to the Administration Agent, provides and requires authentication for data exchange.

This function allows during Use phase to:

- Manage symmetric authentication using Administration Agent keys,
- Configure the size or value of the Chip Authentication key to be modified in USE phase,
- Change the key parameters during the key generation process,
- Read that Proof that a key has been on board generated,
- Create or Delete Files in Use Phase,
- Invalidate one of the Chip Authentication key in USE phase and to set the secondary key as being the primary key

10.2 SFRs and TSS

10.2.1 SFRs and TSS - Rationale

All SSCD parts

Protection of the TSF (FPT)

FPT_EMS.1 is met by SF.PHYS

FPT_FLS.1 is met by SF.SAFESTATE_MGT

FPT_PHP.1 is met by SF.PHYS

FPT_PHP.3 is met by SF.PHYS

FPT_TST.1 is met by SF.SAFESTATE_MGT

Security management (FMT)

FMT_SMR.1 is met by SF.PIN_MGT and SF.AUTH

FMT_SMF.1 is met by SF.PIN_MGT, SF.SIG, SF.AUTH, SF.KEY_MGT and SF.CONF

FMT_MOF.1 is met by SF.SIG

FMT_MSA.1/Admin is met by SF.AUTH

FMT_MSA.1/Signatory is met by SF.SIG

FMT_MSA.2 is met by SF.SIG, SF.AUTH, SF.KEY_MGT and SF.CONF

FMT_MSA.3 is met by SF.SIG, SF.AUTH, SF.KEY_MGT and SF.CONF

FMT_MSA.4 is met by SF.SIG, SF.AUTH and SF.KEY_MGT

FMT_MTD.1/Admin is met by SF.ADMIN

FMT_MTD.1/Signatory is met by SF.PIN_MGT

Identification and authentication (FIA)

FIA_UID.1 is met by SF.PIN_MGT, SF.SIG, SF.AUTH and SF.KEY_MGT

FIA_AFL.1/RAD is met by SF.PIN_MGT

FIA_UAU.1 is met by SF.PIN_MGT, SF.SIG, SF.AUTH and SF.KEY_MGT

User data protection (FDP)

FDP_SDI.2/DTBS is met by SF.SIG and SF.SAFESTATE_MGT

FDP_SDI.2/Persistent is met by SF.SAFESTATE_MGT

FDP_RIP.1 is met by SF.SAFESTATE_MGT

FDP_ACC.1/Signature_Creation is met by SF.SIG

FDP_ACF.1/Signature_Creation is met by SF.SIG

Cryptographic support (FCS)

FCS_COP.1/Sign is met by SF.SIG

FCS_CKM.4 is met by SF.KEY_MGT

SSCD parts 2, 4 and 5 only

Cryptographic support (FCS)

FCS_CKM.1/SCD/SVD_Generation is met by SF.KEY_MGT

User data protection (FDP)

FDP_ACC.1/SVD_Transfer is met by SF.KEY_MGT

FDP_ACF.1/SVD_Transfer is met by SF.KEY_MGT

FDP_ACC.1/SCD/SVD_Generation is met by SF.KEY_MGT

FDP_ACF.1/SCD/SVD_Generation is met by SF.KEY_MGT

SSCD parts 3 and 6 only

Trusted path/channels (FTP)

FTP_ITC.1/SCD is met by SF.AUTH and SF.SM

User data protection (FDP)

FDP_UCT.1/SCD is met by SF.SM

FDP_ITC.1/SCD is met by SF.KEY_MGT

FDP_ACC.1/SCD_Import is met by SF.KEY_MGT

FDP_ACF.1/SCD_Import is met by SF.KEY_MGT

SSCD part 4 only

Trusted path/channels (FTP)

FTP_ITC.1/SVD is met by SF.AUTH and SF.SM

User data protection (FDP)

FDP_DAU.2/SVD is met by SF.SM

Identification and authentication (FIA)

FIA_API.1 is met by SF.AUTH and SF.SM

SSCD parts 5 and 6 only

User data protection (FDP)

FDP_UIT.1/DTBS is met by SF.SIG

Trusted path/channels (FTP)

FTP_ITC.1/VAD is met by SF.PIN_MGT

FTP_ITC.1/DTBS is met by SF.SM

Additional SFRs

FCS_RND.1 is met by SF.AUTH

FCS_CKM.1/DH_PACE is met by SF.AUTH

FCS_CKM.1/Session Keys is met by SF.SM

FCS_COP.1/GP Secret Data Protection is met by SF.AUTH and SF.SM

FCS_COP.1/SM in Confidentiality is met by SF.AUTH and SF.SM

FCS_COP.1/SM in Integrity is met by SF.AUTH and SF.SM

FCS_COP.1/Digital Auth is met by SF.ESERVICE

FCS_COP.1/Enc Key Decipherment is met by SF.ESERVICE

FCS_COP.1/SIG_VER is met by SF.AUTH and SF.SM

FDP_ACC.1/TRM is met by SF.AUTH and SF.SM

FDP_ACF.1/TRM is met by SF.AUTH and SF.SM

FDP_ACC.1/MNG_File is met by SF.AUTH and SF.SM

FDP_ACF.1/MNG_File is met by SF.AUTH and SF.SM

FDP_UCT.1/TRM is met by SF.AUTH, SF.SM and SF.KEY_MGT

FDP_UIT.1/TRM is met by SF.SM and SF.KEY_MGT

FIA_UID.1/PACE is met by SF.PIN_MGT, SF.AUTH and SF.SM

FIA_UAU.1/PACE is met by SF.PIN_MGT, SF.AUTH and SF.SM

FIA_UAU.4/PACE is met by SF.PIN_MGT, SF.AUTH and SF.SM

FIA_UAU.5/PACE is met by SF.PIN_MGT, SF.AUTH and SF.SM

FIA_UAU.6/PACE is met by SF.AUTH and SF.SM

FIA_UAU.6/EAC is met by SF.AUTH and SF.SM

FIA_AFL.1/AUTH is met by SF.PIN_MGT, SF.AUTH and SF.SM

FIA_API.1/TOE Authentication is met by SF.AUTH and SF.SM

FMT_SMR.1/PACE is met by SF.PIN_MGT and SF.AUTH

FMT_MTD.1/CVCA_INI is met by SF.AUTH

FMT_MTD.1/CVCA_UPD is met by SF.AUTH

FMT_MTD.1/DATE is met by SF.AUTH

FMT_MTD.1/CAPK is met by SF.AUTH

FMT_MTD.1/KEY_READ is met by SF.AUTH

FMT_MTD.1/Key_Usage_Counter is met by SF.KEY_MGT

FMT_MTD.1/Initialize_PIN is met by SF.PIN_MGT

FMT_MTD.1/Resume_PIN is met by SF.PIN_MGT

FMT_MTD.1/Change_PIN is met by SF.PIN_MGT

FMT_MTD.1/Unblock_PIN is met by SF.PIN_MGT

FMT_MTD.1/UnblockChange_RAD is met by SF.PIN_MGT

FMT_MTD.1/Erase_PIN is met by SF.PIN_MGT

FMT_MTD.1/Reinitialize_PIN is met by SF.PIN_MGT

FMT_MTD.1/UnblockChange_PUK is met by SF.PIN_MGT

FMT_MTD.1/TOE State is met by SF.CONF

FMT_MTD.3 is met by SF.PIN_MGT and SF.AUTH

FMT_MTD.1/INI_ENA

- is met by SF.AUTH that provides the authentication protocol.

FMT_MTD.1/INI_DIS

- is met by SF.AUTH that provides the authentication protocol.

FMT_LIM.1 is met by SF.PHYS

FMT_LIM.2 is met by SF.PHYS

FPT_EMS.1/PIN-PUK-KEYS is met by SF.PHYS

FTP_ITC.1/PACE is met by SF.PIN_MGT, SF.AUTH and SF.SM

10.2.1.1 TOE Summary Specification

SF.PIN_MGT The implementation of this security function contributes to:

- FIA_UID.1, FIA_UAU.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE that provide user identification and user authentication prior to enabling access to authorized functions.
- FIA_AFL.1/RAD, FIA_AFL.1/AUTH that handle the authentication failure.
- FMT_SMR.1, FMT_SMR.1/PACE that define security roles for the TOE.
- FMT_SMF.1.
- FTP_ITC.1/PACE that ensures a trusted channel between them TOE and a PACE terminal to protect the exchanged data in contactless from modification and disclosure.
- FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_MTD.1.1/Initialize_PIN, FMT_MTD.1.1/Resume_PIN,FMT_MTD.1/Change_PIN,FMT_MTD.1/Unblock_PIN,FMT_MTD.1.1/UnblockChange_RAD, FMT_MTD.1.1/Erase_PIN, FMT_MTD.1.1/Reinitialize_PIN, FMT_MTD.1.1/UnblockChange_PUK, FMT_MTD.3 that manage the TSFs date by defining access rules.

SF.SIG The implementation of this security function contributes to:

- FCS_COP.1/Sign that provide cryptographic operations.
- FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation that enforce the signature creation SFP.
- FIA_UID.1, FIA_UAU.1 that provide user identification and user authentication prior to enabling access to autorized functions.
- FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4 that manages the access right policy of the TOE.
- FMT_MOF.1 that ensures the management of the signature creation function.
- FMT_SMF.1.
- FDP_SDI.2/DTBS that ensures the integrity of DTBS.

SF.AUTH The implementation of this security function contributes to:

- FCS_CKM.1.1/DH_PACE that ensures cryptographic key generation.
- FCS_COP.1/SM in confidentiality, FCS_COP.1/SM in integrity, FCS_COP.1/GP secret data protection, FCS_RND.1, FCS_COP.1.1/SIG_VER that provide cryptographic operations.
- FIA_API.1, FIA_API.1/TOE Authentication

- FMT_SMR.1, FMT_SMR.1/PACE that define security roles for the TOE.
- FMT_SMF.1
- FMT_MSA.1/Admin, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4 that manages the access right policy of the TOE.
- FTP_ITC.1/SCD, FTP_ITC.1/SVD, FTP_ITC.1/PACE that ensure a trusted channel between them TOE and a Terminal to protect the exchanged data from modification and disclosure.
- FIA_UID.1, FIA_UAU.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/EAC that provide user identification and user authentication prior to enabling access to authorized functions.
- FIA_AFL.1/AUTH that handles the authentication failure.
- FDP_ACC.1/TRM, FDP_ACF.1/TRM that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular, that only users authenticated as authenticated terminal.
- FDP_UCT.1/TRM that ensures data exchange confidentiality.
- FMT_MTD.1.1/CVCA_INI, FMT_MTD.1.1/CVCA_UPD, FMT_MTD.1.1/DATE, FMT_MTD.1.1/CAPK, FMT_MTD.1.1/KEY_READ, FMT_MTD.3 that manage the TSFs date by defining access rules.

SF.SM The implementation of this security function contributes to:

- FCS_CKM.1/Session Keys that ensure cryptographic key generation.
- FCS_COP.1/SM in confidentiality, FCS_COP.1/SM in integrity, FCS_COP.1/GP secret data protection, FCS_COP.1.1/SIG_VER that provide cryptographic operations.
- FDP_DAU.2/SVD that ensures that exported SVD to the CGA is authenticated and unmodified.
- FIA_API.1, FIA_API.1/TOE Authentication.
- FTP_ITC.1/SCD, FTP_ITC.1/SVD, FTP_ITC.1/PACE that ensure a trusted channel between them TOE and a Terminal to protect the exchanged data from modification and disclosure.
- FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE,FIA_UAU.6/PACE, FIA_UAU.6/EAC that provide user identification and user authentication prior to enabling access to authorized functions.
- FIA_AFL.1/AUTH.
- FDP_ACC.1/TRM, FDP_ACF.1/TRM that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular, that only users authenticated as authenticated terminal.
- FDP_UCT.1/SCD, FDP_UCT.1/TRM that ensures data exchange confidentiality.
- FDP_UIT.1/TRM that ensures data exchange integrity.

SF.KEY_MGT The implementation of this security function contributes to:

- FCS_CKM.1/SCD/SVD_Generation that ensures cryptographic key generation.
- FCS_CKM.4 that manages that ensure cryptographic key destruction.
- FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation,FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import that

ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular, that only users authenticated as administrator or signatory.

- FDP_ITC.1/SCD that ensures a trusted channel between them TOE and a Terminal to protect the exchanged data from modification and disclosure.
- FIA_UID.1, FIA_UAU.1 that provide user identification and user authentication prior to enabling access to authorized functions.
- FMT_SMF.1.
- FMT_MSA.2, FMT_MSA.3, FMT_MSA.4 that manage the access right policy of the TOE.
- FDP_UCT.1/TRM that ensures data exchange confidentiality.
- FDP_UIT.1/TRM that ensures data exchange integrity.

SF.CONF The implementation of this security function contributes to:

- FMT_SMF.1.
- FMT_MSA.2, FMT_MSA.3 that manage the access right policy of the TOE.
- FMT_MTD.1/TOE_State that restrict the ability to switch the TOE from phase 6 to phase 7 to the personalization agent.

SF.ESERVICE The implementation of this security function contributes to:

- FCS_COP.1/Digital Auth, FCS_COP.1/Enc Key Decipherment that provide cryptographic operations.

SF.SAFESTATE_MGT The implementation of this security function contributes to:

- FDP_RIP.1 that ensures erasure of data in FLASH and in RAM.
- FDP_SDI.2/Persistent, FDP_SDI.2/DTBS that ensure the integrity of data stored in the TOE.
- FPT_FLS.1 that ensure the preservation of secure state when failures occur.
- FPT_TST.1 that ensures the integrity of the data stored on the TOE.

SF.PHYS The implementation of this security function contributes to:

- FPT_EMS.1, FPT_EMS.1/PIN-PUK-KEYS that ensure the TOE emanation.
- FPT_PHP.1, FPT_PHP.3 that ensures the detection of physical tampering of the TOE and the resistance to it.
- FMT_LIM.1, FMT_LIM.2.

10.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FPT_EMS.1	SF.PHYS
FPT_FLS.1	SF.SAFESTATE_MGT
FPT_PHP.1	SF.PHYS

FPT_PHP.3	SF.PHYS
FPT_TST.1	SF.SAFESTATE_MGT
FMT_SMR.1	SF.PIN_MGT, SF.AUTH
FMT_SMF.1	SF.PIN_MGT, SF.SIG, SF.AUTH, SF.KEY_MGT, SF.CONF
FMT_MOF.1	SF.SIG
FMT_MSA.1/Admin	SF.AUTH
FMT_MSA.1/Signatory	SF.SIG
FMT_MSA.2	SF.SIG, SF.AUTH, SF.KEY_MGT, SF.CONF
FMT_MSA.3	SF.SIG, SF.AUTH, SF.KEY_MGT, SF.CONF
FMT_MSA.4	SF.SIG, SF.AUTH, SF.KEY_MGT
FMT_MTD.1/Admin	SF.ADMIN
FMT_MTD.1/Signatory	SF.PIN_MGT
FIA_UID.1	SF.PIN_MGT, SF.SIG, SF.AUTH, SF.KEY_MGT
FIA_AFL.1/RAD	SF.PIN_MGT
FIA_UAU.1	SF.PIN_MGT, SF.SIG, SF.AUTH, SF.KEY_MGT
FDP_SDI.2/DTBS	SF.SIG, SF.SAFESTATE_MGT
FDP_SDI.2/Persistent	SF.SAFESTATE_MGT
FDP_RIP.1	SF.SAFESTATE_MGT
FDP_ACC.1/Signature_Creation	SF.SIG
FDP_ACF.1/Signature_Creation	SF.SIG
FCS_COP.1/Sign	SF.SIG
FCS_CKM.4	SF.KEY_MGT
FCS_CKM.1/SCD/SVD_Generation	SF.KEY_MGT
FDP_ACC.1/SVD_Transfer	SF.KEY_MGT
FDP_ACF.1/SVD_Transfer	SF.KEY_MGT
FDP_ACC.1/SCD/SVD_Generation	SF.KEY_MGT
FDP_ACF.1/SCD/SVD_Generation	SF.KEY_MGT
FTP_ITC.1/SCD	SF.AUTH, SF.SM
FDP_UCT.1/SCD	SF.SM
FDP_ITC.1/SCD	SF.KEY_MGT
FDP_ACC.1/SCD_Import	SF.KEY_MGT
FDP_ACF.1/SCD_Import	SF.KEY_MGT
FTP_ITC.1/SVD	SF.AUTH, SF.SM

FDP_DAU.2/SVD	SF.SM
FIA_API.1	SF.AUTH, SF.SM
FDP_UIT.1/DTBS	SF.SIG
FTP_ITC.1/VAD	SF.PIN_MGT
FTP_ITC.1/DTBS	SF.SM
FCS_RND.1	SF.AUTH
FCS_CKM.1/DH_PACE	SF.AUTH
FCS_CKM.1/Session Keys	SF.SM
FCS_COP.1/GP Secret Data Protection	SF.AUTH, SF.SM
FCS_COP.1/SM in Confidentiality	SF.AUTH, SF.SM
FCS_COP.1/SM in Integrity	SF.AUTH, SF.SM
FCS_COP.1/Digital Auth	SF.ESERVICE
FCS_COP.1/Enc Key Decipherment	SF.ESERVICE
FCS_COP.1/SIG_VER	SF.AUTH, SF.SM
FDP_ACC.1/TRM	SF.AUTH, SF.SM
FDP_ACF.1/TRM	SF.AUTH, SF.SM
FDP_ACC.1/MNG_File	SF.AUTH, SF.SM
FDP_ACF.1/MNG_File	SF.AUTH, SF.SM
FDP_UCT.1/TRM	SF.AUTH, SF.SM, SF.KEY_MGT
FDP_UIT.1/TRM	SF.SM, SF.KEY_MGT
FIA_UID.1/PACE	SF.PIN_MGT, SF.AUTH, SF.SM
FIA_UAU.1/PACE	SF.PIN_MGT, SF.AUTH, SF.SM
FIA_UAU.4/PACE	SF.PIN_MGT, SF.AUTH, SF.SM
FIA_UAU.5/PACE	SF.PIN_MGT, SF.AUTH, SF.SM
FIA_UAU.6/PACE	SF.AUTH, SF.SM
FIA_UAU.6/EAC	SF.AUTH, SF.SM
FIA_AFL.1/AUTH	SF.PIN_MGT, SF.AUTH, SF.SM
FIA_API.1/TOE Authentication	SF.AUTH, SF.SM
FMT_SMR.1/PACE	SF.PIN_MGT, SF.AUTH
FMT_MTD.1/CVCA_INI	SF.AUTH
FMT_MTD.1/CVCA_UPD	SF.AUTH
FMT_MTD.1/DATE	SF.AUTH
FMT_MTD.1/CAPK	SF.AUTH

FMT_MTD.1/KEY_READ	SF.AUTH
FMT_MTD.1/Key_Usage_Counter	SF.KEY_MGT
FMT_MTD.1/Initialize_PIN	SF.PIN_MGT
FMT_MTD.1/Resume_PIN	SF.PIN_MGT
FMT_MTD.1/Change_PIN	SF.PIN_MGT
FMT_MTD.1/Unblock_PIN	SF.PIN_MGT
FMT_MTD.1/UnblockChange_RAD	SF.PIN_MGT
FMT_MTD.1/Erase_PIN	SF.PIN_MGT
FMT_MTD.1/Reinitialize_PIN	SF.PIN_MGT
FMT_MTD.1/UnblockChange_PUK	SF.PIN_MGT
FMT_MTD.1/TOE State	SF.CONF
FMT_MTD.3	SF.PIN_MGT, SF.AUTH
FMT_MTD.1/INI_ENA	SF.AUTH
FMT_MTD.1/INI_DIS	SF.AUTH
FMT_LIM.1	SF.PHYS
FMT_LIM.2	SF.PHYS
FPT_EMS.1/PIN-PUK-KEYS	SF.PHYS
FTP_ITC.1/PACE	SF.PIN_MGT, SF.AUTH, SF.SM

Table 26 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
SF.PIN_MGT	FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_AFL.1/AUTH, FMT_SMR.1/PACE, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/UnblockChange_RAD, FMT_MTD.1/Erase_PIN, FMT_MTD.1/Reinitialize_PIN, FMT_MTD.1/UnblockChange_PUK, FMT_MTD.3, FTP_ITC.1/PACE, FMT_SMR.1, FMT_SMF.1, FMT_MTD.1/Signatory, FIA_UID.1, FIA_AFL.1/RAD, FIA_UAU.1, FTP_ITC.1/VAD
SF.SIG	FMT_SMF.1, FMT_MOF.1, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FIA_UID.1, FIA_UAU.1, FDP_SDI.2/DTBS, FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, FCS_COP.1/Sign, FDP_UIT.1/DTBS
SF.AUTH	FCS_RND.1, FCS_CKM.1/DH_PACE, FCS_COP.1/GP Secret Data Protection, FCS_COP.1/SM in Confidentiality, FCS_COP.1/SM in Integrity, FCS_COP.1/SIG_VER, FDP_ACC.1/TRM, FDP_ACF.1/TRM,

	FDP_ACC.1/MNG_File, FDP_ACF.1/MNG_File, FDP_UCT.1/TRM, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/EAC, FIA_AFL.1/AUTH, FIA_API.1/TOE Authentication, FMT_SMR.1/PACE, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.3, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FTP_ITC.1/PACE, FMT_SMR.1, FMT_SMF.1, FMT_MSA.1/Admin, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FIA_UID.1, FIA_UAU.1, FTP_ITC.1/SCD, FTP_ITC.1/SVD, FIA_API.1
SF.SM	FCS_CKM.1/Session Keys, FCS_COP.1/GP Secret Data Protection, FCS_COP.1/SM in Confidentiality, FCS_COP.1/SM in Integrity, FCS_COP.1/SIG_VER, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_ACC.1/MNG_File, FDP_ACF.1/MNG_File, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/EAC, FIA_AFL.1/AUTH, FIA_API.1/TOE Authentication, FTP_ITC.1/PACE, FTP_ITC.1/SCD, FDP_UCT.1/SCD, FTP_ITC.1/SVD, FDP_DAU.2/SVD, FIA_API.1, FTP_ITC.1/DTBS
SF.KEY_MGT	FDP_UCT.1/TRM, FDP_UIT.1/TRM, FMT_MTD.1/Key_Usage_Counter, FMT_SMF.1, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FIA_UID.1, FIA_UAU.1, FCS_CKM.4, FCS_CKM.1/SCD/SVD_Generation, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FDP_ITC.1/SCD, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import
SF.CONF	FMT_MTD.1/TOE State, FMT_SMF.1, FMT_MSA.2, FMT_MSA.3
SF.ESERVICE	FCS_COP.1/Digital Auth, FCS_COP.1/Enc Key Decipherment
SF.SAFESTATE_MGT	FPT_FLS.1, FPT_TST.1, FDP_SDI.2/DTBS, FDP_SDI.2/Persistent, FDP_RIP.1
SF.PHYS	FMT_LIM.1, FMT_LIM.2, FPT_EMS.1/PIN-PUK-KEYS, FPT_EMS.1, FPT_PHP.1, FPT_PHP.3
SF.ADMIN	FMT_MTD.1/Admin

Table 27 TSS and SFRs - Coverage