IDEMIA SMART IDENTITY by IN GROUPE

Public Security Target

CombICAO v3.1

on Cosmo X²

(EAC with PACE for French ID Configuration)

Reference: FQR 151 007 - 428

DOCUMENT EVOLUTION

Date	Version	Name	Revision
16/09/2025	Ed 1	INSI	Initial version
10/11/2025	Ed 2	INSI	Update sites in 4.2 section

TABLE OF CONTENTS

Table of figures

Table of tables

1 Security Target Introduction

ST Identification

Title	CombICAO v3.1 in EAC with PACE configuration for French ID on Cosmo X² Public Security Target
ST Identification	FQR 151 007 - 428 Ed2
CC Version	3.1 revision 5
Assurance Level	EAL5 augmented with ALC_DVS.2, ALC_FLR.3 and AVA_VAN.5
ITSEF	SERMA
Certification Body	ANSSI
Compliant to Protection Profile	[PP_EACwPACE]

NB: the underlying platform full name is "**ID-One Cosmo X²**". Please note that in the all the document the diminutive "**Cosmo X²**" will be used instead.

1.1 TOE Identification

TOE Commercial Name	CombICAO v3.1 in EAC with PACE configuration for French ID on Cosmo X²
Applet Code Versions (SAAAAR Code)	'20 38 21 FF'
Applet Internal Version	'01 03 04 11'
Platform Name	Cosmo X²
Platform Certificate	[PTF_CERT]
Guidance Documents	[AGD_PRE], [AGD_OPE], [PTF_AGD_OPE], [PTF_AGD_PRE], [PTF_AGD_ALP]

2 Technical Terms, Abbreviations and Associated References

2.1 Technical Terms

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [TR-03110-3].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a travel document and a terminal as required by [TR-03110-3], namely (i) PACE, (ii) Chip Authentication v1, (iii) Passive Authentication with SO_D and (iv) Terminal Authentication v1. AIP can generally be used by EIS-AIP-PACE.
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).
Audit records	Write-only-once non-volatile memory area of the eDigitalIdentity document's chip to store the Initialisation Data and Pre-personalisation Data.
Authenticity	Ability to confirm the eDigitalIdentity document and its data elements on the eDigitalIdentity document's chip were created by the issuing State or Organization
Basic Access Control	Security mechanism defined in [ICAO_9303] by which means the eDigitalIdentity document's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
Basic Inspection System (BIS)	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the eDigitalIdentity document presenter as the eDigitalIdentity document holder (for ePassport: by comparing the real biometric data (face) of the eDigitalIdentity document presenter with the stored biometric data (DG2) of the eDigitalIdentity document holder). The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorised by the eDigitalIdentity document Issuer through the Document Verifier of receiving state to read a subset of data stored on the eDigitalIdentity document.

Term	Definition
Biographical data (bio data).	The personalised details of the bearer of the eDigitalIdentity document appearing as text in the visual and machine-readable zones on the biographical data page of a eDigitalIdentity document [ICAO_9303].
Biometric reference data	Data stored for biometric authentication of the eDigitalIdentity document holder in the eDigitalIdentity 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 eDigitalIdentity document Issuer with respect to confirming correctness of user and TSF data stored in the eDigitalIdentity document. The CSCA represents the country specific root of the PKI for the eDigitalIdentity 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 eDigitalIdentity document Issuer with respect to protection of user data stored in the eDigitalIdentity 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.

Term	Definition
	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 Basic Access Key Derivation Algorithm	The [ICAO_9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Details Data	Data printed on and electronically stored in the eDigitalIdentity document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the eDigitalIdentity document's chip and the inspection system [ICAO_9303]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
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 eDigitalIdentity 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 eDigitalIdentity 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.

Term	Definition
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 eDigitalIdentity 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 eDigitalIdentity document Issuer und a foreign CVCA ensuring enforcing the eDigitalIdentity document Issuer's privacy policy) [1] [2]
Eavesdropper	A threat agent with low attack potential reading the communication between the eDigitalIdentity document's chip and the inspection system to gain the data on the eDigitalIdentity document's chip.
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]
eDigitalIdentity 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	[PACE-PP] definition A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable eDigitalIdentity document (MRTD). See [TR-03110-1]. [PP-EAC] definition Non-executable data defining the functionality of the operating system on the IC as the eDigitalIdentity document's chip. It includes the file structure implementing the LDS [ICAO_9303],

[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
	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 eDigitalIdentity 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 eDigitalIdentity document and TSF data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
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 eDigitalIdentity 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.
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.

Term	Definition
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as eDigitalIdentity document material during the IC manufacturing and the delivery process to the eDigitalIdentity 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 eDigitalIdentity document or an invalid visa; (b) a counterfeit, forged or altered eDigitalIdentity 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 eDigitalIdentity document material (IC identification data).
Inspection	The act of a State examining an eDigitalIdentity document presented to it by a traveller (the eDigitalIdentity 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 eDigitalIdentity document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as eDigitalIdentity document holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The eDigitalIdentity document's chip is an integrated circuit.
Integrity	Ability to confirm the eDigitalIdentity document and its data elements on the eDigitalIdentity document's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official eDigitalIdentity document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO_9303]]
Issuing State	The Country issuing the eDigitalIdentity document. [ICAO_9303]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. The capacity expansion technology used is the eDigitalIdentity document's chip.

Term	Definition
Logical Data Structure 2 (LDS2)	The file structures required to support the ICAO LDS2 [9303-10_LDS2] consisting of LDS file structure with three additional and optional applications: • Travel records (stamps); • Visa records; and • Additional biometrics.
Logical eDigitalIdentity document	Data of the eDigitalIdentity 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 eDigitalIdentity 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 eDigitalIdentity document or MRP Data Page or, in the case of the TD1, the back of the eDigitalIdentity document, containing mandatory and optional data for machine reading using OCR methods. [ICAO_9303] The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a eDigitalIdentity 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 eDigitalIdentity document Manufacturer completing the IC to the eDigitalIdentity 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 eDigitalIdentity 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,

Term	Definition
	- Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date.
Optional biometric reference data	Data stored for biometric authentication of the eDigitalIdentity document holder in the eDigitalIdentity 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.
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 eDigitalIdentity 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 eDigitalIdentity document Issuer to personalise the eDigitalIdentity document for the eDigitalIdentity document holder by some or all of the following activities: ICAO eDigitalIdentity document (i) establishing the identity of the eDigitalIdentity document holder for the biographic data in the eDigitalIdentity document, (ii) enrolling the biometric reference data of the eDigitalIdentity document holder, (iii) writing a subset of these data on the physical eDigitalIdentity document (optical personalisation) and storing them in the eDigitalIdentity document (electronic personalisation) for the eDigitalIdentity document holder as defined in [TR-03110-1], (iv) writing the document details data,

Term	Definition
	(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 eDigitalIdentity document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
Personalisation Data	A set of data incl. individual-related data (biographic and biometric data) of the eDigitalIdentity 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 eDigitalIdentity document and by the eDigitalIdentity document's chip to verify the authentication attempt of a terminal as Personalisation Agent according to the SFR FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE.
Physical part of the eDigitalIdentity document	eDigitalIdentity 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 eDigitalIdentity 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 eDigitalIdentity document Manufacturer (Phase 2) for traceability of non-personalised eDigitalIdentity 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).

Term	Definition
Pre-personalised eDigitalIdentity document's chip	eDigitalIdentity document's chip equipped with a unique identifier.
Receiving State	The Country to which the eDigitalIdentity 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.
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 eDigitalIdentity document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Skimming	Imitation of the inspection system to read the logical eDigitalIdentity document or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Standard Inspection Procedure	A specific order of authentication steps between an eDigitalIdentity document and a terminal as required by [ICAO_9303] and [TR-03110-1], namely PACE or BAC and Passive Authentication with SO_D. SIP can generally be used by BIS-PACE and BIS-BAC.
Inspection Procedure for multi-application eDigitalIdentity document's	This section describes an inspection procedure designed for eDigitalIdentity document's containing one or more applications besides the eDigitalIdentity 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 eDigitalIdentity document and the related value presented to the terminal by the eDigitalIdentity document presenter. In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE.

Term	Definition
	Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the eDigitalIdentity document using a shared password (CAN or MRZ).
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 eDigitalIdentity document gathered by inconspicuous (for the eDigitalIdentity document holder) recognising the eDigitalIdentity document.
eDigitalIdentity 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, reflecting essential data elements capable of being machine read; see [ICAO_9303] (there "Machine readable eDigitalIdentity document").
eDigitalIdentity document (electronic)	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: *ePassport*.
eDigitalIdentity document Holder	The rightful holder of the eDigitalIdentity document for whom the issuing State or Organisation personalised the eDigitalIdentity document.
eDigitalIdentity 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 eDigitalIdentity document to the inspection system and claiming the identity of the eDigitalIdentity document holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [CC1]).
Unpersonalised eDigitalIdentity document	The eDigitalIdentity document that contains the eDigitalIdentity 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 eDigitalIdentity document as defined in [5] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE.

Term	Definition
	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
BAC	Basic Access Control
BAP	Basic Access Protection
BIS	Basic Inspection System
BIS-PACE	Basic Inspection System with PACE
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
CLFDB	Ciphered Load File Data Block
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DF	Dedicated File
DH	Diffie Hellman
DSK	Dump Secret Key
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EF	Elementary File
FID	File identifier
GP	Global Platform
IC	Integrated Chip
ICAO	International Civil Aviation Organization
ICC	Integrated Chip card
ICCSN	Integrated Circuit Card Serial Number.
IFD	Interface Device
IS	Inspection System
IDL	ISO-compliant Driving Licence
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
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile

PS	Personalisation System
PT	Personalisation Terminal
RF	Radio Frequency
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
RSA CRT	Rivest Shamir Adleman – Chinese Remainder Theorem
SAI	Scanning Area Identifier
SAR	Security assurance requirement
SCP	Secure Channel Procotol
SFR	Security functional requirement
SHA	Secure Hashing Algorithm
SIP	Standard Inspection Procedure
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 1760 Ed 2 CombICAO v3.1 on Cosmo X² - Operational User Guidance (AGD_OPE)
[AGD_PRE]	FQR 220 1759 Ed 2 CombICAO v3.1 on Cosmo X² - Preparative Procedures (AGD_PRE)
[PTL_AGD_OPE]	Cosmo X^2 Reference Guide, FQR 110 A334
[PTL_AGD_PRE]	Cosmo X^2 Pre-Perso Guide, FQR 110 A335
[PTF_AGD_ALP]	Cosmo X^2 Application Loading Protection Guidance, FQR 110 A336
[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.
[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

Reference	Description
[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.
[SPECDI]	Electronic National Identity Card technical specifications A022 – 10/10/2019
[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
[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

Reference	Description
[NIST_800_38B]	NIST Special Publication 800-38B: 2005, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005
[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.
[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 419211-2:2013, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, Version 2.0.1, June 30 2016
[PP-SSCD3]	Protection profiles for secure signature creation device – Part3: Device with key import, EN 419211-3:2013, CEN/TC 224, BSI-CC-PP-0075-2012-MA-01, Version 1.0.2, 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 419211-4:2013, CEN/TC 224, BSI-CC-PP-0071-2012-MA-01, Version 1.0.1, 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 419211-5:2013, CEN/TC 224, BSI-CC-PP-0072-2012-MA-01, Version 1.0.1, June 30 2016

Reference	Description
[PP-SSCD6]	Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application, EN 419211-6:2013, CEN/TC 224, BSI-CC-PP-0076-2013-MA-01, Version 1.0.4, June 30 2016
[PTF_CERT]	NSCIB-2400104-01
[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
[ST_PTF]	Security Target Lite Cosmo X², FQR 110 A329
[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
[X9.62]	AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry (rDSA), 9 september 1998
[PP_JAVACARD]	Java Card System - Open Configuration Protection Profile, Version 3.0.5 December 2017, BSI-CC-PP-0099-2017

3 TOE Overview and Description

3.1 TOE Overview

The TOE is a composite product that consist of an IN SMART IDENTITY applet named CombICAO v3.1 loaded on Cosmo X² Global Platform and Java Card Operating system. The product is contact and/or contactless smart card security controller in **EAC with PACE configuration for French ID** Products.

This Security Target addresses the protection of the logical eDigitalIdentity document
(i) in integrity by write-only-once access control and by physical means, and
(ii) in confidentiality with the Extended Access Control Mechanism.

TOE implements the Extended Access Control as defined in [TR-03110-1] and [TR-03110-3].

The Extended Access Control consists of two parts
(i) Chip Authentication Protocol Version 1 (v1), and
(ii) Terminal Authentication Protocol Version 1 (v1).

Chip Authentication acts as an alternative to the Active Authentication stated in [ICAO_9303].

The Chip Authentication Protocol v1
(i) authenticates the eDigitalIdentity document's chip to the inspection system and
(ii) establishes secure messaging which will be used by Terminal Authentication v1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the Extended Inspection System. Therefore Terminal Authentication v1 can only be performed if Chip Authentication v1 has been successfully executed.

The Terminal Authentication Protocol v1 consists of
(i) the authentication of the Extended Inspection System as entity authorized by the receiving State or Organisation through the issuing State, and
(ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

Within the scope of this ST, the TOE can be configured as a stand-alone application or as a combination of the following official ID document applications:
- eDigitalIdentity document
- ICAO/EAC eMRTD and
- EU/ISO Driving Licence compliant to [ISO_18013-3] or [ISO_TR_19446].

The TOE may be used as an ISO Driving Licence (IDL) as both eMRTD and IDL applications share the same protocols and data structure organization.

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The eDigitalIdentity document shall strictly conform to ([PP_PACE]) as it considers high attack potential.

For the PACE protocol according to [ICAO_9303], the following steps shall be performed:

(i) The eDigitalIdentity document's chip encrypts a nonce with the shared password, derived from the MRZ, CAN, PIN or PUK data and transmits the encrypted nonce together with the domain parameters to the terminal.

(ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data, or processing PIN or PUK data provided by the document holder.

(iii) The eDigitalIdentity document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.

(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation the terminal and the eDigitalIdentity document's chip provide private communication (secure messaging) [TR-03110-3], [ICAO_9303].

The CombICAO v3.1 on Cosmo X² is also evaluated in other configurations as mentioned in the Table below.

This ST considers the CombICAO v3.1 on Cosmo X² in the **EAC with PACE configuration for French ID** .

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
EAC with PACE	[PP_PACE]	- Active Authentication (AA) - Automatic BAC phasing out

Configuration	PP Conformity	Extensions to the PP
	[PP_EACwPACE]	- Enhanced protection over Sensitive biometric data reading
EAC with PACE for French ID	**[PP_PACE]**	- **[ADDENDUM]** - **Active Authentication (AA)** - **Automatic BAC phasing out** - **Enhanced protection over Sensitive biometric data reading**
	[PP_EACwPACE]	
SSCD	Config#1 [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
	Config#2 [PP-SSCD2], [PP-SSCD3], [PP-SSCD4]	
	Config#3 [PP-SSCD2], [PP-SSCD3]	

Table 1 Different evaluated configurations of the CombICAO v3.1

3.2 TOE Description

The TOE in the PACE with EAC for French ID configuration encompasses the following features:

- In Personalisation phase:
  - authentication protocol for personalisation agent authentication;
  - 3DES, AES128, AES192 and AES256 Global Platform secure messaging;
  - access control;
  - Creation and configuration of application instances and their logical data structure;
  - Secure data loading;
  - Secure import and/or on-chip generation of Chip Authentication key pairs for CAv1;
  - Secure import and/or on-chip generation of the AA key pair;
  - life-cycle phase switching to operational phase;

- In operational phase:

  - PACE passwords: MRZ, CAN, PIN and PUK;

- PACE PIN/PUK suspend/resume mechanism according to [TR-03110-2];
- PIN/PUK verify and PIN reset;
- EAC: Chip Authentication v1 (CAv1) and Terminal Authentication v1 (TAv1);
- Active Authentication (AA);
- After CAv1: restart ICAO secure messaging in 3DES, AES128, AES192 or AES256 cipher mode;
- After PACE start ICAO secure messaging in 3DES, AES128, AES192 or AES256 cipher mode;
- After EAC: access control to DG3 and DG4 based on the effective authorization established during TAv1;
- Automatic BAC phasing out;
- CA Key Renewal;
- Key Usage Counter;

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 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.

The TOE may be used on several physical medium within an inlay, or eCover; in a plastic card are not part of the TOE.

The physical form of the module is depicted in Figure below. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads, shown as circles in the following figure :

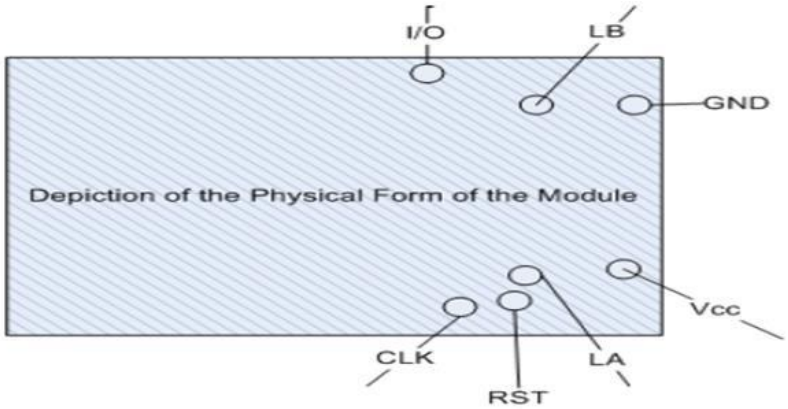


Figure 3 Physical form of the module

3.2.2 Logical scope of the TOE

The TOE is composed of:

- Circuitry of the MRTD's chip (the IC)

- Cosmo X² Java Card Open Platform
- CombICAO v3.1

The prepersonalisation and personalisation are performed by the Manufacturer and the Personalisation Agent, which controls the TOE. All along this phase, the TOE is self-protected, as it requires the authentication of the Manufacturer and the Personalisation Agent prior to any operation.

By being authenticated, the Personalisation Agent gets the rights (access control) for
(1) reading and writing data,
(2) instantiating the application, and
(3) writing of personalisation data. The Personalisation Agent can so create the file structure (MF / ADF) required for this configuration.

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

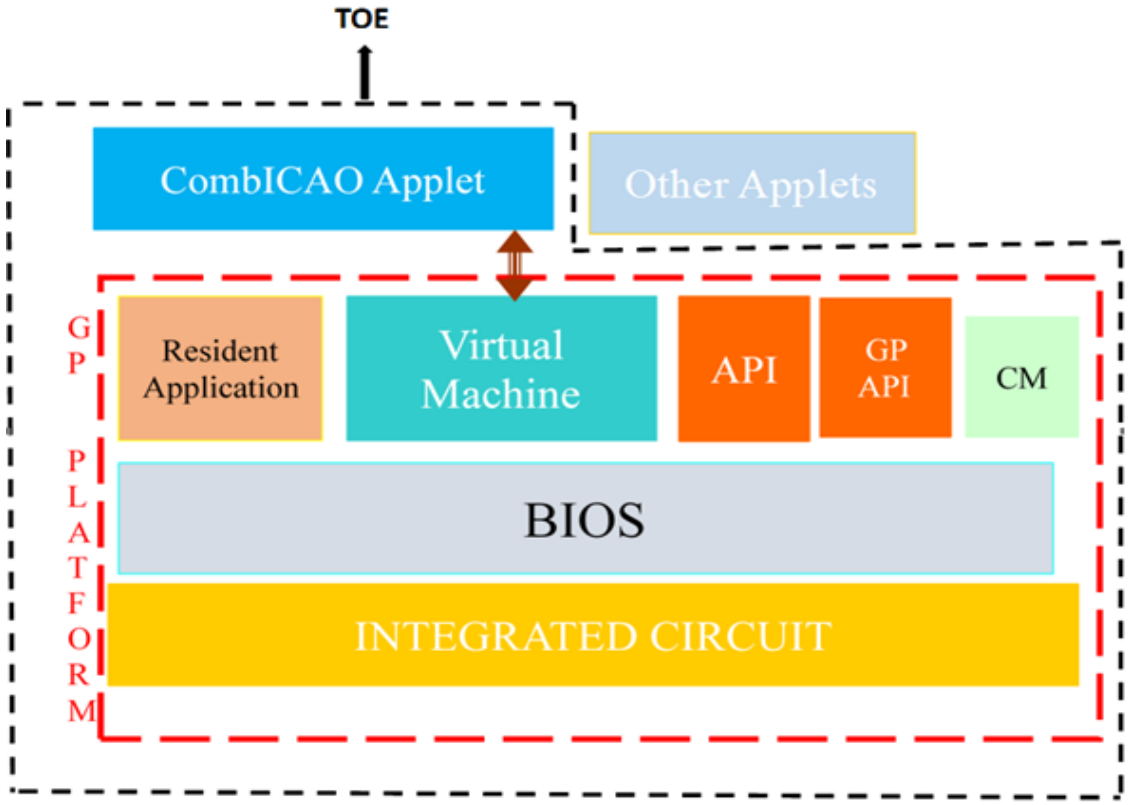


Figure 1 TOE's logical architecture

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	

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

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

Note: In particular, the TOE may be used in contact mode, without any inlay or antenna.

3.4 TOE Usage and major security features of the TOE

A State or Organization issues MRTDs to be used by the holder for international travel. The eDigitalIdentity document presenter presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this Security Target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the eDigitalIdentity document presenter is based on (i) the possession of a valid MRTD personalised for a holder with the claimed identity as given on the biographical data page and (ii) optional biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

The MRTD is viewed as unit of

(a) the **physical MRTD** as eDigitalIdentity document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder
   (1) the biographical data on the biographical data page of the passport book,
   (2) the printed data in the Machine-Readable Zone (MRZ) and
   (3) the printed portrait.

(b) the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder
   (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
   (2) the digitized portraits (EF.DG2),
   (3) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
   (4) the other data according to LDS (EF.DG5 to EF.DG16) and
   (5) the Document security object.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalisation procedures) [ICAO_9303]. These security measures include the binding of the MRTD's chip to the passport book.

The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Extended Access Control to and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [ICAO_9303]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

3.4.1 Active Authentication (AA)

Active Authentication is an authentication mechanism ensuring the chip is genuine. It uses a challenge-response protocol between the IS and the chip.
Active Authentication is realised with the INTERNAL AUTHENTICATE command. The key and algorithms supported are the following:

RSA ISO/IEC 9796-2 with a key length of 1024, 1536 and 2048 bits and hashing algorithm of SHA1 or SHA2 (i.e. SHA256, SHA384 and SHA512).

ECDSA over prime field curves with hashing algorithm of SHA1 or SHA2 (i.e. SHA256, SHA384 and SHA512) and the key sizes 192 to 521.

3.4.2 Basic Access Control (BAC)

The protocol for Basic Access Control is specified by [ICAO_9303]. Basic Access Control checks that the terminal has physical access to the MRTD's data page. This is enforced by requiring the terminal to derive an authentication key from the optically read MRZ of the MRTD. The protocol for Basic Access Control is based on [ISO11770-2] key establishment mechanism 6. This protocol is also used to generate session keys that are used to protect the confidentiality (and integrity) of the transmitted data.

The Basic Access Control (BAC) is a security feature that is supported by the TOE. The inspection system reads the printed data on the document (MRZ), authenticates itself as inspection system by means of keys derived from MRZ data. After successful 3DES based authentication, the TOE provides read access to data requiring BAC rights by means of a private communication (secure messaging) with the inspection system.

The purpose of this mechanism is to ensure that the holder gives access to the IS to the logical MRTD (data stored in the chip); It is achieved by a mutual authentication.

Once the mutual authentication is performed, a secure messaging is available to protect the communication between the chip and the IS.

This table lists the supported configurations for BAC protocol:

Configuration	Key Algo	Key Length	Hash Algo	MAC Algo
BAC	3DES 2Key	16-bytes	SHA-1	Retail MAC

Table 2 BAC Configuration

3.4.3 Chip Authentication Protocol (v1)

The Chip Authentication Protocol is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the MRTD chip.

The protocol establishes Secure Messaging between an MRTD chip and a terminal based on a static key pair stored on the MRTD chip. Chip Authentication is an alternative to the optional ICAO Active Authentication, i.e. it enables the terminal to verify that the MRTD chip is genuine but has two advantages over the original protocol:

- Challenge Semantics are prevented because the transcripts produced by this protocol are non-transferable.
- Besides authentication of the MRTD chip this protocol also provides strong session keys.

CAv1 provides implicit authentication of both the MRTD chip itself and the stored data by performing Secure Messaging using the new session keys.

3.4.4 Terminal Authentication Protocol (v1)

The Terminal Authentication Protocol is a two-move challenge-response protocol that provides explicit unilateral authentication of the terminal.

This protocol enables the MRTD chip to verify that the terminal is entitled to access sensitive data. As the terminal may access sensitive data afterwards, all further communication MUST be protected appropriately. Terminal Authentication therefore also authenticates an ephemeral public key chosen by the terminal that was used to set up Secure Messaging with Chip Authentication. The MRTD chip MUST bind the terminal's access rights to Secure Messaging established by the authenticated ephemeral public key of the terminal.

3.4.5 Password Authenticated Connection Establishment (PACE)

PACE is an access control mechanism that is supplemental to BAC. It is a cryptographically stronger access control mechanism than BAC since it uses asymmetric cryptography compared to BAC's symmetric cryptography.

PACE is realized through five commands:

1. MSE SET – AT command
2. GENERAL AUTHENTICATE command – Encrypted Nonce
3. GENERAL AUTHENTICATE command – Map Nonce
4. GENERAL AUTHENTICATE command – Perform Key Agreement
5. GENERAL AUTHENTICATE command – Mutual Authentication

Once the mutual authentication is performed, a secure messaging is available to protect the communication between the chip and the IS.

This table lists the supported configurations for PACE protocol:

Configuration	Mapping	Key Algo	Key Length (in bytes)	Secure Messaging	Auth. Token	Hash Algo
PACE–ECDH–GM–3DES	Generic	3DES 2Key	16	CBC / Retail MAC	Retail MAC	SHA-1

PACE–ECDH–GM–AES–128	Generic	AES	16	CBC / CMAC	CMAC	SHA-1
PACE–ECDH–GM–AES–192	Generic	AES	24	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–GM–AES–256	Generic	AES	32	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–IM–3DES	Integrated	3DES 2Key	16	CBC / Retail MAC	Retail MAC	SHA-1
PACE–ECDH–IM–AES–128	Integrated	AES	16	CBC / CMAC	CMAC	SHA-1
PACE–ECDH–IM–AES–192	Integrated	AES	24	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–IM–AES–256	Integrated	AES	32	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–CAM–AES–128	Chip Authentication	AES	16	CBC / CMAC	CMAC	SHA-1
PACE–ECDH–CAM–AES–192	Chip Authentication	AES	24	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–CAM–AES–256	Chip Authentication	AES	32	CBC / CMAC	CMAC	SHA-256

Table 3 PACE configuration

3.4.6 Other features

3.4.6.1 Automatic BAC phasing out

The TOE also supports a mechanism allowing the automatic deactivation of the BAC protocol after the current date (of the TOE) has reached a reference date - chosen by the issuer and configured by the personalisation Agent. The current date is the internal date updated through the EAC protocol. Thanks to this feature, it is possible to issue MRTD supporting both PACE and BAC as needed for interoperability reasons, and perform smooth phasing out of the BAC protocol in the medium term (due to its cryptographic weaknesses) during the life time of the issued MRTD, without having to wait for the complete renewal of issued MRTD (> 10 years).

3.4.6.2 Enhanced protection over Sensitive biometric data reading

The access to sensitive biometric data: the fingerprint and iris stored in DG3 and DG4 are protected in accordance with the requirements of the protection profile and specification. Beyond that, the TOE also provides a feature able to ensure a high level of confidentiality when reading these data. The TOE supports a mechanism enforcing to use a minimum cryptographic strength for the confidentiality, integrity and authenticity protection of these sensitive biometric data when being read. This may be useful for issuing authority that do not

consider DES algorithm strong enough to ensure a sufficient level of confidentiality. This mechanism allows the TOE to enforce the terminal using a stronger algorithm such as AES 128, or 192 bits, or 256 bits when reading the sensitive biometric data, and deny access to them if this condition is not met (algorithm not strong enough).

3.4.6.3 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.

3.4.6.4 CA Key Renewal / Invalidation

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

3.5 TOE delivery

The TOE is composed of:

- Circuitry of the MRTD's chip (the IC)
- IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- JavaCard open Platform Cosmo X²: see [ST_PTF] and [PTF_CERT]
- CombICAO v3.1: the application can be delivered as part of the OS and loaded in the flash or as Cap-file that can be loaded using the GP-mechanisms implemented
- Associated guidance documentation (delivered in electronic version)

The current Public ST Lite version will also be provided as a guidance document along with above-mentioned documents:

TOE Component	Identification	Form Factor of Delivery	Delivery method
CombICAO v3.1	20 38 21 FF	ID1 or ID3 Passport booklets ID1 cards or ID3 holder pages Antenna[1] inlays Chip in modules on a reel	Pre-Personalisation and personalisation tool is used in the case of an Image delivery. Otherwise, trusted courier is used.
CombICAO v3.1 guidance	[AGD_PRE] [AGD_OPE]	PDF Electronic doc	PGP-encrypted parts on USB or CD media, off-line registered distribution by trusted courier
Underlying platform guidance	[PTF_AGD_OPE] [PTF_AGD_PRE] [PTF_AGD_ALP]		

[1] The inlay production including the application of the antenna is not part of the TOE

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].

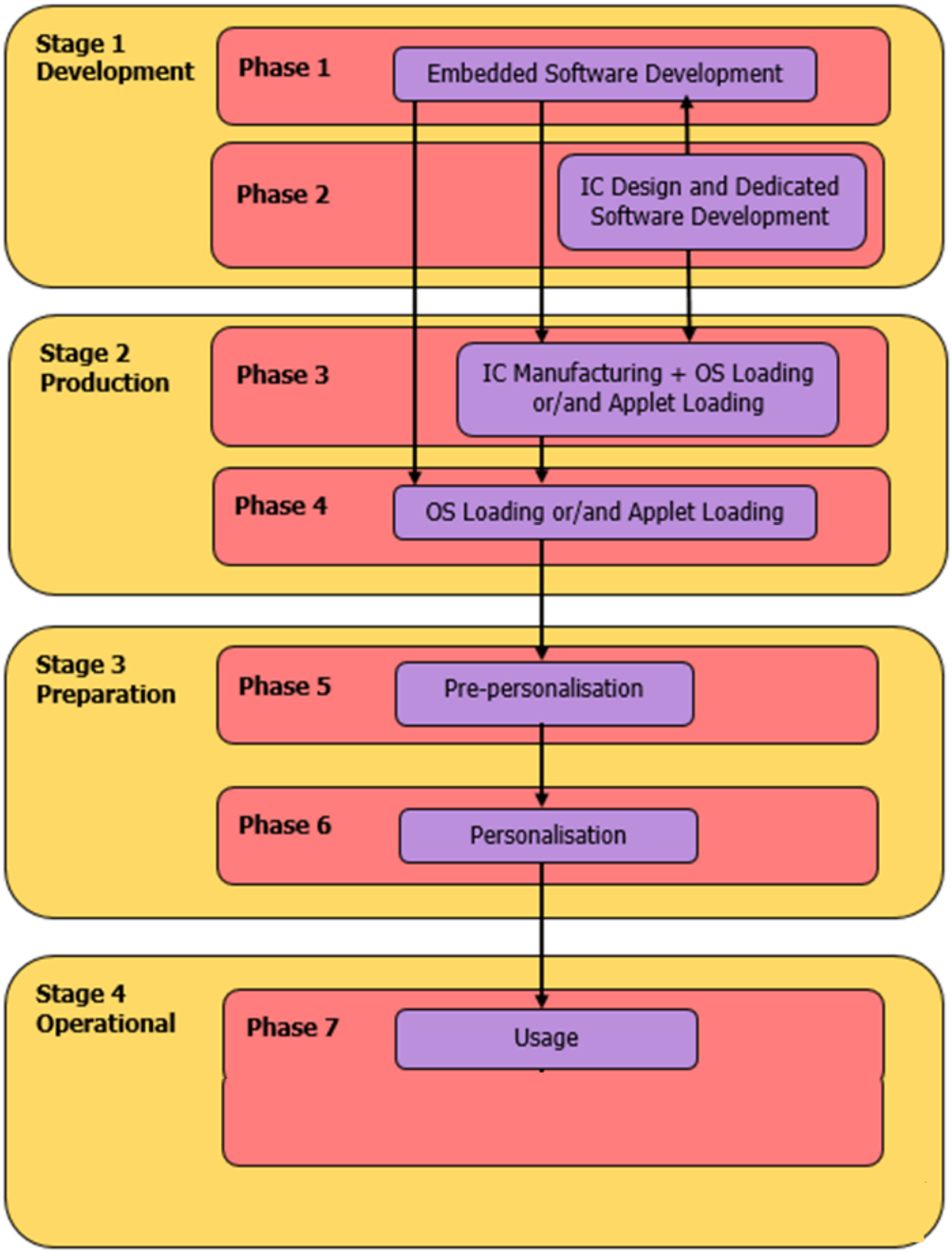


Figure 2 Life cycle Overview

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 v3.1 on Cosmo X²)
- 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 v3.1).

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 v3.1 Developer	IN SMART IDENTITY	MANILA, COURBEVOIE R&D sites	ALC
Embedded Software Developer (Java Card Open Platform)	IN SMART IDENTITY	Platform Developer Refer to [ST_PTF]	ALC
Redaction and Review of Documents	IN SMART IDENTITY	MANILA, COURBEVOIE R&D sites	ALC
IC Developer	STARCHIP	IC Manufacturer Refer to [ST_PTF]	ALC

Table 4 : Development R&D Sites

4.2 Production Environment

In this environment, the following two phases take place:

- Phase 3: IC Manufacturing
- Phase 4: Cosmo X² platform loading and CombICAO v3.1 on Cosmo X² loading

The CombICAO v3.1 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].**

IN Smart Identity and IDEMIA CC Audited Production Sites are listed below:

IN Smart Identity and IDEMIA CC Audited Production Sites/Plants	Country
Haarlem	Netherlands
Noida	India
Ostrava	Czech Republic
Shenzhen	China
Vitré	France

Table 5 : Audited Production Sites

(Option 1) Image Loading audited IC Manufacturer site

FLASH image containing both the " Cosmo X²" Java Card Platform OS along with the CombICAO v3.1 is securely delivered directly from the software developer (IN Smart Identity R&D Audited Site) to the **IC Manufacturer** (Starchip 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 Cosmo X² Platform + CombICAO v3.1 by the IC Manufacturer has been completed.

Package	Actor for FLASH image loading	Site For FLASH image loading	Covered by CC
FLASH image containing Cosmo X² Platform + CombICAO v3.1	IC Manufacturer	IC Manufacturer CC Audited Production Plants specified in [ST_PTF]	ALC

Table 6 Option 1: Both Platform and Applet packages are loaded at IC Manufacturer Site

(Option 2) Image loading at IN Smart Identity or IDEMIA Audited sites

FLASH image containing both Cosmo X² Platform along with CombICAO v3.1 is securely delivered directly from the software developer (IN Smart Identity R&D Audited Site) for loading to **CC Audited IN Smart Identity or IDEMIA Production Sites** (Refer Audited Production Sites Table).

TOE Delivery point:

- Loading of Cosmo X² Platform + CombICAO v3.1 is performed in Audited IN Smart Identity or IDEMIA Production Sites, then TOE delivery is considered at the end of Phase 4.

Package	Actor for FLASH image loading	Site for FLASH image loading	Covered by CC
FLASH image containing the Cosmo X² Platform + CombICAO v3.1	IN Smart Identity Authorized Entity	Refer Audited Production Sites Table	ALC

Table 7 Option 2: Both Platform and Applet packages are loaded at CC Audited IN Smart Identity or IDEMIA Sites

(Option 3) Platform loaded by IC Manufacturer, Applet loaded by IN Smart Identity or IDEMIA or 3rd party

Only the Cosmo X² Platform is delivered to the IC Manufacturer (Starchip Audited Sites) to be loaded.

With the Cosmo X² Platform already loaded (i.e. present) on the chip, the following options (**3a or 3b or 3c**) can be chosen for loading the CombICAO v3.1.

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

The CombICAO v3.1 along with the TOE's guidance documentation is securely delivered directly from the Software Developer (IN Smart Identity R&D Audited Site) to **Audited IN Smart Identity or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IN Smart Identity or IDEMIA Sites** or **External Sites**.

Loading of the CombICAO v3.1 on top of the already present Cosmo X² 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 v3.1 on top of already loaded Cosmo X² Platform (as described below) is done in a CC Audited IN Smart Identity or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of the CombICAO v3.1 on top of already loaded Cosmo X² Platform (as described below) is done in Non-Audited IN Smart Identity or IDEMIA Production Sites or External Sites then, TOE delivery is considered after phase 4.

Package	Actor	Site	Covered by
Image containing only Cosmo X² Platform	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
CombICAO v3.1 loaded through GP mechanism using CLFDB Key	IN Smart Identity Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IN Smart Identity or IDEMIA Sites or External Sites	AGD

Table 8 Option 3(a): Platform package is loaded at IC Manufacturer Site and Applet package is loaded at Audited IN Smart Identity or IDEMIA Sites or Non-Audited IN Smart Identity or IDEMIA Sites or External Sites through GP Mechanism

(Option 3b) Applet loading using the IN Smart Identity Resident Application

CombICAO v3.1 along with the guidance documentation is securely delivered directly from the Software Developer (IN Smart Identity R&D Audited Site) to **Audited IN Smart Identity or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IN Smart Identity or IDEMIA Sites** or **External Sites**.

CombICAO v3.1 package is securely loaded via LSK on top of the present Cosmo X² Platform Java Card OS in any of these sites. This loading is accomplished by using the IN Smart Identity "Resident Application" of the Cosmo X² Platform.

TOE Delivery points:

- If loading of Applet package on top of already loaded Cosmo X² Platform (as described below) is done in Audited IN Smart Identity or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of Applet package on top of already loaded Cosmo X² Platform (as described below) is done in Non-Audited IN Smart Identity or IDEMIA Production Sites or External Sites then, TOE delivery after Phase 4.

Package	Actor	Site	Covered by
Image containing only Cosmo X² Platform	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
3b CombICAO v3.1 loaded through Resident Application using LSK format	IN Smart Identity Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IN Smart Identity or IDEMIA Sites or External Sites	AGD

Table 9 Platform package is loaded at IC Manufacturer Site and Applet package is loaded through resident application using LSK format in Ciphered format is loaded

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

CombICAO v3.1 along with the guidance documentation is securely delivered directly from the Software Developer (IN Smart Identity R&D Audited Site) to **CC Audited IN Smart Identity Production Sites** (Refer Audited Production Sites Table).

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

TOE Delivery points:

- The loading of CombICAO v3.1 on top of already loaded Cosmo X² Platform is done in plain (unprotected) format in Common Criteria Audited IN Smart Identity Production Sites. The TOE delivery is considered at the end of Phase 4.

Package	Actor	Site	Covered by
Image containing only Cosmo X² Platform	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
CombICAO v3.1 in Plain Format	IN Smart Identity Authorized Entity	Refer Audited Production Sites Table	ALC

Table 10 Option 3(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at Audited IN Smart Identity Sites only

(Option 4) Platform loaded only by IN Smart Identity or IDEMIA Audited sites and Applet loaded by IN Smart Identity or IDEMIA or 3rd party

Only Cosmo X² Platform is securely delivered directly from the software developer (IN Smart Identity R&D Audited Site) for loading to **CC Audited IN Smart Identity or IDEMIA Production Sites** (Refer Audited Production Sites Table)

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

(Option 4a) Applet loading using GP CLFDB mechanism
CombICAO v3.1 along with the guidance documentation is securely delivered directly from the Software Developer (IN Smart Identity R&D Audited Site) to **Audited IN Smart Identity or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IN Smart Identity 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 IN Smart Identity or IDEMIA Production Sites** or **Non-Audited IN Smart Identity or IDEMA Sites** or **External Sites**.

TOE Delivery points:

- If loading of the CombICAO v3.1 on top of already loaded Cosmo X² Platform (as described below) is done in CC Audited IN Smart Identity or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of the CombICAO v3.1 onto the already loaded Cosmo X² Platform (as described below) is done in Non-Audited IN Smart Identity or IDEMIA Production Sites or External Sites then, TOE delivery is considered after Phase 4.

Package	Actor	Site	Covered by
Image containing only Cosmo X² Platform	IN Smart Identity Authorized Entity	Refer Audited Production Sites Table	ALC
CombICAO v3.1 loaded through GP mechanism using CLFDB Key	IN Smart Identity Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IN Smart Identity or IDEMIA Sites or External Sites	AGD

Table 11 Option 4(a): Platform package is loaded at Audited IN Smart Identity or IDEMAI Sites and Applet package is loaded at Audited IN Smart Identity or IDEMIA Sites or Non-Audited IN Smart Identity or IDEMIA Sites or External Sites through GP Mechanism

(Option 4b) Applet loading using the IN Smart Identity Resident Application

CombICAO v3.1 along with the guidance documentation is securely delivered directly from the Software Developer (IN Smart Identity R&D Audited Site) to **Audited IN Smart Identity** or IDEMIA **Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IN Smart Identity** or IDEMIA **Sites** or **External Sites**.

Secure loading of CombICAO v3.1 is done via LSK on top of the present Cosmo X² Java Card OS (already loaded by **Audited IN Smart Identity** or IDEMIA **Production Sites)** in any of these sites. This loading is accomplished by using the IN Smart Identity "Resident Application" of the Cosmo X² Platform OS

TOE Delivery points:

- If loading of Applet package on top of already loaded Cosmo X² Platform (as described below) is done in Audited IN Smart Identity or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of Applet package on top of already loaded Cosmo X² Platform (as described below) is done in Non-Audited IN Smart Identity or IDEMIA Production Sites or External Sites then, TOE delivery is considered after Phase 4.

Package	Actor	Site	Covered by
Image containing only Cosmo X² Platform	IN Smart Identity Authorized Entity	Refer Audited Production Sites Table	ALC
4b CombICAO v3.1 package loaded through Resident Application using LSK format	IN Smart Identity Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IN Smart Identity or IDEMIA Sites or External Sites	AGD

Table 12 Platform package is loaded at Audited IN Smart Identity or IDEMIA Sites and Applet package is loaded at Audited IN Smart Identity or IDEMIA Sites or Non-Audited sites or External Sites through Resident application using LSK format

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

CombICAO v3.1 along with the guidance documentation is securely delivered directly from the Software Developer (IN Smart Identity R&D Audited Site) to **Audited IN Smart Identity Production Sites** (Refer Audited Production Sites Table).

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

TOE Delivery points:

- Here, since the loading of Applet package on top of already loaded Cosmo X² Platform (as described below) is done in Plain format in CC Audited IN Smart Identity Production Sites, so TOE delivery is considered at the end of Phase 4.

Package	Actor	Site	Covered by
Image containing only Platform	IN Smart Identity Authorized Entity	Refer Audited Production Sites Table	ALC
CombICAO v3.1 in Plain Format	IN Smart Identity Authorized Entity	Refer Audited Production Sites Table	ALC

Table 13 Option 4(c): Platform package is loaded at Audited IN Smart Identity or IDEMIA Sites and Applet package in plain format is loaded at Audited IN Smart Identity 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 v3.1 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 Cosmo X² 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] and [CEM].

The conformance to the CC is claimed as follows:

CC	Conformance rationale
Part 2	Conformance with the extended[3] part: ▪ FAU_SAS.1 "Audit Storage" ▪ 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 "Authentication Proof of Identity"
Part 3	Conformance to EAL 5, augmented with ▪ AVA_VAN.5: "Advanced methodical vulnerability analysis" ▪ ALC_DVS.2: "Sufficiency of security measures" ▪ ALC_FLR.3: "Systematic Flaw Remediation"

Table 14 Common Criteria conformance claim

5.2 Protection Profile Conformance Claim

This security target (ST) claims strict conformance to:

- [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, version 1.3.2, 5th December 2012.

The [PP_EACwPACE] claims strict conformance to the PACE Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01, 22 July 2014, BSI.

The extensions do not contradict any of the threats, assumptions, organisational policies, objectives or SFRs stated in the [PP_EACwPACE] that covers the advanced security methods PACE and EAC in operational use phase.

[3] The rationale for SFR addition is described in the relative PP

The underlying integrated circuit is successfully evaluated and certified in accordance with the Security IC Platform Protection Profile [PP_IC].

The underlying Java Card Open Platform of the TOE is evaluated and certified in accordance with the Java Card™ System Protection Profile Open Configuration [PP_JAVACARD].

Even though the ST claims conformance to [PP_EACwPACE], certain terminology has been updated in the ST and Assets, Threats, Objectives and SFRs added according to the [ADDENDUM].

The following parts list assumptions, threats, OSP, OT and OE for this TOE (i.e. from [PP_EACwPACE] and additional).

5.2.1 Assumptions

The following Assumptions are assumed for this TOE:

- **A.Insp_Sys** *"Inspection Systems for global interoperability"* defined in [PP_EACwPACE],
- **A.Auth_PKI** *"PKI for Inspection Systems"* defined in [PP_EACwPACE],
- **A.Passive_Auth** *"PKI for Passive Authentication"* defined in [PP_EACwPACE],

5.3 Package Claim

This ST is conforming to assurance package EAL5 augmented with ALC_DVS.2, ALC_FLR.3 and AVA_VAN.5 defined in CC part 3 [CC3].

5.3.1 EAL Rationale

5.3.1.1 AVA_VAN.5 Advanced methodical vulnerability analysis

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfill the security objectives OT.Chip_Auth_Proof.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 "Security architecture description"
- ADV_FSP.4 "Security-enforcing functional specification"
- ADV_TDS.3 "Basic modular design"
- ADV_IMP.1 "Implementation representation of the TSF"
- AGD_OPE.1 "Operational user guidance"
- AGD_PRE.1 "Preparative procedures"
- ATE_DPT.1 "Testing: basic design"

All of these are met or exceeded in the EAL5 assurance package

5.3.1.2 ALC_DVS.2 Sufficiency of security measures

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing especially for the secure handling of the MRTD's material.

The component ALC_DVS.2 augmented to EAL5 has no dependencies to other security requirements.

5.4 PP Conformance Rationale

This ST	[PACE/EACPP]
eDigitalIdentity document	travel document
eDigitalIdentity document holder	travel document holder
eDigitalIdentity document presenter	travel document presenter
Identification user data	user data
PACE terminal	BIS-PACE

5.4.1 Main aspects

- The TOE description is based on the TOE definition and TOE usage of [PP_EACwPACE] and [ADDENDUM]. It was enhanced by product specific details.

- All definitions of the security problem definition in [PP_EACwPACE] and [ADDENDUM]have been taken exactly from the protection profile in the same wording.

- The security objectives have been taken exactly from [PP_EACwPACE] and [ADDENDUM] in the same wording.

- The part of extended components definition has been taken originally from [PP_EACwPACE] and [ADDENDUM].

- The SFRs for the TOE have been taken originally from the [PP_EACwPACE] and [ADDENDUM] added by according iterations, selections and assignments.

- The security assurance requirements (SARs) have been taken originally from the [PP_EACwPACE]. The requirements are shifted to those of EAL 5+.

5.4.2 Overview of differences between the PP and the ST

The following parts list additional Subject, Threats and Objectives for this TOE which are not in [PP_EACwPACE] and [ADDENDUM].

These additions do not contradict with any other Subjects, Threats and Objectives of the TOE of the original PP nor mitigate a threat (or part of a threat) , meant to be addressed by security objectives for the TOE in the PP.

5.4.3 Subjects

The following additional Subjects are identified for this TOE:

- **eDigitalIdentity document packaging responsible**
- **Embedded software loading responsible**
- **Pre-personalisation Agent**
- **Administrator**

5.4.4 Threats

The following additional Threats are identified for this TOE:

- **T.Configuration**
- **T. Forgery_Supplemental_Data**
- **T.ADMIN_Configuration**
- **T.Key_Usage**

5.4.5 Security Objectives

The following additional Security Objectives of the TOE are identified for this TOE:

- **OT.AA_Proof**
- **OT.Data_Int_AA**
- **OT.Configuration**
- **OT.Update_File**
- **OT.AC_SM_Level**
- **OT.ADMIN_Configuration**
- **OT.Key_Usage_Counter**

5.5 CC Conformance and usage in real life

In the real life, for interoperability purposes, the MRTD will most likely support BAC, PACE and EAC.

- If the terminal reads MRTD data by performing only BAC, the security of the MRTD will be covered by the security evaluation of the TOE described in the ST claiming compliance to the [PP_BAC] only.

- If the terminal reads the content of the MRTD by performing BAC then EAC, the security of the MRTD will be covered by the security evaluation of (1) the TOE described by the ST claiming compliance to [PP_BAC] and (2) the TOE described by the ST claiming compliance to [PP_EAC], assuming PACE is not supported by the terminal (as not used for the inspection procedure)

- If the terminal reads the content of the MRTD by performing PACE then EAC, the security of the MRTD will be covered by the security evaluation of the TOE described by the ST claiming compliance to [PP_EACwPACE], assuming PACE is supported by the terminal (as not used for the inspection procedure).

6 Security Problem Definition

6.1 Assets

Overview

The following table presents the assets of the TOE and their corresponding phase(s) according to TOE life cycle:

Asset	Step 5	Step 6	Step 7
Biometric Data	No	Yes	Yes
Personal Data	No	Yes	Yes
EF.COM	No	Yes	Yes
EF.SOD	No	Yes	Yes
CA_SK	No	Yes	Yes
CA_PK	No	Yes	Yes
AA_PK	No	Yes	Yes
AA_SK	No	Yes	Yes
Session_K	Yes	Yes	Yes
PACE_Kmac	No	No	Yes
PACE_Kenc	No	No	Yes
ephem-Skpicc-PACE	No	No	Yes
PACE_PWD	No	Yes	Yes
Perso_K	No	Yes	No
Pre-Perso_K	Yes	No	No
LCS	Yes	Yes	Yes
Updatable data	No	Yes	Yes

The assets to be protected by the TOE include the Sensitive Identification User Data on the eDigitalIdentity document's chip, Sensitive Identification user data transferred between the TOE and the terminal, and eDigitalIdentity document tracing data.

6.1.1 Primary Assets

Logical MRTD Sensitive User Data

Sensitive biometric reference data (EF.DG3, EF.DG4)

Application Note:

(5 in [PP_EACwPACE]): Due to interoperability reasons the [ICAO_9303] requires that Basic Inspection Systems may have access to logical eDigitalIdentity document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode, if it is accessed using BAC [ICAO_9303]. Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [PP_BAC]). If supported, it is therefore recommended to use PACE instead of BAC. If nevertheless BAC has to be used, it is recommended to perform Chip Authentication v1 before getting access to data (except DG14), as this mechanism is resistant to high potential attacks.

Authenticity of the MRTD's chip

The authenticity of the MRTD's chip personalised by the issuing State or Organisation for the MRTD holder is used by the eDigitalIdentity document presenter to prove his possession of a genuine MRTD.

User data stored on the TOE

All data (being not authentication data) stored in the context of the ePassport application of the MRTD as defined in [ICAO_9303] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO_9303]).

This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [PP_BAC].

It includes:

Personal Data

The Personal Data are the logical MRTD standard Identification User Data of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16).

Active Authentication key (AA_SK)

The Active Authentication Private Key is used by the application to process Active Authentication.

Active Authentication key (AA_PK)

The public key is stored in data group DG15 and thus protected by Passive Authentication.

EF.COM

The EF.COM is an elementary file containing the list of the existing elementary files (EF) with the Identification user data.

EF.SOD

The elementary file Document Security Object is used by the inspection system for Passive Authentication of the logical MRTD.

User data transferred between the TOE and the terminal connected

All data (being not authentication data) being transferred in the context of the ePassport application of the MRTD as defined in [ICAO_9303] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO_9303]).

User data can be received and sent (exchange receive, send).

MRTD tracing data

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

6.1.2 Secondary Assets

Accessibility to the TOE functions and data only for authorised subjects

Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.

Genuineness of the TOE

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

This asset also covers 'Authenticity of the MRTD's chip in [PP_BAC].

TOE internal secret cryptographic keys

Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.

It includes:

Chip Authentication Private Key (CA_SK)

The Chip Authentication Private Key is used by the application to process Chip Authentication.

Chip Authentication Public Key (CA_PK)

The Chip Authentication Public Key (contained in EF.DG14) is used by the inspection system for the Chip Authentication.

Secure Messaging session keys (Session_K)

Session keys are used to secure communication in confidentiality and authenticity.

PACE session keys (PACE-Kmac, PACE-Kenc)

PACE session keys are secure messaging keys for message authentication and for message encryption agreed between the TOE and a terminal as result of the PACE Protocol.

Ephemeral private key PACE (ephem-Skpicc-PACE) The ephemeral PACE Authentication Key Pair is used for Key Agreement Protocol.

TOE internal non-secret cryptographic material

Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality.

MRTD communication establishment authorisation data

Restricted-revealable authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be send to it.

It includes:

PACE password (PACE_PWD)

Password needed for PACE authentication.

Personalisation Agent keys (Perso_K)

This key set used for mutual authentication between the Personalisation agent and the chip, and secure communication establishment.

Pre-Personalization Agent keys (Pre-Perso_K)

This key set used for mutual authentication between the Pre-personalization agent and the chip, and secure communication establishment.

TOE Life Cycle State (LCS)

This is the Life Cycle State of the TOE.

Updatable Data

Data other than Personal Data, Biometric Data, EF.COM, EF.SOD, CA_PK, CA_SK, AA_PK , AA_SK, Pre-Perso_K, Perso_K, Session_K, LCS and Configuration Data which can be modified in Operational Use phase.

6.1.3 Additional Assets identified as per ADDENDUM

6.1.3.1 Primary Assets

Sensitive ID User Data

Person identification data, which have been classified as sensitive data by the eDigitalIdentity document issuer. Sensitive identification user data are a subset of all user data.

Generic security property to be maintained by the current security policy: Confidentiality, Integrity, Authenticity

6.1.3.2 Secondary Assets identified as per ADDENDUM

eDigitalIdentity document Communication Establishment Authorization Data

Restricted-revealable authorization information for a human user being used for verification of the authorization attempts as an authorized user (PACE PIN & PUK). These data are stored in the TOE, and are not send to it.

Generic security property to be maintained by the current security policy: Confidentiality, Integrity

Secret eDigitalIdentity document Holder Authentication Data

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

Generic security property to be maintained by the current security policy: Confidentiality, Integrity

6.2 Subjects and external entities

Overview

The following table presents the assets of the TOE and their corresponding phase(s) according to life cycle defined in this ST.

Subject	Step 3	Step 4	Step 5	Step 6	Step 7
MRTD Holder	No	No	No	No	Yes
eDigitalIdentity document presenter	No	No	No	No	Yes
Basic Inspection System with PACE	No	No	No	No	Yes
Document Signer	No	No	No	Yes	No
Country Signing Certification Authority	No	No	No	Yes	No
Personalisation Agent	No	No	No	Yes	No
Administrator	No	No	No	No	Yes
IC manufacturer (Manufacturer role)	Yes	No	No	No	No
eDigitalIdentity document packaging responsible (Manufacturer role)	No	Yes	No	No	No
Embedded software loading responsible (Manufacturer role)	No	Yes	No	No	No
Pre-personalization Agent (Manufacturer role)	No	No	Yes	No	No
Country Verifying Certification Authority	No	No	No	No	Yes
Document Verifier	No	No	No	No	Yes
Terminal	No	No	Yes	Yes	Yes
Inspection System	No	No	No	No	Yes
Attacker	Yes	Yes	Yes	Yes	Yes

6.2.1 Subjects

MRTD holder

MRTD holder is the eDigitalIdentity document holder defined in [PP_PACE]:

A person for whom the eDigitalIdentity document Issuer has personalised the travel document. This entity is commensurate with 'MRTD Holder' in [PP_BAC]. Please note that a eDigitalIdentity document holder can also be an attacker.

eDigitalIdentity document presenter

A person presenting the eDigitalIdentity document to a terminal and claiming the identity of the eDigitalIdentity document holder. This external entity is commensurate with 'eDigitalIdentity document presenter' in [PP_BAC]. Please note that a eDigitalIdentity document presenter can also be an attacker.

Terminal

A terminal is any technical system communicating with the TOE through the contactless interface.

Note: as the TOE may also be used in contact mode, the terminal may also communicate using the contact interface.

Basic Inspection System with PACE (BIS-PACE terminal)

A technical system being used by an inspecting authority and verifying the eDigitalIdentity document presenter as the eDigitalIdentity document holder (for ePassport: by comparing the real biometric data (face) of the eDigitalIdentity document presenter with the stored biometric data (DG2) of the eDigitalIdentity document holder).

PACE terminal implements the terminal's part of the PACE protocol and authenticates itself to the eDigitalIdentity document using a shared password (PACE password) and supports Passive Authentication.

See also par. 1.2.5 in [PP_PACE].

Document Signer (DS)

An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the eDigitalIdentity document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate, see [ICAO_9303]. This role is usually delegated to a Personalisation Agent.

Country Signing Certification Authority (CSCA)

An organisation enforcing the policy of the eDigitalIdentity document Issuer with respect to confirming correctness of user and TSF data stored in the eDigitalIdentity document. The CSCA represents the country specific root of the PKI for the eDigitalIdentity document and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate having to be distributed by strictly secure diplomatic means, see [ICAO_9303], 5.5.1.

Personalisation Agent

An organisation acting on behalf of the eDigitalIdentity document Issuer to personalise the eDigitalIdentity document for the eDigitalIdentity document holder by some or all of the following activities: (i) establishing the identity of the eDigitalIdentity document holder for the biographic data in the eDigitalIdentity document, (ii) enrolling the biometric reference data of the eDigitalIdentity document holder, (iii) writing a subset of these data on the physical eDigitalIdentity document (optical personalisation) and storing them in the eDigitalIdentity document (electronic personalisation) for the eDigitalIdentity document holder as defined in [ICAO_9303], (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 eDigitalIdentity document Issuer. This entity is commensurate with 'Personalisation agent' in [PP_BAC].

IC Manufacturer

This additional subject is a refinement of the role Manufacturer as described in [PP_PACE]. It is the manufacturer of the IC.

If scheme 1 is applied (cf. § 1.3.6), this subject is responsible for the embedded software downloading in the IC. This subject does not use Flash loader, even if it is embedded in the IC

Attacker

Additionally to the definition from [PP_PACE], chap 3.1 the definition of an attacker is refined as followed: A threat agent trying (i) to manipulate the logical eDigitalIdentity document without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iii) to forge a genuine eDigitalIdentity document, or (iv) to trace a eDigitalIdentity document.

Application Note:

(7 in [PP_EACwPACE]): An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged eDigitalIdentity document. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

Country Verifying Certification Authority (CVCA)

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organisation with respect to the protection of sensitive biometric reference data stored in the eDigitalIdentity document. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

Document Verifier (DV)

The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the eDigitalIdentity document in the limits provided by the issuing States or Organisations in the form of the Document Verifier Certificates.

Inspection system (IS)

A technical system used by the border control officer of the receiving State (i) examining an eDigitalIdentity document presented by the eDigitalIdentity document presenter and verifying its authenticity and (ii) verifying the eDigitalIdentity document presenter as eDigitalIdentity document holder.

The Extended Inspection System (EIS) performs the Advanced Inspection Procedure (figure1) and therefore (i) contains a terminal for the communication with the eDigitalIdentity document's chip, (ii) implements the terminals part of PACE and/or BAC; (iii) gets the authorization to read the logical eDigitalIdentity document either under PACE

or BAC by optical reading the eDigitalIdentity document providing this information, (iv) implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [TR-03110-1] and [TR-03110-3] and (v) is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.

6.2.2 Additional Subjects identified as per ADDENDUM

PACE Terminal

A technical system verifying correspondence between the password stored in the eDigitalIdentity document and the related value presented to the terminal by the eDigitalIdentity document presenter.

A PACE terminal performs the Remote Inspection Procedure (figure 2) and therefore (i) contains a terminal for the communication with the eDigitalIdentity document's chip, (ii) implements the terminal part of the PACE protocol, (iii) authenticates the eDigitalIdentity / travel holder to the eDigitalIdentity document using a shared password (PIN, PUK or CAN) and (iv) implements the Chip Authentication Protocols Version 1 according to [ICAO9303].

The remote terminal authentication, the decryption of sensitive user data and the passive authentication are performed outside of the TOE.

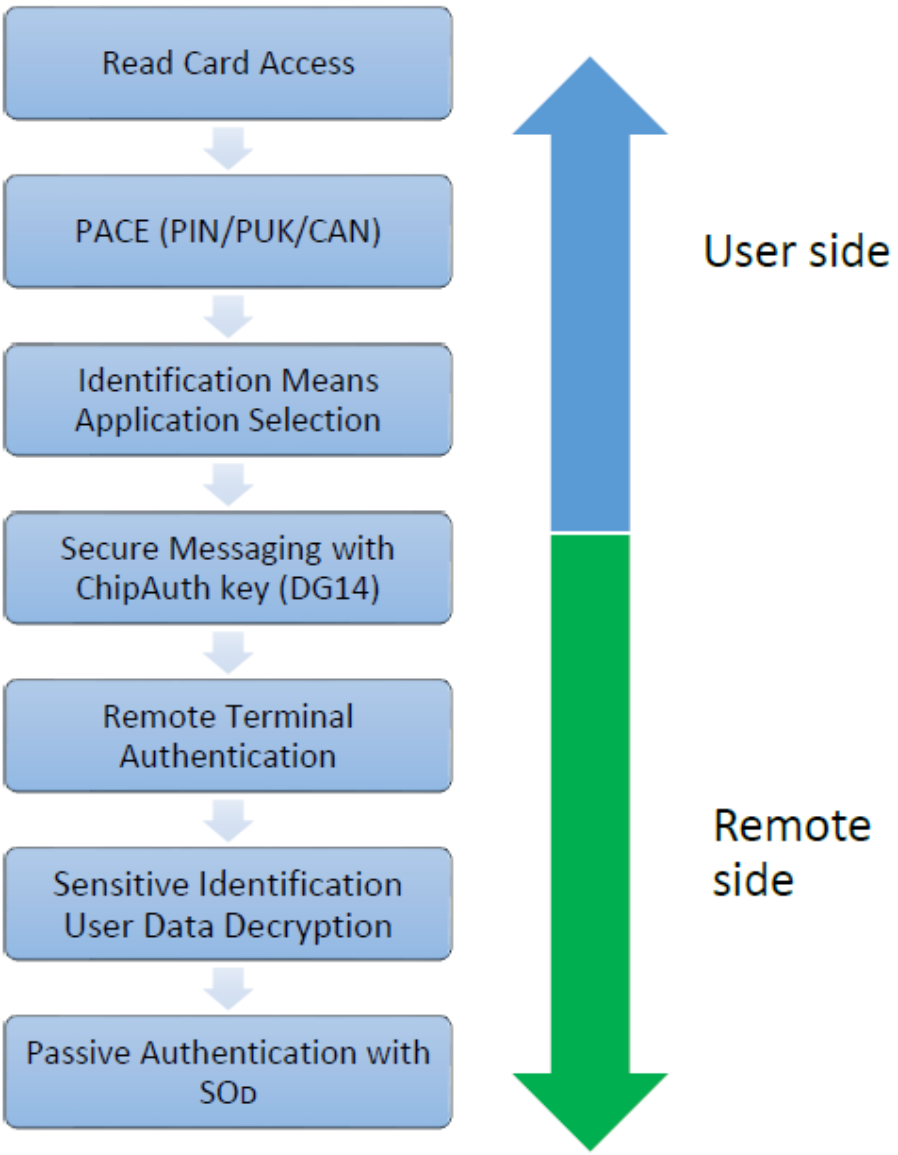


Figure 3 Remote Inspection Procedure

6.2.3 Additional Subjects Identified

EDigitalIdentity document packaging responsible

This additional subject is a refinement of the role Manufacturer as described in [PP_PACE]. This subject is responsible for the combination of the IC with hardware for the contactless and/or contact interface.

Embedded software loading responsible

This additional subject is a refinement of the role Manufacturer as described in [PP_PACE]. This subject is responsible for the embedded software loading when scheme 2 is applied

(cf. § 1.3.6). This subject does not exist if scheme 1 is applied (cf. § 1.3.6). This subject used the Flash loader embedded in the IC.

Pre-personalisation Agent

This additional subject is a refinement of the role Manufacturer as described in [PP_PACE]. This subject is responsible for the preparation of the card, i.e. creation of the MF and MRTD ADF. He also sets Personalisation Agent keys, Administrator keys and Configuration data.

Administrator

The role ADMIN is an Administrator in use phase who can act on the TOE configuration.

The administrative actions are dedicated 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,
- Invalidate one of the Chip Authentication key in USE phase and to set the secondary key as being the primary key.

6.3 Threats

6.3.1 Threats from PP

T.Read_Sensitive_Data

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the eDigitalIdentity document's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [PP_BAC]) in respect of the attack path (communication interface) and the motivation (to get data stored on the eDigitalIdentity document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the eDigitalIdentity document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the eDigitalIdentity document as well.

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

Asset: confidentiality of logical eDigitalIdentity document sensitive user data (i.e. biometric reference.

T.Forgery

Adverse action: An attacker fraudulently alters the User Data or/and TSF-data stored on the eDigitalIdentity document or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated PACE terminal by means of changed eDigitalIdentity document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

Threat agent: having high attack potential.

Asset: integrity of the eDigitalIdentity document.

T.Counterfeit

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

Threat agent: having high attack potential, being in possession of one or more legitimate eDigitalIdentity documents

Asset: authenticity of user data stored on the TOE

T.Abuse-Func

Adverse action: 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 initialisation and personalisation in the operational phase after delivery to the eDigitalIdentity document holder.

Threat agent: having high attack potential, being in possession of one or more legitimate eDigitalIdentity documents integrity and authenticity of the eDigitalIdentity document, availability of the functionality of the eDigitalIdentity document

Asset: integrity and authenticity of the eDigitalIdentity document, availability of the functionality of the eDigitalIdentity document.

Application Note:

Application Note (16 in [PP_PACE]): Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

T.Information_Leakage

Adverse action: 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 travel 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.

Threat agent: having high attack potential.

Asset: confidentiality of User Data and TSF-data of the eDigitalIdentity document.

Application Note:

Application Note (17 in [PP_PACE]): Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission, but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are Differential Electromagnetic Analysis

(DEMA) and Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

T.Phys-Tamper

Adverse action: An attacker may perform physical probing of the eDigitalIdentity 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 eDigitalIdentity 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 eDigitalIdentity document.

Threat agent: having high attack potential, being in possession of one or more legitimate eDigitalIdentity documents

Asset: integrity and authenticity of the eDigitalIdentity document, availability of the functionality of the eDigitalIdentity document, confidentiality of User Data and TSF-data of the eDigitalIdentity document.

Application Note:

Application Note (18 in [PP_PACE]): Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the eDigitalIdentity document) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the eDigitalIdentity document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

T.Malfunction

Adverse action: An attacker may cause a malfunction the eDigitalIdentity 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 eDigitalIdentity document outside the normal operating conditions, exploiting errors in the eDigitalIdentity document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation having information about the functional operation.

Threat agent: having high attack potential, being in possession of one or more legitimate eDigitalIdentity documents, having information about the functional operation

Asset: integrity and authenticity of the eDigitalIdentity document, availability of the functionality of the eDigitalIdentity document, confidentiality of User Data and TSF-data of the eDigitalIdentity document

Application Note:

Application note (19 in [PP_PACE]): A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a

manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals

T.Skimming

Adverse action: An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless/contact interface of the TOE..

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance

Asset: confidentiality of logical eDigitalIdentity document data

Application Note:

Application Note (10 in [PP_PACE]): A product using BIS-BAC cannot avert this threat in the context of the security policy defined in [PP_PACE].

Application Note (11 in [PP_PACE]): MRZ is printed and CAN is printed or stuck on the eDigitalIdentity document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Travel_Document_Holder.

T.Eavesdropping

Adverse action: An attacker is listening to the communication between the eDigitalIdentity document and the PACE authenticated PACE terminal in order to gain the user data transferred between the TOE and the terminal connected.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: confidentiality of logical eDigitalIdentity document data.

Application Note:

Application Note (12 in [PP_PACE]): A product using BIS-BAC cannot avert this threat in the context of the security policy defined in [PP_PACE]

T.Tracing

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

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: privacy of the eDigitalIdentity document holder.

Application Note:

Application Note (13 in [PP_PACE]): This Threat completely covers and extends "T.Chip-ID" from [PP_BAC].

Application Note (14 in [PP_PACE]): A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert this threat in the context of the security policy defined in [PP_PACE], see also the par. 1.2.5 in [PP_PACE].

Application Note (15 in [PP_PACE]): Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the eDigitalIdentity document's chip (no Chip Authentication), a threat like T.Counterfeit (counterfeiting eDigitalIdentity document) cannot be averted by the current TOE.

Application Note: As our TOE supports Chip Authentication in addition to Standard Inspection Procedure, the previous application note extracted from PP does not apply.

6.3.2 Additional Threats as per ADDENDUM

T.Sentitive_ID_User_Data

Adverse action: An attacker tries to gain access to identification user data through the communication interface of the eDigitalIdentity document's chip. The threat T.Sentitive_ID_User_Data is similar to the threat T.Skimming from [PACE/EACPP] w.r.t. the attack path (communication interface) and the motivation (to get data stored on the eDigitalIdentity document's chip) but differs from those in the asset under the attack (identification user data vs. CAN, PIN, PUK and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods.

Threat agent: having high attack potential, knowing the PACE passwords, being in possession of one or more legitimate eDigitalIdentity document

Asset: confidentiality of identification user data stored on the TOE

6.3.3 Additional Threats Identified

T.Configuration

Adverse action: An attacker may access to the TOE at Manufacturing and Personalisation phases (steps 5 and 6) to try to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

Threat agent: having high attack potential, being in possession of one or more MRTD in Pre-personalisation or Personalisation phases.

Asset: authenticity of logical MRTD data.

T.Forgery_Supplemental_Data

Adverse action: An attacker alters fraudulently the data stored in files other than EF.DG1 to EF.DG16, EF.COM and EF document security object. This may lead the extended inspection system (EIS) using these data to be deceived

Threat agent: having high attack potential, being in possession of one or more legitimate MRTDs.

Asset: authenticity of data stored in files other than EF.DG1 to EF.DG16, EF.COM and EF document security object

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.

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.

T.Key_Usage

Adverse action: An attacker may use the internal secret keys of the TOE while the maximum of Key_Usage_Counter is not reached.

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

Asset: TOE internal secret cryptographic keys

6.4 Organisational Security Policies

P.Sensitive_Data

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the eDigitalIdentity document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the eDigitalIdentity document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The eDigitalIdentity document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1.

P.Manufact

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

P.Personalisation

The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical eDigitalIdentity document with respect to the eDigitalIdentity document holder. The personalisation of the eDigitalIdentity document for the holder is performed by an agent authorized by the issuing State or Organisation only.

P.Pre-Operational

1) The eDigitalIdentity document Issuer issues the eDigitalIdentity document and approves it using the terminals complying with all applicable laws and regulations.

2) The eDigitalIdentity document Issuer guarantees correctness of the user data (amongst other of those, concerning the eDigitalIdentity document holder) and of the TSF-data permanently stored in the TOE.

3) The eDigitalIdentity document Issuer uses only such TOE's technical components (IC) which enable traceability of the eDigitalIdentity documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. sec. 1.2.3 in [PP_PACE].

4) If the eDigitalIdentity document Issuer authorises a Personalisation Agent to personalise the eDigitalIdentity document for eDigitalIdentity document holders, the eDigitalIdentity document Issuer has to ensure that the Personalisation Agent acts in accordance with the eDigitalIdentity document Issuer's policy.

P.Card_PKI

1) The eDigitalIdentity document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the eDigitalIdentity document. For this aim, he runs a Country Signing Certification Authority (CSCA). The eDigitalIdentity document Issuer shall publish the CSCA Certificate (CCSCA).

2) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the eDigitalIdentity document Issuer by strictly secure means, see [ICAO_9303], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the eDigitalIdentity document Issuer, see [ICAO_9303], 5.5.1.

3) A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of eDigitalIdentity documents.

Application Note:

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.

P.Trustworthy_PKI

The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the eDigitalIdentity document.

P.Terminal

The Basic Inspection Systems with PACE (PACE terminal) shall operate their terminals as follows:

1) The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by eDigitalIdentity document holders as defined in [ICAO_9303].

2) They shall implement the terminal parts of the PACE protocol [ICAO_9303], of the Passive Authentication [ICAO_9303] and use them in this order28. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3) The related terminals need not to use any own credentials.

4) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the eDigitalIdentity document, [ICAO_9303]).

5) The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to [PP_PACE].

6.5 Assumptions

A.Insp_Sys

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [ICAO_9303] and/or BAC [PP_BAC]. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical eDigitalIdentity document under PACE or BAC and performs the Chip Authentication v1 to verify the logical eDigitalIdentity document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Justification: The assumption A.Insp_Sys does not confine the security objectives of the [PP_PACE] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the EAC functionality of the TOE.

A.Auth_PKI

The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their eDigitalIdentity document's chip.

Justification: This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [PP_PACE] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.

A.Passive_Auth

The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical eDigitalIdentity document. The issuing State or Organisation runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the eDigitalIdentity documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [ICAO_9303].

7 Security Objectives

7.1 Security Objectives for the TOE

7.1.1 Security Objectives from the PP

OT.AC_Pers

Personalisation of the Electronic Document

The TOE must ensure that the logical eDigitalIdentity document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [ICAO_9303] and the TSF data can be written by authorized Personalisation Agents only. The logical eDigitalIdentity document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document.

Application Note:

The OT.AC_Pers implies that the data of the LDS groups written during personalisation for eDigitalIdentity document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.

OT.Data_Integrity

Integrity of Data

The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying).The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated PACE terminal) after the PACE Authentication.

OT.Sens_Data_Conf

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organisation. The TOE must ensure the confidentiality of the logical eDigitalIdentity document data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

OT.Identification

IIdentification of the TOE

The TOE must provide means to store Initialisation 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 eDigitalIdentity document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

OT.Chip_Auth_Proof

The TOE must support the Inspection Systems to verify the identity and authenticity of the eDigitalIdentity document's chip as issued by the identified issuing State or Organisation by means of the Chip Authentication Version 1 as defined in [TR-03110-1] and [TR-03110-3]. The authenticity proof provided by eDigitalIdentity document's chip shall be protected against attacks with high attack potential.

Application Note:

The OT.Chip_Auth_Proof implies the eDigitalIdentity document's chip to have (i) a unique identity as given by the eDigitalIdentity document's number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of eDigitalIdentity document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the eDigitalIdentity document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [SPECDI] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

OT.Prot_Abuse-Func

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.

OT.Prot_Inf_Leak

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 eDigitalIdentity 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.

Application Note:

This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

OT.Prot_Phys-Tamper

Protection against Physical Tampering

The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the eDigitalIdentity 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

- o 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),
- o manipulation of the hardware and its security functionality, as well as
- o controlled manipulation of memory contents (User Data, TSF-data) with a prior
- o reverse-engineering to understand the design and its properties and functionality.

OT.Prot_Malfunction

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.

OT.Data_Authenticity

Authenticity of Data The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side.The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated PACE terminal) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE).

OT.Data_Confidentiality

Confidentiality of Data

The TOE must ensure confidentiality of the User Data and the TSF-data by granting read access only to the PACE authenticated PACE terminal connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated PACE terminal) after the PACE Authentication.

OT.Tracing

Tracing eDigitalIdentity document

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

Application Note:

Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the eDigitalIdentity document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of eDigitalIdentity document authenticity) cannot be achieved by the current TOE.

As our TOE supports Chip Authentication in addition to Standard Inspection Procedure, the previous application note extracted from PP does not apply.

7.1.2 Additional Objectives as per ADDENDUM

OT.Sens_Ident_User_Data_Conf

Confidentiality of sensitive identification user data

The TOE must ensure the confidentiality of sensitive identification user data by granting read access only to authorized Inspection Systems. The authorization of the inspection system is drawn by the eDigitalIdentity document holder by consciously entering his secret PIN. The identification user data may be decrypted to authorized Inspection Systems by the eDigitalIdentity document issuer State or Organisation. The TOE must ensure the confidentiality of the identification user data during their transmission to the Inspection System. The confidentiality of the identification user data shall be protected against attacks with high attack potential.

7.1.3 Additional Objectives for Active Authentication

OT.AA_Proof

The TOE must support the Inspection Systems to verify the identity and authenticity of MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [ICAO_9303]. The authenticity proof through AA provided by MRTD's chip shall be protected against attacks with high attack potential.

OT.Data_Int_AA

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the logical MRTD data during their transmission to the General Inspection System after Active Authentication.

7.1.4 Additional Security Objectives Identified

OT.Configuration

Protection of the TOE preparation

During Pre-personalisation and Personalisation phases, the TOE must control the access to its sensitive information and its functions and must provide the means to secure exchanges using cryptographic functions. It must also ensure secure erasing of useless keys.

OT.Update_File

Modification of file in Operational Use Phase

During Operational Use phase, the TOE must allow the modification of Updatable Data if the write access to these objects is fulfilled by the Terminal.

OT.AC_SM_Level

Access control to sensitive biometric reference data according to SM level

The TOE must protect the Access control to sensitive biometric reference data according to SM level defined.

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.

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.

7.1.5 OT origin

OT	Origin PP/Add/CC
OT.AC_Pers	[PP_EACwPACE]
OT.Data_Integrity	[PP_EACwPACE]
OT.Sens_Data_Conf	[PP_EACwPACE]
OT.Identification	[PP_EACwPACE]
OT.Chip_Auth_Proof	[PP_EACwPACE]
OT.Prot_Abuse-Func	[PP_EACwPACE]
OT.Prot_Inf_Leak	[PP_EACwPACE]
OT.Prot_Phys-Tamper	[PP_EACwPACE]
OT.Prot_Malfunction	[PP_EACwPACE]
OT.Data_Authenticity	[PP_EACwPACE]
OT.Data_Confidentiality	[PP_EACwPACE]
OT.Tracing	[PP_EACwPACE]
OT.AA_Proof	Add
OT.Data_Int_AA	Add
OT.Configuration	Add
OT.Update_File	Add
OT.AC_SM_Level	Add
OT.ADMIN_Configuration	Add
OT.Key_Usage_Counter	Add
T.Sentitive_ID_User_Data	[ADDENDUM]

7.2 Security Objectives for the Operational Environment

7.2.1 EDigitalIdentity document Issuer and CVCA: eDigitalIdentity document's PKI (issuing) branch

The eDigitalIdentity document Issuer and the related CSCA will implement the following security objectives for the TOE environment:

OE.Passive_Auth_Sign

Authentication of eDigitalIdentity document by Signature

The eDigitalIdentity document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the eDigitalIdentity document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (CCSCA). Hereby authenticity and integrity of these certificates are being maintained. A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine eDigitalIdentity documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [ICAO_9303]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [ICAO_9303]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on eDigitalIdentity document.

OE.Personalisation

Personalisation of eDigitalIdentity document

The eDigitalIdentity document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the eDigitalIdentity document holder and create the biographical data for the eDigitalIdentity document, (ii) enrol the biometric reference data of the eDigitalIdentity document holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the eDigitalIdentity document (electronic personalisation) for the eDigitalIdentity document holder as defined in [ICAO_9303], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [ICAO_9303] (in the role of a DS).

7.2.2 Issuing State or Organisation

The issuing State or Organisation will implement the following security objectives of the TOE environment.

OE.Auth_Key_Travel_Document

eDigitalIdentity document Authentication Key

The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the eDigitalIdentity document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data

in EF.DG14 and (iii) support inspection systems of receiving States or Organisations to verify the authenticity of the eDigitalIdentity document's chip used for genuine eDigitalIdentity document by certification of the Chip Authentication Public Key by means of the Document Security Object.

Justification: This security objective for the operational environment is needed additionally to those from [PP_PACE] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE described only in this Protection Profile and not in [PP_PACE].

OE.Authoriz_Sens_Data

Authorization for Use of Sensitive Biometric Reference Data

The issuing State or Organisation has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of eDigitalIdentity document holders to authorized receiving States or Organisations. The Country Verifying Certification Authority of the issuing State or Organisation generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

Justification: This security objective for the operational environment is needed additionally to those from [PP_PACE] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v1 is one of the additional features of the TOE described only in this Protection Profile and not in [PP_PACE].

7.2.3 Receiving State or Organisation

The receiving State or Organisation will implement the following security objectives of the TOE environment.

OE.Exam_Travel_Document

Examination of the physical part of the eDigitalIdentity document

The inspection system of the receiving State or Organisation must examine the travel document presented by the eDigitalIdentity document presenter to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the eDigitalIdentity document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and (ii) implements the terminal part of PACE [ICAO_9303] and/or the Basic Access Control [ICAO_9303]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented eDigitalIdentity document's chip.

Justification: This security objective for the operational environment is needed additionally to those from [PP_PACE] in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v1. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in [PP_PACE] and therefore also counters T.Forgery and A.Passive_Auth from [PP_PACE]. This is done because a new type of Inspection System is introduced in [PP_EACwPACE] as the Extended Inspection System is needed to handle the additional features of a eDigitalIdentity document with Extended Access Control.

OE.Prot_Logical_Travel_Document

Protection of data from the logical eDigitalIdentity document

The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical eDigitalIdentity document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.

Justification: This security objective for the operational environment is needed additionally to those from [PP_PACE] in order to handle the Assumption A.Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v1.

OE.Ext_Insp_Systems

Authorization of Extended Inspection Systems

The Document Verifier of receiving States or Organisations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical eDigitalIdentity document. The Extended Inspection System authenticates themselves to the eDigitalIdentity document's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

Justification: This security objective for the operational environment is needed additionally to those from [PP_PACE] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

7.2.4 EDigitalIdentity document Issuer as the general responsible

The eDigitalIdentity document Issuer as the general responsible for the global security policy related will implement the following security objectives for the TOE environment:

OE.Legislative_Compliance

Issuing of the eDigitalIdentity document

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

7.2.5 Terminal operator: Terminal's receiving branch

OE.Terminal

Terminal operating

The terminal operators must operate their terminals as follows:

1) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by eDigitalIdentity document holders as defined in [ICAO_9303]. 2) The related terminals implement the terminal parts of the PACE protocol [ICAO_9303], of the Passive Authentication [ICAO_9303] (by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann). 3) The related terminals need not to use any own credentials. 4) The

related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_CSCA and C_DS) in order to enable and to perform Passive Authentication of the eDigitalIdentity document (determination of the authenticity of data groups stored in the eDigitalIdentity document, [ICAO_9303]) 5) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the [PP_PACE].

Application Note:

OE.Terminal completely covers and extends "OE.Exam_MRTD", "OE.Passive_Auth_Verif" and "OE.Prot_Logical_MRTD" from [PP_BAC].

7.2.6 EDigitalIdentity document holder Obligations

OE.Travel_Document_Holder

eDigitalIdentity document holder Obligations

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

7.2.7 OE Origin

Security Objectives	Origin PP/Add/CC
OE.Auth_Key_Travel_Document	[PP_EACwPACE]
OE.Authoriz_Sens_Data	[PP_EACwPACE]
OE.Exam_Travel_Document	[PP_EACwPACE]
OE.Prot_Logical_Travel_Document	[PP_EACwPACE]
OE.Ext_Insp_Systems	[PP_EACwPACE]
OE.Legislative_Compliance	[PP_EACwPACE]
OE.Passive_Auth_Sign	[PP_EACwPACE]
OE.Personalisation	[PP_EACwPACE]
OE.Terminal	[PP_EACwPACE]
OE.Travel_Document_Holder	[PP_EACwPACE]

7.3 Security Objectives Rationale

7.3.1 Threats

7.3.1.1 Threats

T.Read_Sensitive_Data The OSP P.Sensitive_Data "Privacy of sensitive biometric reference data"is fulfilled and the threat T.Read_Sensitive_Data "Read the sensitive biometric reference data" is countered by the TOE-objective OT.Sens_Data_Conf "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organisation as required by OE.Authoriz_Sens_Data "Authorization for Use of Sensitive Biometric Reference Data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by OE.Ext_Insp_Systems "Authorization of Extended Inspection Systems".

This threat is also covered by OT.AC_SM_Level "Access control to sensitive biometric reference data according to SM level" that enhences this protection by allowing the issuing State or Organization to require the usage of a secure messaging with a minimum security level for accessing the sensitive biometric reference data. The strength of the secure messaging is tightly bound to the underlying block Cipher involved (3DES, AES-128/192/256). This objective allows an issuing State or Organization to set a secure messaging level it considers as sufficient to ensure a long term confidentiality of the sensitive biometric data of its citizen when being read.

T.Forgery The threat T.Forgery "Forgery of Data" 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 "Access Control for Personalisation of logical MRTD" requires the TOE to limit the write access for the eDigitalIdentity document to the trustworthy Personalisation Agent (cf. OE.Personalisation). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives OT.Data_Integrity "Integrity of Data" and OT.Data_Authenticity "Authenticity of Data", respectively. The objectives OT.Prot_Phys-Tamper "Protection against Physical Tampering" and OT.Prot_Abuse-Func "Protection against Abuse of Functionality" contribute 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 "Terminal operating" and performing the Passive Authentication using the Document Security Object as aimed by OE.Passive_Auth_Sign "Authentication of eDigitalIdentity document by Signature" will be able to effectively verify integrity and authenticity of the data received from the TOE.

Additionally to the security objectives from [PP_PACE] (see above) which counter this threat, the examination of the presented MRTD passport book according to OE.Exam_Travel_Document "Examination of the physical part of the eDigitalIdentity document" shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the eDigitalIdentity document.

T.Counterfeit The threat T.Counterfeit "Counterfeit of eDigitalIdentity document chip data"addresses the attack of unauthorized copy or reproduction of the genuine eDigitalIdentity document's chip. This attack is thwarted by chip an identification and authenticity proof required by OT.Chip_Auth_Proof "Proof of the eDigitalIdentity document's chip authenticity"using an authentication key pair to be generated by the issuing State or Organisation. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by OE.Auth_Key_Travel_Document "eDigitalIdentity document Authentication Key". According to OE.Exam_Travel_Document "Examination of the physical part of the eDigitalIdentity document" the General Inspection system has to perform the Chip Authentication Protocol Version 1 to verify the authenticity of the eDigitalIdentity document's chip. This threat is also covered by OE.Auth_Key_Travel_Document "eDigitalIdentity document Authentication Key"using a authentication key pair to be generated by the issuing State or Organization. This attack is also thwarted by Active Authentication proving the authenticity of the chip as required by OT.AA_Proof and OT.Data_Int_AA using a authentication key pair to be generated by the issuing State or Organization. OE.Activ_Auth_Verif and OE.Activ_Auth_Sign covers also this threat enabling the possibility of performing an Active Authentication which reinforce the security associated to the communication.

T.Abuse-Func The threat T.Abuse-Func "Abuse of Functionality" 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.Prot_Abuse-Func "Protection against Abuse of Functionality" ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

T.Information_Leakage The threat 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 obviously addressed by the directly related security objective OT.Prot_Inf_Leak

T.Phys-Tamper The threat 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 obviously addressed by the directly related security objective OT.Prot_Phys-Tamper

T.Malfunction The threat 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 obviously addressed by the directly related security objective OT.Prot_Malfunction

T.Skimming The threat T.Skimming "Skimming eDigitalIdentity document / Capturing Card-Terminal Communication" addresses accessing the User Data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact interface. This threat is countered by the security objectives OT.Data_Integrity "Integrity of Data", OT.Data_Authenticity "Authenticity of Data" and OT.Data_Confidentiality "Confidentiality of Data" through the PACE authentication. The objective OE.Travel_Document_Holder "eDigitalIdentity document holder Obligations" ensures that a

PACE session can only be established either by the eDigitalIdentity 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.Sens_Ident_User_Data_Conf that demands a trusted channel based on Chip Authentication, and requires that read access to sensitive identification user data is only granted to authorized Inspection Systems.

T.Eavesdropping The threat T.Eavesdropping "Eavesdropping on the communication between the TOE and the PACE terminal" addresses listening to the communication between the TOE and a rightful terminal in order to gain the User Data transferred there. This threat is countered by the security objective OT.Data_Confidentiality "Confidentiality of Data" through a trusted channel based on the PACE authentication.

Additionally, the threat is also addressed by OT.Sens_Ident_User_Data_Conf that demands a trusted channel based on Chip Authentication.

T.Tracing The threat T.Tracing "Tracing eDigitalIdentity document" addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless/contact 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 "Tracing eDigitalIdentity document" (no gathering TOE tracing data) and OE.Travel_Document_Holder "eDigitalIdentity document holder Obligations" (the attacker does not a priori know the correct values of the shared passwords).

7.3.1.2 Additional Threats as per ADDENDUM

T.Sentitive_ID_User_Data The threat T.Sentitive_ID_User_Data is countered by the TOE-Objective OT.Sens_Ident_User_Data_Conf that requires that read access to sensitive user data is only granted to authorized Inspection Systems. Furthermore, it is required that the confidentiality of the data is ensured during transmission.

7.3.1.3 Additional Threats Identified

T.Configuration The threat T.Configuration "Tampering attempt of the TOE during preparation" addresses attacks in Pre-personalisation and Personalisation phases. The attacker trying to access to unauthorized TOE functions, trying to access or to modify sensitive information exchanged between the TOE and the Personalisation system. Protection of the TOE during these two phases is directly addressed by OT.Configuration "Protection of the TOE preparation".

T.Forgery_Supplemental_Data The threat T. Forgery_Supplemental_Data "Forgery of supplemental data stored in the TOE" addresses the fraudulent alteration of Updatable Data. The TOE protects the update of these data thanks to OT.Update_File "Modification of file in Operational Use Phase" that ensures inspection system are authenticated and data

to be updated are sent through a secure channel ensuring integrity, authenticity and confidentiality.

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. Protection of the TOE during this phases is directly addressed by OT.ADMIN_Configuration "Protection of the TOE administration".

T.Key_Usage The threat T.Key_Usage 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.

7.3.1.4 Threats Origin

Threats	Origin PP/Add/CC
T.Read_Sensitive_Data	[PP_EACwPACE]
T.Forgery	[PP_EACwPACE]
T.Counterfeit	[PP_EACwPACE]
T.Abuse-Func	[PP_EACwPACE]
T.Information_Leakage	[PP_EACwPACE]
T.Phys-Tamper	[PP_EACwPACE]
T.Malfunction	[PP_EACwPACE]
T.Skimming	[PP_EACwPACE]
T.Eavesdropping	[PP_EACwPACE]
T.Tracing	[PP_EACwPACE]
T.Configuration	Add
T.Forgery_Supplemental_Data	Add
T.ADMIN_Configuration	Add
T.Key_Usage	Add
T.Sentitive_ID_User_Data	[ADDENDUM]

7.3.2 Organisational Security Policies

P.Sensitive_Data The OSP P.Sensitive_Data "Privacy of sensitive biometric reference data"is fulfilled and the threat T.Read_Sensitive_Data "Read the sensitive biometric reference data" is countered by the TOE-objective OT.Sens_Data_Conf "Confidentiality of sensitive

biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organisation as required by OE.Authoriz_Sens_Data "Authorization for Use of Sensitive Biometric Reference Data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by OE.Ext_Insp_Systems "Authorization of Extended Inspection Systems".

This threat is also covered by OT.AC_SM_Level "Access control to sensitive biometric reference data according to SM level" that enhences this protection by allowing the issuing State or Organization to require the usage of a secure messaging with a minimum security level for accessing the sensitive biometric reference data. The strength of the secure messaging is tightly bound to the underlying block Cipher involved (3DES, AES-128/192/256). This objective allows an issuing State or Organization to set a secure messaging level it considers as sufficient to ensure a long term confidentiality of the sensitive biometric data of its citizen when being read

P.Manufact The OSP P.Manufact "Manufacturing of the eDigitalIdentity 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 "Identification of the TOE".

P.Personalisation The OSP P.Personalisation "Personalisation of the travel document by issuing State or Organisation only" addresses the (i) the enrolment of the logical eDigitalIdentity document by the Personalisation Agent as described in the security objective for the TOE environment OE.Personalisation "Personalisation of eDigitalIdentity document", and (ii) the access control for the user data and TSF data as described by the security objective OT.AC_Pers "Access Control for Personalisation of logical MRTD" Note the manufacturer equips the TOE with the Personalisation Agent Key(s) according to OT.Identification "Identification of the TOE". The security objective OT.AC_Pers "Access Control for Personalisation of logical MRTD" limits the management of TSF data and the management of TSF to the Personalisation Agent.

P.Pre-Operational The OSP P.Pre-Operational "Pre-operational handling of the eDigitalIdentity document" is enforced by the following security objectives: OT.Identification "Identification of the TOE" is affine to the OSP's property 'traceability before the operational phase'; OT.AC_Pers "Access Control for Personalisation of logical MRTD" and OE.Personalisation "Personalisation of eDigitalIdentity document" together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorisation of Personalisation Agents'; OE.Legislative_Compliance "Issuing of the eDigitalIdentity document" is affine to the OSP's property 'compliance with laws and regulations'.

P.Card_PKI The OSP P.Card_PKI "PKI for Passive Authentication (issuing branch)" is enforced by establishing the issuing PKI branch as aimed by the objectives

OE.Passive_Auth_Sign "Authentication of eDigitalIdentity document by Signature" (for the Document Security Object).

P.Trustworthy_PKI The OSP P.Trustworthy_PKI "Trustworthiness of PKI" is enforced by OE.Passive_Auth_Sign "Authentication of eDigitalIdentity document by Signature" (for CSCA, issuing PKI branch).

P.Terminal The OSP P.Terminal "Abilities and trustworthiness of terminals" is obviously enforced by the objective OE.Terminal "Terminal operating", whereby the one-to-one mapping between the related properties is applicable.

The OSP P.Terminal "Abilities and trustworthiness of terminals" is countered by the security objective OE.Exam_Travel_Document "Examination of the physical part of the eDigitalIdentity document" additionally to the security objectives from [PP_PACE] (see above). OE.Exam_Travel_Document "Examination of the physical part of the eDigitalIdentity document" enforces the terminals to perform the terminal part of the PACE protocol.

7.3.3 OSP Origin

OSP	Origin PP/Add/CC
P.Sensitive_Data	[PP_EACwPACE]
P.Manufact	[PP_EACwPACE]
P. Personalisation	[PP_EACwPACE]
P.Pre-Operational	[PP_EACwPACE]
P.Card_PKI	[PP_EACwPACE]
P.Trustworthy_PKI	[PP_EACwPACE]
P.Terminal	[PP_EACwPACE]

7.3.4 Assumptions

A.Insp_Sys The examination of the eDigitalIdentity document addressed by the assumption A.Insp_Sys "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment OE.Exam_Travel_Document "Examination of the physical part of the eDigitalIdentity document"which requires the inspection system to examine physically the eDigitalIdentity document, the Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented eDigitalIdentity document's chip. The security objectives for the TOE environment OE.Prot_Logical_Travel_Document "Protection of data from the logical

eDigitalIdentity document" require the Inspection System to protect the logical eDigitalIdentity document data during the transmission and the internal handling.

A.Auth_PKI The assumption A.Auth_PKI "PKI for Inspection Systems" is covered by the security objective for the TOE environment OE.Authoriz_Sens_Data "Authorization for Use of Sensitive Biometric Reference Data" requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organisations only. The Document Verifier of the receiving State is required by OE.Ext_Insp_Systems "Authorization of Extended Inspection Systems" to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organisation has to establish the necessary public key infrastructure

A.Passive_Auth The assumption A.Passive_Auth "PKI for Passive Authentication" is directly covered by the security objective for the TOE environment OE.Passive_Auth_Sign "Authentication of eDigitalIdentity document by Signature" from [PP_PACE] covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by OE.Exam_Travel_Document "Examination of the physical part of the eDigitalIdentity document".

7.3.5 Assumptions Origin

Assumptions	Origin PP/Add/CC
A.Insp_Sys	[PP_EACwPACE]
A.Auth_PKI	[PP_EACwPACE]
A.Passive_Auth	[PP_EACwPACE]

7.3.6 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Read_Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems, OT.AC_SM_Level	Section 7.3.1
T.Forgery	OT.AC_Pers, OT.Data_Authenticity, OT.Data_Integrity, OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper, OE.Personalisation, OE.Passive_Auth_Sign, OE.Terminal, OE.Exam_Travel_Document	Section 7.3.1
T.Counterfeit	OT.Chip_Auth_Proof, OE.Auth_Key_Travel_Document, OE.Exam_Travel_Document, OT.AA_Proof, OT.Data_Int_AA	Section 7.3.1
T.Abuse-Func	OT.Prot_Abuse-Func	Section 7.3.1
T.Information_Leakage	OT.Prot_Inf_Leak	Section 7.3.1

T.Phys-Tamper	OT.Prot_Phys-Tamper	Section 7.3.1
T.Malfunction	OT.Prot_Malfunction	Section 7.3.1
T.Skimming	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OE.Travel_Document_Holder, OT.Sens_Ident_User_Data_Conf	Section 7.3.1
T.Eavesdropping	OT.Data_Confidentiality, OT.Sens_Ident_User_Data_Conf	Section 7.3.1
T.Tracing	OT.Tracing, OE.Travel_Document_Holder	Section 7.3.1
T.Sentitive_ID_User_Data	OT.Sens_Ident_User_Data_Conf	Section 7.3.1
T.Configuration	OT.Configuration	Section 7.3.1
T.Forgery_Supplemental_Data	OT.Update_File	Section 7.3.1
T.ADMIN_Configuration	OT.ADMIN_Configuration	Section 7.3.1
T.Key_Usage	OT.Key_Usage_Counter	Section 7.3.1

Table 15 Threats and Security Objectives - Coverage

Security Objectives	Threats	Rationale
OT.AC_Pers	T.Forgery	
OT.Data_Integrity	T.Forgery, T.Skimming	
OT.Sens_Data_Conf	T.Read_Sensitive_Data	
OT.Identification		
OT.Chip_Auth_Proof	T.Counterfeit	
OT.Prot_Abuse-Func	T.Forgery, T.Abuse-Func	
OT.Prot_Inf_Leak	T.Information_Leakage	
OT.Prot_Phys-Tamper	T.Forgery, T.Phys-Tamper	
OT.Prot_Malfunction	T.Malfunction	
OT.Data_Authenticity	T.Forgery, T.Skimming	
OT.Data_Confidentiality	T.Skimming, T.Eavesdropping	
OT.Tracing	T.Tracing	
OT.Sens_Ident_User_Data_Conf	T.Skimming, T.Eavesdropping, T.Sentitive_ID_User_Data	
OT.AA_Proof	T.Counterfeit	
OT.Data_Int_AA	T.Counterfeit	
OT.Configuration	T.Configuration	
OT.Update_File	T.Forgery_Supplemental_Data	
OT.AC_SM_Level	T.Read_Sensitive_Data	

OT.ADMIN_Configuration	T.ADMIN_Configuration	
OT.Key_Usage_Counter	T.Key_Usage	
OE.Passive_Auth_Sign	T.Forgery	
OE.Personalisation	T.Forgery	
OE.Auth_Key_Travel_Document	T.Counterfeit	
OE.Authoriz_Sens_Data	T.Read_Sensitive_Data	
OE.Exam_Travel_Document	T.Forgery, T.Counterfeit	
OE.Prot_Logical_Travel_Document		
OE.Ext_Insp_Systems	T.Read_Sensitive_Data	
OE.Legislative_Compliance		
OE.Terminal	T.Forgery	
OE.Travel_Document_Holder	T.Skimming, T.Tracing	

Table 16 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems, OT.AC_SM_Level	Section 7.3.2
P.Manufact	OT.Identification	Section 7.3.2
P.Personalisation	OT.AC_Pers, OT.Identification, OE.Personalisation	Section 7.3.2
P.Pre-Operational	OT.Identification, OT.AC_Pers, OE.Personalisation, OE.Legislative_Compliance	Section 7.3.2
P.Card_PKI	OE.Passive_Auth_Sign	Section 7.3.2
P.Trustworthy_PKI	OE.Passive_Auth_Sign	Section 7.3.2
P.Terminal	OE.Terminal, OE.Exam_Travel_Document	Section 7.3.2

Table 17 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
OT.AC_Pers	P.Personalisation, P.Pre-Operational
OT.Data_Integrity	
OT.Sens_Data_Conf	P.Sensitive_Data
OT.Identification	P.Manufact, P.Personalisation, P.Pre-Operational
OT.Chip_Auth_Proof	
OT.Prot_Abuse-Func	

OT.Prot_Inf_Leak	
OT.Prot_Phys-Tamper	
OT.Prot_Malfunction	
OT.Data_Authenticity	
OT.Data_Confidentiality	
OT.Sens_Ident_User_Data_Conf	
OT.Tracing	
OT.AA_Proof	
OT.Data_Int_AA	
OT.Configuration	
OT.Update_File	
OT.AC_SM_Level	P.Sensitive_Data
OT.ADMIN_Configuration	
OT.Key_Usage_Counter	
OE.Passive_Auth_Sign	P.Card_PKI, P.Trustworthy_PKI
OE.Personalisation	P.Personalisation, P.Pre-Operational
OE.Auth_Key_Travel_Document	
OE.Authoriz_Sens_Data	P.Sensitive_Data
OE.Exam_Travel_Document	P.Terminal
OE.Prot_Logical_Travel_Document	
OE.Ext_Insp_Systems	P.Sensitive_Data
OE.Legislative_Compliance	P.Pre-Operational
OE.Terminal	P.Terminal
OE.Travel_Document_Holder	

Table 18 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.Insp_Sys	OE.Exam_Travel_Document, OE.Prot_Logical_Travel_Document	Section 7.3.3
A.Auth_PKI	OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 7.3.3
A.Passive_Auth	OE.Passive_Auth_Sign, OE.Exam_Travel_Document	Section 7.3.3

Table 19 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions
OE.Passive_Auth_Sign	A.Passive_Auth
OE.Personalisation	
OE.Auth_Key_Travel_Document	
OE.Authoriz_Sens_Data	A.Auth_PKI
OE.Exam_Travel_Document	A.Insp_Sys, A.Passive_Auth
OE.Prot_Logical_Travel_Document	A.Insp_Sys
OE.Ext_Insp_Systems	A.Auth_PKI
OE.Legislative_Compliance	
OE.Terminal	
OE.Travel_Document_Holder	

Table 20 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.

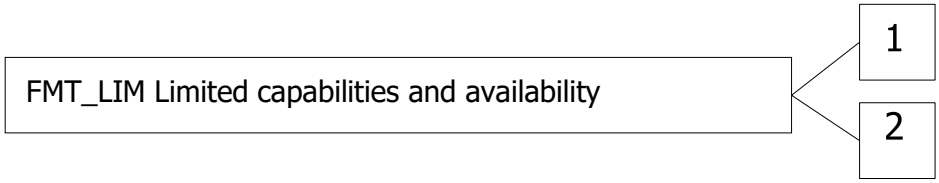
8.1.2.2 Extended Components

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 FAU_SAS - Audit data storage

8.1.4.1 Description

To describe the security functional requirements of the TOE, the family FAU_SAS of the class FAU (Security audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

The family 'Audit data storage (FAU_SAS)' is specified as follows:

FAU_SAS Audit data storage

Family behavior

This family defines functional requirements for the storage of audit data.

Component levelling

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

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

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

FAU_SAS.1 Audit storage

FAU_SAS.1.1: The TSF shall provide [assignment: authorised users] with the capability to store [assignment: list of audit information] in the audit records.

Hierarchical to: No other components

Dependencies: No Depenedencies

8.1.5 Extended Family FCS_RND - Generation of random numbers

8.1.5.1 Description

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

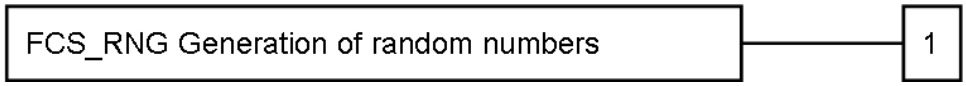
8.1.5.2 Extended Components

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.

9.1.1 Class FAU Security Audit

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide **the Manufacturer** with the capability to store **the Initialisation and Pre-Personalisation Data** in the audit records.

9.1.2 Class FCS Cryptographic Support

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 **ECDH compliant to [TR-03111]** and specified cryptographic key sizes **192 to 521 bit** that meet the following: **[ICAO_9303]**.

FCS_CKM.1/CA Cryptographic key generation

FCS_CKM.1.1/CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **see table below** and specified cryptographic key sizes **see table below** that meet the following: **see table below:**

Key Generation Algorithm	Key Sizes	Standard
based on ECDH compliant to [ISO11770-3]	192 to 521 bit	[TR-03111]
based on DH	1024, 1536 and 2048	[TR-03110-3] and PKCS#3

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 **zeroisation** that meets the following: **none**.

FCS_COP.1/PACE_ENC Cryptographic operation

FCS_COP.1.1/PACE_ENC The TSF shall perform **refer to table below** in accordance with a specified cryptographic algorithm **refer to table below** and cryptographic key sizes **refer to table below** that meet the following: **refer to table below**

Cryptographic Operations	Algorithms	Key sizes	Norms
secure messaging-encryption and decryption	AES in CBC mode	128, 192 and 256 bits	[ICAO_9303]
secure messaging-encryption and decryption	TDES in CBC mode	112 bits	[ICAO_9303]

FCS_COP.1/PACE_MAC Cryptographic operation

FCS_COP.1.1/PACE_MAC The TSF shall perform **refer table below** in accordance with a specified cryptographic algorithm **refer table below** and cryptographic key sizes **refer table below** that meet the following: **refer table below**

Cryptographic Operations	Algorithms	Key sizes	Norms
secure messaging - message authentication code	AES CMAC	128, 192 and 256 bits	[ICAO_9303]
secure messaging - message authentication code	Retail MAC	112 bits	[ICAO_9303]

FCS_COP.1/CA_ENC Cryptographic operation

FCS_COP.1.1/CA_ENC The TSF shall perform **refer to table below** in accordance with a specified cryptographic algorithm **refer to table below** and cryptographic key sizes **refer to table below** that meet the following: **refer to table below**

Cryptographic Operations	Algorithms	Key sizes	Norms
secure messaging-encryption and decryption	AES in CBC mode	128, 192 and 256 bits	[TR-03110-3]
secure messaging-encryption and decryption	TDES in CBC mode	112 bits	[TR-03110-3]

FCS_COP.1/SIG_VER Cryptographic operation

FCS_COP.1.1/SIG_VER The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

Cryptographic Operation	Algorithm	Key Sizes
digital signature verification	ECDSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 as defined in [FIPS_186_3]	192 to 512
digital signature verification	RSA PKCS#1 v1.5 with SHA-1, SHA-256 and SHA-512	1024, 1536 and 2048
digital signature verification	RSA PKCS#1-PSS with SHA-1, SHA-256 and SHA-512	1024, 1536 and 2048

FCS_COP.1/CA_MAC Cryptographic operation

FCS_COP.1.1/CA_MAC The TSF shall perform **refer table below** in accordance with a specified cryptographic algorithm **refer table below** and cryptographic key sizes **refer table below** that meet the following: **refer table below**

Cryptographic Operations	Algorithms	Key sizes	Norms
secure messaging - message authentication code	AES CMAC	128, 192 and 256 bits	[TR-03110-3]
secure messaging - message authentication code	Retail MAC	112 bits	[TR-03110-3]

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **the average Shannon entropy per internal random bit exceeds 0.994**.

9.1.3 Additional FCS SFR's Identified

FCS_CKM.1/CAM Cryptographic key generation

FCS_CKM.1.1/CAM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **based on ECDH compliant to [ISO11770-3]** and specified cryptographic key sizes **192 to 521 bit** that meet the following: **[TR-03110-3]**.

FCS_CKM.1/CA_DATA_GEN Cryptographic key generation

FCS_CKM.1.1/CA_DATA_GEN The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **see table below** and specified cryptographic key sizes **see table below** that meet the following: **see table below**

Algorithm	Key Size	Standard
Chip Authentication Data Generation using DH keys compliant to PKCS#3	1024 to 2048 bits in steps of 512 bits	PKCS#3
Chip authentication data generation using ECDH keys compliant to [ISO11770-3]	192 to 521 bits	[TR-03111]

FCS_CKM.1/GP Cryptographic key generation

FCS_CKM.1.1/GP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **see table below** and specified cryptographic key sizes **see table below** that meet the following: **see table below:**

Key Generation Algorithm	Key Sizes	Standard
Triple-DES in CBC mode	112 bit	[GPC_SPE_034]
AES in CBC mode	128, 192 and 256	[GPC_SPE_014]

FCS_COP.1/GP_ENC Cryptographic operation

FCS_COP.1.1/GP_ENC The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below:**

Cryptographic Operation	Algorithm	Key Sizes	Standard
secure messaging (GP) – encryption and decryption	Triple-DES in CBC mode	112 bit	[FIPS_46_3]
secure messaging (GP) – encryption and decryption	AES in CBC mode	128, 192 and 256 bits	[NIST_800_38A]

FCS_COP.1/GP_MAC Cryptographic operation

FCS_COP.1.1/GP_MAC The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below:**

Cryptographic Operation	Algorithm	Key Sizes	Standard

secure messaging – message authentication code	Retail MAC	112 bit	[ISO_9797_1]
secure messaging – message authentication code	AES CMAC	128, 192 and 256 bits	[NIST_800_38B]

FCS_COP.1/GP_AUTH Cryptographic operation

FCS_COP.1.1/GP_AUTH The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below:**

Cryptographic Operation	Algorithm	Key Sizes	Standard
symmetric authentication – message authentication code	Full 3DES MAC	112 bit	[ISO_9797_1]
symmetric authentication – message authentication code	AES CMAC	128, 192 and 256 bits	[NIST_800_38B]

Application Note:

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

FCS_COP.1/GP_KEY_DEC Cryptographic operation

FCS_COP.1.1/GP_KEY_DEC The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below:**

Cryptographic Operation	Algorithm	Key Sizes	Standard
key decryption	Triple-DES in ECB mode	112 bit	[FIPS_46_3]
key decryption	AES in CBC mode	128, 192 and 256 bits	[FIPS_197]

FCS_COP.1/AA Cryptographic operation

FCS_COP.1.1/AA The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below:**

Cryptographic Operation	Cryptographic Algorithm	Cryptographic Key Sizes(bits)	Standard

Digital Signature Creation	ECDSA with SHA1, 256, 384, 512	192 to 521 over prime field curves	[ISO_9796-2], [PKCS#3], [FIPS_180_4] and [X.92]
Digital Signature Creation	RSA signature (CRT) with SHA1, 256, 384, 512	1024, 1536 and 2048	[ISO_9796-2]

9.1.4 Class FDP User Data Protection

FDP_ACC.1/TRM Subset access control

FDP_ACC.1.1/TRM The TSF shall enforce the **Access Control SFP** on **terminals gaining access to user data and data stored in EF.SOD of the logical eDigitalIdentity document**.

FDP_ACF.1/TRM Security attribute based access control

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

1) Subjects:

a) Terminal,

b) PACE terminal,

c) Extended Inspection System

2) Objects:

a) data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16,EF.SOD and EF.COM of the logical eDigitalIdentity document,

b) data in EF.DG3 of the logical eDigitalIdentity document,

c) data in EF.DG4 of the logical eDigitalIdentity document,

d) all TOE intrinsic secret cryptographic keys stored in the eDigitalIdentity document

3) Security attributes:

a) PACE PIN Authentication

b) Chip Authentication v1

c) Terminal Authentication v1

d) Authorisation of the Terminal.

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

- **A PACE terminal is allowed to read data objects from FDP_ACF.1/TRM according to [ICAO_9303] after at least a successful PACE authentication as required by FIA_UAU.1/PACE**
- **A PACE Terminal is allowed to read data objects 2a) of FDP_ACF.1.1/TRM according to [SPECDI] only after a successful PACE authentication followed by Chip Authentication v1 as required by FIA_UAU.1/PACE. Data object 2a) may also require terminal authentication v1. This rule is not applicable for EF.DG14.**
- **A PACE Terminal is allowed to read data objects 2b) and 2c) of FDP_ACF.1.1/TRM according to [SPECDI] only after a successful PACE**

authentication followed by Chip Authentication v1 and Terminal Authentication v1 as required by FIA_UAU.1/PACE.

Refinement:

The TOE can be configured to restrict access to data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical eDigitalIdentity document to a successful PACE Authentication followed by a successful Chip Authentication.

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:

1) Any terminal being not authenticated at least as PACE authenticated PACE terminal is not allowed to read, to write, to modify, to use any User Data stored on the eDigitalIdentity document.

2) Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the eDigitalIdentity document.

3) Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.

4) Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.

5) Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.

6) Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.

7) Moreover, the Extended Inspection System shall communicate with at least the minimum secure messaging level identified at the creation of the DG3 and DG4, to be able to read these DGs.

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:

- **Session Keys (immediately after closing related communication session),**
- **the ephemeral private key ephem-SK picc -PACE (by having generated a DH shared secret K)**
- **PIN and PUK**.

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.

9.1.5 Additional FDP SFR's Identified

FDP_ACC.1/UPD_FILE Subset access control

FDP_ACC.1.1/UPD_FILE The TSF shall enforce the **UPD_FILE Access Control SFP** on **terminals gaining write, read and modification access to data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**.

FDP_ACF.1/UPD_FILE Security attribute based access control

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

- **Subjects:**
  - **Personalisation Agent,**
  - **Extended Inspection System**
  - **Terminal,**
- **Objects:**
  - **data in the file(s)EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**
- **Security attributes**
  - **authentication status of terminals**.

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

- **the Personalisation Agent is allowed to write, read and modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD,**

- o **the successfully authenticated Extended Inspection System following FMT_MTD.1.1/UPD_FILE is allowed to modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**.

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

FDP_ACF.1.4/UPD_FILE The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Any Terminal is not allowed to modify the data in the file(s) EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**.

FDP_DAU.1/AA Basic Data Authentication

FDP_DAU.1.1/AA The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **the TOE itself**.

FDP_DAU.1.2/AA The TSF shall provide **any users** with the ability to verify evidence of the validity of the indicated information.

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

FDP_ITC.1.1/AA The TSF shall enforce the **Active Authentication Access Control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/AA The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **None**.

9.1.6 Class FIA Identification and Authentication

FIA_UID.1/PACE Timing of identification

FIA_UID.1.1/PACE The TSF shall allow

- **To establish a communication channel,**
- **Carrying out the PACE protocol according to [ICAO_9303],**
- **To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS**
- **To carry out the Chip Authentication Protocol v1 according to [TR-03110-1] and [TR-03110-3]**
- **To carry out the Terminal Authentication Protocol v1 according to [TR-03110-1] and [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,**
- **carrying out the PACE Protocol according to [ICAO_9303]**
- **to read the Initialization Data if it is not disable by TSF according to FMT_MTD.1/INI_DIS,**
- **to identify themselves by selection of the authentication key**
- **to carry out the Chip Authentication Protocol v1 according to [TR-03110-1] and [TR-03110-3]**
- **To carry out the Terminal Authentication Protocol v1 according to [TR-03110-1] and [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 according to [ICAO_9303],**
- **Authentication Mechanisms based on Triple-DES and AES**

- **Terminal Authentication Protocol v1 according to [TR-03110-1] and [TR-03110-3]**.

Application Note:

The authentication mechanisms based on Triple-DES and 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 according to [ICAO_9303]],**
- **Passive Authentication according to [ICAO_9303],**
- **Secure messaging in MAC-ENC mode according to [ICAO_9303]**
- **Symmetric Authentication Mechanism based on Triple-DES and AES**
- **Terminal Authentication Protocol v1 according to [TR-03110-1] and [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 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 TOE accepts the authentication attempt as Personalisation Agent by the Authentication Mechanism with Personalisation Agent Key(s).**
- **After run of the Chip Authentication Protocol v1 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 as Administrator by the Authentication Mechanism with Administrator Key(s)**.

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 v1 shall be verified as being sent by the Inspection System**.

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 PACE terminal**.

FIA_AFL.1/PACE Authentication failure handling

FIA_AFL.1.1/PACE The TSF shall detect when **10** unsuccessful authentication attempts occur related to **authentication attempts using the PACE password as shared password**.

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **wait for an increasing time between receiving of the terminal challenge and sending of the TSF response during the PACE authentication attempts**.

Application Note:

The PACE password being referred here are MRZ or CAN.

9.1.7 Additional FIA SFRs identified as per ADDENDUM

FIA_API.1/TOE Authentication Proof of Identity

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

Application Note:

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

9.1.8 Additional FIA SFR's Identified

FIA_AFL.1/MP Authentication failure handling

FIA_AFL.1.1/MP The TSF shall detect when **1** unsuccessful authentication attempts occur related to **authentication of the Manufacturer and the Personalisation Agent**.

FIA_AFL.1.2/MP When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **slow down exponentially the next authentication**.

FIA_API.1/CA Authentication Proof of Identity

FIA_API.1.1/CA The TSF shall provide a **Chip Authentication Protocol v1 according to [TR-03110-1] and [TR-03110-3]** to prove the identity of the **TOE**.

FIA_UAU.6/MP Re-authenticating

FIA_UAU.6.1/MP The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful authentication of the terminal with the Symmetric Authentication Mechanism shall be verified as being sent by the authenticated terminal**.

9.1.9 Class FMT Security Management

FMT_SMF.1 Specification of Management Functions

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

- **Initialization,**
- **Pre-personalisation,**
- **Personalisation,**
- **Configuration,**
- **Administration,**
- **Basic Access Control expiration,**
- **Initialize, and Resume and Unblock the PIN and PUK.**
- **Change the PIN.**

Application Note:

This SFR is an extension of the SFR 'FMT_SMF.1' defined in [PP_PACE]. It is here refined by including mechanisms for PIN management (Initialization, Resume and unblock the PIN and PUK). This extension does not conflict with the strict conformance to [PP_PACE] and [PP_EACwPACE].

FMT_SMR.1/PACE Security roles

FMT_SMR.1.1/PACE The TSF shall maintain the roles

- **Manufacturer,**
- **Personalisation Agent,**
- **Terminal,**
- **PACE authenticated PACE terminal**

- **Country Verifying Certificate Authority,**
- **Document Verifier,**
- **Domestic Extended Inspection System,**
- **Foreign Extended Inspection System,**
- **Administrator**

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

Application Note:

This SFR also applies to the refinement of the role Manufacturer and to the additional role Administrator.

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 do not allow

- **User Data to be manipulated and disclosed,**
- **TSF data to be manipulated or disclosed,**
- **software to be reconstructed,**
- **substantial information about construction of TSF to be gathered which may enable other attacks,**
- **sensitive User Data (EF.DG3 and EF.DG4) to be disclosed**

FMT_LIM.2 Limited capabilities

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 do not allow

- **User Data to be manipulated and disclosed,**
- **TSF data to be manipulated or disclosed,**
- **software to be reconstructed,**
- **substantial information about construction of TSF to be gathered which may enable other attacks,**
- **sensitive User Data (EF.DG3 and EF.DG4) to be disclosed**

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**.

Application Note:

Please refer to F.ACW for details of the data written by 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_MTD.1/PA Management of TSF data

FMT_MTD.1.1/PA The TSF shall restrict the ability to **write** the **document Security Object (SO D)** to **the Personalisation Agent**.

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**
- **none**

to **the Personalisation 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**
- **Document Verifier**
- **Domestic Extended Inspection System**.

FMT_MTD.1/CAPK Management of TSF data

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to **load or create** the **Chip Authentication private key** to **the personalization agent or the admin**.

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,**
- **Manufacturer Keys**
- **Pre-personalisation Agent Keys,**
- **Personalisation Agent Keys,**
- **Chip Authentication Private Key**
- **Administrator Keys**

to **none**.

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 [Editorially Refined] The TSF shall ensure that only secure values of the certificate chain are accepted for **TSF data of the Terminal Authentication Protocol v1 and the Access Control**.

Refinement:

The certificate chain is valid if and only if

- the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,
- the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,

- the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE.

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

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

9.1.10 Additional FMT SFRs identified as per ADDENDUM

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 and PUK** to **the Personalisation 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 the PUK** to **the eDigitalIdentity document holder**.

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** to **eDigitalIdentity document holder**.

FMT_MTD.1/Unblock_PIN Management of TSF data

FMT_MTD.1.1/Unblock_PIN The TSF shall restrict the ability to **unblock** the **blocked PIN** to **the eDigitalIdentity document holder (using the PUK for unblocking)**.

9.1.11 Additional FMT SFR's Identified

FMT_MTD.1/PACE_PWD Management of TSF data

FMT_MTD.1.1/PACE_PWD The TSF shall restrict the ability to **load** the **PACE Password** to **Personalisation Agent**.

FMT_MTD.1/LCS_PERS Management of TSF data

FMT_MTD.1.1/LCS_PERS The TSF shall restrict the ability to **switch** the **LCS from phase 6 to phase 7** to **the Personalisation Agent**.

FMT_MTD.1/UPD_FILE Management of TSF data

FMT_MTD.1.1/UPD_FILE The TSF shall restrict the ability to **set** the **identifiers of files that can be modified in phase 7 (different from EF.COM, EF.SOD, EF.DG1 to EF.DG16)** to **the Personalisation Agent**.

FMT_MTD.1/SM_LVL_DG3_DG4 Management of TSF data

FMT_MTD.1.1/SM_LVL_DG3_DG4 The TSF shall restrict the ability to **set** the **minimum Secure Messaging level required to access DG3 and DG4** to **Personalisation Agent**.

Application Note:

Possible secure messaging levels are: 3DES, AES 128, AES 192 or AES 256

FMT_MTD.1/SM_LVL Management of TSF data

FMT_MTD.1.1/SM_LVL The TSF shall restrict the ability to **set** the **allowed Secure Messaging level when performing PACE and Chip Authentication** to **Personalisation Agent**.

Application Note:

Possible secure messaging levels are: 3DES, AES 128, AES 192 or AES 256

FMT_MTD.1/AA_KEY_READ Management of TSF data

FMT_MTD.1.1/AA_KEY_READ The TSF shall restrict the ability to **read** the **AA_SK** to **none**.

FMT_MTD.1/AA_KEY_WRITE Management of TSF data

FMT_MTD.1.1/AA_KEY_WRITE The TSF shall restrict the ability to **write** the **AA_SK** to **Personalisation Agent**.

FMT_MTD.1/ADMIN Management of TSF data

FMT_MTD.1.1/ADMIN The TSF shall restrict the ability to **see table below** the **see table below** to **Admin**

Operation	TSF Data
Modify	The Chip Authentication key parameters to be used during key generation 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/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_MOF.1/GP Management of security functions behaviour

FMT_MOF.1.1/GP The TSF shall restrict the ability to **enable** the functions

- **transmission of user data in a manner protected from unauthorized disclosure,**
- **reception of user data in a manner protected from unauthorized disclosure,**
- **transmission of user data in a manner protected from modification, deletion, insertion and replay errors,**
- **reception of user data in a manner protected from modification, deletion, insertion and replay errors,**

to **the Manufacturer, Administrator and Personalisation agent**.

FMT_MOF.1/AA Management of security functions behaviour

FMT_MOF.1.1/AA The TSF shall restrict the ability to **enable and disable** the functions **TSF Active Authentication** to **Personalisation Agent**.

9.1.12 Class FPT Protection of the Security Functions

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to

- **Chip Authentication Session Keys,**
- **PACE session keys (PACE-K mac, PACE-K enc),**
- **The ephemeral private key ephem SK picc -PACE,**
- **The ephemeral private key SK Map ,**
- **Personalisation Agent Key(s),**
- **Chip Authentication Private Key,**
- **Active Authentication Private Key (AA_SK).**
- **Administrator authentication Key(s)**.

FPT_EMS.1.2 The TSF shall ensure **users** are unable to use the following interface **smart card circuit contacts** to gain access to

- **Chip Authentication Session Keys,**
- **PACE session keys (PACE-K mac, PACE-K enc),**
- **The ephemeral private key ephem SK picc -PACE,**
- **Personalisation Agent Key(s),**
- **Chip Authentication Private Key,**
- **Active Authentication Private Key (AA_SK).**
- **Administrator authentication Key(s)**.

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:

- **Exposure to operating conditions causing a TOE malfunction,**
- **Failure detected by TSF according to FPT_TST.1,**
- **none**.

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 **at the conditions**

- **At reset** 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 **stored TSF executable code**.

9.1.13 Class FTP Trusted Path/Channels

FTP_ITC.1/PACE Inter-TSF trusted channel

FTP_ITC.1.1/PACE 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/PACE The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE [Editorially Refined] The TSF shall **enforce** communication via the trusted channel for **any data exchange between the TOE and the Terminal**.

9.1.14 Additional FTP SFR's Identified

FTP_ITC.1/MP Inter-TSF trusted channel

FTP_ITC.1.1/MP 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/MP The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/MP The TSF shall initiate communication via the trusted channel for **loading sensitive data (Pre-Perso_K, Perso_K, PACE_PWD, CA_SK) shall be encrypted**.

9.1.15 SFRs Origin

SFR	Origin **PP/CC/Added**
FAU_SAS.1	[PP_EACwPACE]
FCS_CKM.1/DH_PACE	[PP_EACwPACE]
FCS_CKM.1/CA	[PP_EACwPACE]
FCS_CKM.4	[PP_EACwPACE]
FCS_COP.1/PACE_ENC	[PP_EACwPACE]
FCS_COP.1/PACE_MAC	[PP_EACwPACE]
FCS_COP.1/CA_ENC	[PP_EACwPACE]
FCS_COP.1/SIG_VER	[PP_EACwPACE]
FCS_COP.1/CA_MAC	[PP_EACwPACE]
FCS_RND.1	[PP_EACwPACE]
FCS_CKM.1/CAM	Add
FCS_CKM.1/CA_DATA_GEN	Add
FCS_CKM.1/GP	Add
FCS_COP.1/CAM	Add
FCS_COP.1/GP_ENC	Add
FCS_COP.1/GP_MAC	Add
FCS_COP.1/GP_AUTH	Add
FCS_COP.1/GP_KEY_DEC	Add
FCS_COP.1/AA	Add

FDP_ACC.1/TRM	PP
FDP_ACF.1/TRM	[PP_EACwPACE]
FDP_RIP.1	[PP_EACwPACE]
FDP_UCT.1/TRM	[PP_EACwPACE]
FDP_UIT.1/TRM	[PP_EACwPACE]
FDP_ACC.1/UPD_FILE	Add
FDP_ACF.1/UPD_FILE	Add
FDP_DAU.1/AA	Add
FDP_ITC.1/AA	Add
FIA_UID.1/PACE	[PP_EACwPACE]
FIA_UAU.1/PACE	[PP_EACwPACE]
FIA_UAU.4/PACE	[PP_EACwPACE]
FIA_UAU.5/PACE	[PP_EACwPACE]
FIA_UAU.6/EAC	[PP_EACwPACE]
FIA_UAU.6/PACE	[PP_EACwPACE]
FIA_AFL.1/PACE	[PP_EACwPACE]
FIA_AFL.1/MP	Add
FIA_API.1/CA	[ADDENDUM]
FIA_UAU.6/MP	Add
FMT_SMF.1	[PP_EACwPACE]
FMT_SMR.1/PACE	[PP_EACwPACE]
FMT_LIM.1	[PP_EACwPACE]
FMT_LIM.2	[PP_EACwPACE]
FMT_MTD.1/INI_ENA	[PP_EACwPACE]
FMT_MTD.1/INI_DIS	[PP_EACwPACE]
FMT_MTD.1/PA	[PP_EACwPACE]
FMT_MTD.1/CVCA_INI	[PP_EACwPACE]
FMT_MTD.1/CVCA_UPD	[PP_EACwPACE]
FMT_MTD.1/DATE	[PP_EACwPACE]
FMT_MTD.1/CAPK	[PP_EACwPACE]
FMT_MTD.1/KEY_READ	[PP_EACwPACE]
FMT_MTD.3	[PP_EACwPACE]
FMT_MTD.1/PACE_PWD	Add
FMT_MTD.1/LCS_PERS	Add

FMT_MTD.1/UPD_FILE	Add
FMT_MTD.1/SM_LVL_DG3_DG4	Add
FMT_MTD.1/SM_LVL	Add
FMT_MTD.1/BAC_EXP	Add
FMT_MTD.1/AA_KEY_READ	Add
FMT_MTD.1/AA_KEY_WRITE	Add
FMT_MTD.1/ADMIN	Add
FMT_MTD.1/Key_Usage_Counter	Add
FMT_MOF.1/GP	Add
FMT_MOF.1/BAC_EXP	Add
FMT_MOF.1/AA	Add
FPT_EMS.1	[PP_EACwPACE]
FPT_FLS.1	[PP_EACwPACE]
FPT_PHP.3	[PP_EACwPACE]
FPT_TST.1	[PP_EACwPACE]
FTP_ITC.1/PACE	[PP_EACwPACE]
FTP_ITC.1/MP	Add
FMT_MTD.1/Initialize_PIN	[ADDENDUM]
FMT_MTD.1/Resume_PIN	[ADDENDUM]
FMT_MTD.1/Change_PIN	[ADDENDUM]
FMT_MTD.1/Unblock_PIN	[ADDENDUM]

9.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL5 augmented with AVA_VAN.5, ALC_FLR.3 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.3 Systematic Flaw Remediation

ALC_FLR.3.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.3.2C 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.3.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.3.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.3.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE

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

Security Objectives from the PP

OT.AC_Pers The security objective OT.AC_Pers "Access Control for Personalisation of logical eDigitalIdentity document" addresses the access control of the writing the logical eDigitalIdentity document. The justification for the SFRs FAU_SAS.1, 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. The write access to the logical eDigitalIdentity document data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalisation Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical eDigitalIdentity document only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SOD and, in generally, personalisation data). The SFR FMT_SMR.1/PACE lists the roles (including Personalisation Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalisation). The SFRs FMT_MTD.1/KEY_READ and FPT_EMS.1 restrict the access to the Personalisation Agent Keys and the Chip Authentication Private Key.

The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. If the Personalisation Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol v1 (after Chip Authentication v1) with the Personalisation Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA (for the derivation of the new session keys after Chip Authentication v1), FCS_CKM.1/CA_DATA_GEN for generation of CA Data in phase 6, and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol v1) and FIA_UAU.6/EAC (for the re-authentication). If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalisation Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The Personalisation Agent can load the PACE password according to FMT_MTD.1/PACE_PWD.

FMT_MTD.1/LCS_PERS ensures only personalisation agent can transfer the TOE from life cycle phase 6 to phase 7.

FIA_UAU.6/MP ensures all commands in personalisation phase are sent via secure messaging. FIA_AFL.1/MP helps block the Authentication in Phase 6 if too many failed authentication attempts occur to prevent attacks.

FDP_ACC.1/UPD_FILE and FDP_ACF.1/UPD_FILE restrict write access to files to personalisation agent.

Additionally to the SFRs from [PACE/EACPP] which cover this objective, the security objective OT.AC_Pers is achieved by terminal identification/authentication using and managing the PIN/PUK as required by the SFRs FIA_AFL.1/PACE. The SFR FMT_SMF.1

support the related functions. The SFR FDP_RIP.1 requires erasing the temporal values PIN and PUK.

OT.Data_Integrity The security objective OT.Data_Integrity "Integrity of personal data" requires the TOE to protect the integrity of the logical eDigitalIdentity document stored on the eDigitalIdentity document's chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Personalisation Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical eDigitalIdentity document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical eDigitalIdentity document (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The Personalisation Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

Unauthorised modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. For PACE secured data exchange, a prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. The trusted channel is established using PACE, Chip Authentication v1, and Terminal Authentication v1. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC).

The TOE supports the inspection system detect any modification of the transmitted logical eDigitalIdentity document data after Chip Authentication v1. The SFR FIA_UAU.6/EAC and FDP_UIT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v1 by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA and FCS_CKM.1/CAM(for the generation of shared secret andfor the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

The SFRs FDP_ACC.1/UPD_FILE and FDP_ACF.1/UPD_FILE ensure that no terminal is allowed to modify the user data.

FIA_UAU.6/MP and FMT_MOF.1/GP makes sure that the data is transmitted via secure messaging to maintain integrity.

Additionally to the SFRs from [PACE/EACPP] which cover these objectives, these security objectives are achieved by establishing a trusted channel via a successful Chip Authentication thanks to the SFRs FIA_API.1/TOE. Since PACE can use the PIN as the shared secret, using and management of PIN, the SFR FIA_AFL.1/PACE, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN also support the achievement of these objectives. The SFR FMT_SMF.1 support the related functions. The SFR FDP_RIP.1 requires erasing the temporal values PIN and PUK.

OT.Sens_Data_Conf The security objective OT.Sense_Data_Conf "Confidentiality of sensitive biometric reference data" is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER. The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v1 by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), FCS_CKM.1/CA_DATA_GEN for generation of Chip Authentication Data in personalisation phase, and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. FIA_UAU.6/MP requires that the sensitive data is sent via Secure Messaging during personalisation phase. To allow a verification of the certificate chain as 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 of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. FMT_MOF.1/GP ensures all data is transmitted and received via secure messaging to ensure confidentiality

OT.Identification The security objective OT.Identification "Identification of the TOE" 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. This will be ensured by TSF according to SFR FAU_SAS.1. 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 roles related.

OT.Chip_Auth_Proof The security objective OT.Chip_Auth_Proof "Proof of eDigitalIdentity document's chip authenticity" is ensured by the Chip Authentication Protocol v1 provided by FIA_API.1/CA proving the identity of the TOE. The Chip Authentication Protocol v1 defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Data is generated by using FCS_CKM.1/CA_DATA_GEN. The Chip Authentication Protocol v1 [TR-03110-1] and [TR-03110-3] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the

ENC_MAC_Mode secure messaging).The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.Prot_Abuse-Func The security objective OT.Prot_Abuse-Func "Protection against Abuse of Functionality" is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

OT.Prot_Inf_Leak The security objective OT.Prot_Inf_Leak "Protection against Information Leakage" requires the TOE to protect confidential TSF data stored and/or processed in the eDigitalIdentity document's chip against disclosure

- 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 which is addressed by the SFR FPT_EMS.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

OT.Prot_Phys-Tamper The security objective OT.Prot_Phys-Tamper "Protection against Physical Tampering" is covered by the SFR FPT_PHP.3.

OT.Prot_Malfunction The security objective OT.Prot_Malfunction "Protection against Malfunctions" is covered by (i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and (ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

OT.Data_Authenticity The security objective OT.Data_Authenticity aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself.This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA or FCS_CKM.1/CAM and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FIA_UAU.6/MP ensures the data that is reaching the TOE is coming from the personalisation agent by maintaining secure messaging for all commands. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_MTD.1/KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy.The SFR FCS_RND.1 represents a general support for cryptographic operations needed.The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

Additionally to the SFRs from [PACE/EACPP] which cover these objectives, these security objectives are achieved by establishing a trusted channel via a successful Chip Authentication thanks to the SFR FIA_API.1/TOE. Since PACE can use the PIN as the shared secret, using and management of PIN, the SFRs FIA_AFL.1/PACE,

FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN support alos the achievement of these objectives. The SFR FMT_SMF.1 support the related functions. The SFR FDP_RIP.1 requires erasing the temporal values PIN and PUK.

OT.Data_Confidentiality The security objective OT.Data_Confidentiality aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged.This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM, FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA or FCS_CKM.1/CAM and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC and FIA_UAU.6/MP for Manufacture and Personalisation Agent authentication. FDP_RIP.1 requires erasing the values of session keys (here: for Kenc). The SFR FMT_MTD.1/KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy. The SFR FCS_RND.1 represents the general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

Additionally to the SFRs from [PACE/EACPP] which cover these objectives, these security objectives are achieved by establishing a trusted channel via a successful Chip Authentication thanks to the SFR FIA_API.1/TOE. Since PACE can use the PIN as the shared secret, using and management of PIN, the SFRs FIA_AFL.1/PACE, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN support alos the achievement of these objectives. The SFR FMT_SMF.1 support the related functions. The SFR FDP_RIP.1 requires erasing the temporal values PIN and PUK.

OT.Tracing The security objective OT.Tracing aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the eDigitalIdentity document remotely through establishing or listening to a communication via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ).This objective is achieved as follows:(i) while establishing PACE communication with PIN, PUK, CAN or MRZ (non-blocking authorisation data) – by FIA_AFL.1/PACE;(ii) for listening to PACE communication (is of importance for the current PP, since SOD is card-individual) – FTP_ITC.1/PACE.

Additional Objectives as per ADDENDUM

OT.Sens_Ident_User_Data_Conf The security objective of OT.Sens_Ident_User_Data_Conf aims to explicitly protect sensitive identification user and TSF-Data during their exchange. It is enforcing by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid

certificate according FCS_COP.1/SIG_VER. A prerequisite for establishing a trusted channel is a successful Chip Authentication thanks to the SFRs FIA_API.1/TOE. Since PACE can use the PIN as the shared secret, the SFRs FIA_AFL.1/PACE, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN support the achievement of this objective. The SFR FMT_SMF.1 support the related functions. The SFR FDP_RIP.1 requires erasing the temporal values PIN and PUK.

Additional Objectives for Active Authentication

OT.AA_Proof The security objective OT.AA_Proof is ensured by the Active Authentication Protocol activated by FMT_MOF.1/AA and provided by FDP_DAU.1/AA, FDP_ITC.1/AA proving the identity and authenticity of the TOE. The Active Authentication relies on FCS_COP.1/AA and FCS_RND.1. It is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AA_KEY_WRITE and FMT_MTD.1/AA_KEY_READ.

OT.Data_Int_AA The security objective OT.AA_Proof is ensured by the Active Authentication Protocol activated by FMT_MOF.1/AA and provided by FDP_DAU.1/AA and FDP_ITC.1/AA proving the identity and authenticity of the TOE.

Additional Security Objectives Identified

OT.Configuration The security objective OT.Configuration "Protection of the TOE preparation" addresses management of the Data Configuration, Pre-personalisation Agent keys, Personalisation Agent keys and the Life Cycle State of the TOE.

The Manufacturer can be authenticated by using the symmetric authentication mechanism (FCS_COP.1/GP_AUTH) with the Pre-personalisation key. FIA_UAU.6/MP describes the re-authentication. In case of failed authentication attempts FIA_AFL.1/MP enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The SFR FTP_ITC.1/MP allows the Manufacturer to communicate with the OS.

Once step 4 is done, the eDigitalIdentity document packaging responsible is allowed to set the Pre-personalisation Agent keys according to the SFR FCS_COP.1/GP_KEY_DEC. The read access to the Pre-personalisation keys is prevented by SFRs FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

The Manufacturer shall be authenticated by using the symmetric authentication mechanism (FCS_COP.1/GP_AUTH).

In case of failed authentication attempts FIA_AFL.1/MP enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack

The SFR FIA_UAU.6/MP describes the re-authentication and FDP_UCT.1/MP the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/GP, FCS_RND.1 (for key generation), and FCS_COP.1/GP_ENC as well as FCS_COP.1/GP_MAC for the ENC_MAC_Mode. The SFR FCS_CKM.4 enforces the destruction of Secure Messaging session keys.

The Manufacturer and the Personalisation Agent can select the protection mode of user data following FMT_MOF.1.1/GP.

The SFR FCS_CKM.4, FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of Personalisation Agent keys.

OT.Update_File The security objective OT.Update_File "Modification of file in Operational Use Phase" addresses the modification of Updatable Data as defined in FDP_ACC.1/UPD_FILE. The SFR FDP_ACF.1/UPD_FILE clarifies what can be done by which subject: after a correct authentication the Personalisation Agent is allowed to write, read and modify these Updatable Data during Pre-Personalisation and Personalisation phases. Any Terminal is not allowed to modify them during Operational phase. Only a successfully authenticated Extended Inspection System is allowed to modify Updatable Data, only if with the name corresponding to the one (or beginning of the one) set following FMT_MTD.1/UPD_FILE by the Personalisation Agent during Pre-Personalisation and Personalisation phases.

OT.AC_SM_Level The security objective OT.AC_SM_Level "Access control to sensitive biometric reference data according to SM level" is covered by FMT_MTD.1/SM_LVL_DG3_DG4 and FMT_MTD.1/SM_LVL.

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. The authentication of the terminal as Administrator is performed by TSF according to FIA_UAU.5/PACE. The Administrator can be authenticated by using the symmetric authentication mechanism (FCS_COP.1/GP_AUTH) with the Administartor key. ADMIN keys are created during pre-personalization. FMT_MTD.1/KEY_READ restricts the ability to read the Administrator Keys to none. The Administartor can select the protection mode of user data following FMT_MOF.1/GP. FPT_EMS.1 protects the confidentially of Administrator Agent keys. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related. The administration TSF data manipulation are supported by FMT_MTD.1/ADMIN. It is now allowed to modify 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. 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.AC_Pers	FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FAU_SAS.1, FIA_UAU.5/PACE, FMT_SMF.1, FMT_SMR.1/PACE, FIA_UAU.6/MP, FIA_AFL.1/MP, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FMT_MTD.1/LCS_PERS, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_ENC,	Section 9.3.1

	FCS_COP.1/SIG_VER, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.6/EAC, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FMT_MTD.1/PACE_PWD, FPT_EMS.1, FCS_CKM.1/CA_DATA_GEN, FCS_COP.1/CA_MAC, FIA_AFL.1/PACE, FDP_RIP.1	
OT.Data_Integrity	FCS_CKM.1/DH_PACE, FCS_COP.1/PACE_MAC, FIA_UAU.1/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FIA_UID.1/PACE, FIA_UAU.4/PACE, FIA_UAU.6/PACE, FDP_ACF.1/TRM, FDP_ACC.1/TRM, FDP_UIT.1/TRM, FTP_ITC.1/PACE, FMT_MTD.1/PA, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FCS_COP.1/CA_MAC, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_ENC, FDP_RIP.1, FMT_SMF.1, FMT_SMR.1/PACE, FPT_PHP.3, FIA_UAU.6/MP, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FCS_RND.1, FMT_MOF.1/GP, FCS_CKM.1/CAM, FIA_AFL.1/PACE, FIA_API.1/TOE, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN	Section 9.3.1
OT.Sens_Data_Conf	FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_ENC, FCS_COP.1/SIG_VER, FCS_COP.1/CA_MAC, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FIA_UAU.6/MP, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_UCT.1/TRM, FMT_MOF.1/GP, 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, FCS_CKM.1/CA_DATA_GEN	Section 9.3.1
OT.Identification	FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FAU_SAS.1, FMT_SMF.1, FMT_SMR.1/PACE	Section 9.3.1
OT.Chip_Auth_Proof	FCS_CKM.1/CA, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FIA_API.1/CA,	Section 9.3.1

	FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK, FCS_CKM.1/CA_DATA_GEN	
OT.Prot_Abuse-Func	FMT_LIM.1, FMT_LIM.2	Section 9.3.1
OT.Prot_Inf_Leak	FPT_FLS.1, FPT_PHP.3, FPT_TST.1, FPT_EMS.1	Section 9.3.1
OT.Prot_Phys-Tamper	FPT_PHP.3	Section 9.3.1
OT.Prot_Malfunction	FPT_FLS.1, FPT_TST.1	Section 9.3.1
OT.Data_Authenticity	FCS_CKM.1/DH_PACE, FCS_COP.1/PACE_MAC, FIA_UAU.1/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FIA_UID.1/PACE, FIA_UAU.4/PACE, FIA_UAU.6/PACE, FTP_ITC.1/PACE, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FCS_CKM.1/CA, FCS_CKM.4, FDP_RIP.1, FMT_SMF.1, FMT_SMR.1/PACE, FIA_UAU.6/MP, FCS_RND.1, FCS_CKM.1/CAM, FIA_AFL.1/PACE, FIA_API.1/TOE, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN	Section 9.3.1
OT.Data_Confidentiality	FCS_CKM.1/DH_PACE, FCS_COP.1/PACE_ENC, FIA_UAU.1/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FIA_UID.1/PACE, FIA_UAU.4/PACE, FIA_UAU.6/PACE, FDP_ACF.1/TRM, FDP_ACC.1/TRM, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FTP_ITC.1/PACE, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_ENC, FDP_RIP.1, FMT_SMF.1, FMT_SMR.1/PACE, FIA_UAU.6/MP, FCS_RND.1, FCS_CKM.1/CAM, FIA_AFL.1/PACE, FIA_API.1/TOE, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN	Section 9.3.1
OT.Tracing	FTP_ITC.1/PACE, FIA_AFL.1/PACE	Section 9.3.1

OT.Sens_Ident_User_Data_Conf	FIA_AFL.1/PACE, FIA_API.1/TOE, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_SMF.1, FDP_RIP.1, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FCS_COP.1/SIG_VER	Section 9.3.1
OT.AA_Proof	FCS_COP.1/AA, FCS_RND.1, FDP_ITC.1/AA, FDP_DAU.1/AA, FMT_MOF.1/AA, FMT_MTD.1/AA_KEY_READ, FMT_MTD.1/AA_KEY_WRITE	Section 9.3.1
OT.Data_Int_AA	FDP_DAU.1/AA, FDP_ITC.1/AA, FMT_MOF.1/AA	Section 9.3.1
OT.Configuration	FCS_CKM.1/GP, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_KEY_DEC, FTP_ITC.1/MP, FIA_AFL.1/MP, FIA_UAU.6/MP, FCS_CKM.4, FCS_RND.1, FPT_EMS.1, FPT_FLS.1, FPT_PHP.3	Section 9.3.1
OT.Update_File	FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FMT_MTD.1/UPD_FILE	Section 9.3.1
OT.AC_SM_Level	FMT_MTD.1/SM_LVL_DG3_DG4, FMT_MTD.1/SM_LVL	Section 9.3.1
OT.ADMIN_Configuration	FIA_UAU.5/PACE, FCS_COP.1/GP_AUTH, FMT_MTD.1/KEY_READ, FMT_MOF.1/GP, FPT_EMS.1, FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/ADMIN	Section 9.3.1
OT.Key_Usage_Counter	FMT_MTD.1/Key_Usage_Counter	Section 9.3.1

Table 21 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FAU_SAS.1	OT.AC_Pers, OT.Identification
FCS_CKM.1/DH_PACE	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality
FCS_CKM.1/CA	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.Data_Authenticity, OT.Data_Confidentiality

FCS_CKM.4	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Configuration
FCS_COP.1/PACE_ENC	OT.Data_Confidentiality
FCS_COP.1/PACE_MAC	OT.Data_Integrity, OT.Data_Authenticity
FCS_COP.1/CA_ENC	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.Data_Confidentiality
FCS_COP.1/SIG_VER	OT.AC_Pers, OT.Sens_Data_Conf, OT.Sens_Ident_User_Data_Conf
FCS_COP.1/CA_MAC	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_RND.1	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Data_Authenticity, OT.Data_Confidentiality, OT.AA_Proof, OT.Configuration
FCS_CKM.1/CAM	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality
FCS_CKM.1/CA_DATA_GEN	OT.AC_Pers, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_CKM.1/GP	OT.Configuration
FCS_COP.1/GP_ENC	OT.Configuration
FCS_COP.1/GP_MAC	OT.Configuration
FCS_COP.1/GP_AUTH	OT.Configuration, OT.ADMIN_Configuration
FCS_COP.1/GP_KEY_DEC	OT.Configuration
FCS_COP.1/AA	OT.AA_Proof
FDP_ACC.1/TRM	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Data_Confidentiality, OT.Sens_Ident_User_Data_Conf
FDP_ACF.1/TRM	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Data_Confidentiality, OT.Sens_Ident_User_Data_Conf
FDP_RIP.1	OT.AC_Pers, OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Sens_Ident_User_Data_Conf
FDP_UCT.1/TRM	OT.Sens_Data_Conf, OT.Data_Confidentiality

FDP_UIT.1/TRM	OT.Data_Integrity, OT.Data_Confidentiality
FDP_ACC.1/UPD_FILE	OT.AC_Pers, OT.Data_Integrity, OT.Update_File
FDP_ACF.1/UPD_FILE	OT.AC_Pers, OT.Data_Integrity, OT.Update_File
FDP_DAU.1/AA	OT.AA_Proof, OT.Data_Int_AA
FDP_ITC.1/AA	OT.AA_Proof, OT.Data_Int_AA
FIA_UID.1/PACE	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Data_Authenticity, OT.Data_Confidentiality
FIA_UAU.1/PACE	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Data_Authenticity, OT.Data_Confidentiality
FIA_UAU.4/PACE	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Data_Authenticity, OT.Data_Confidentiality
FIA_UAU.5/PACE	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Data_Authenticity, OT.Data_Confidentiality, OT.ADMIN_Configuration
FIA_UAU.6/EAC	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Data_Authenticity, OT.Data_Confidentiality
FIA_UAU.6/PACE	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality
FIA_AFL.1/PACE	OT.AC_Pers, OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Tracing, OT.Sens_Ident_User_Data_Conf
FIA_API.1/TOE	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality OT.Sens_Ident_User_Data_Conf
FIA_AFL.1/MP	OT.AC_Pers, OT.Configuration
FIA_API.1/CA	OT.Chip_Auth_Proof
FIA_UAU.6/MP	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Configuration
FMT_SMF.1	OT.AC_Pers, OT.Data_Integrity, OT.Identification, OT.Chip_Auth_Proof, OT.Data_Authenticity, OT.Data_Confidentiality,

	OT.ADMIN_Configuration OT.Sens_Ident_User_Data_Conf
FMT_SMR.1/PACE	OT.AC_Pers, OT.Data_Integrity, OT.Identification, OT.Chip_Auth_Proof, OT.Data_Authenticity, OT.Data_Confidentiality, OT.ADMIN_Configuration
FMT_LIM.1	OT.Prot_Abuse-Func
FMT_LIM.2	OT.Prot_Abuse-Func
FMT_MTD.1/INI_ENA	OT.AC_Pers, OT.Identification
FMT_MTD.1/INI_DIS	OT.AC_Pers, OT.Identification
FMT_MTD.1/PA	OT.AC_Pers, OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality
FMT_MTD.1/CVCA_INI	OT.Sens_Data_Conf
FMT_MTD.1/CVCA_UPD	OT.Sens_Data_Conf
FMT_MTD.1/DATE	OT.Sens_Data_Conf
FMT_MTD.1/CAPK	OT.Data_Integrity, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FMT_MTD.1/KEY_READ	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.Data_Authenticity, OT.Data_Confidentiality, OT.ADMIN_Configuration
FMT_MTD.3	OT.Sens_Data_Conf
FMT_MTD.1/Initialize_PIN	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Sens_Ident_User_Data_Conf
FMT_MTD.1/Resume_PIN	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Sens_Ident_User_Data_Conf
FMT_MTD.1/Change_PIN	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Sens_Ident_User_Data_Conf
FMT_MTD.1/Unblock_PIN	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Sens_Ident_User_Data_Conf
FMT_MTD.1/PACE_PWD	OT.AC_Pers
FMT_MTD.1/LCS_PERS	OT.AC_Pers
FMT_MTD.1/UPD_FILE	OT.Update_File
FMT_MTD.1/SM_LVL_DG3_DG4	OT.AC_SM_Level

FMT_MTD.1/SM_LVL	OT.AC_SM_Level
FMT_MTD.1/AA_KEY_READ	OT.AA_Proof
FMT_MTD.1/AA_KEY_WRITE	OT.AA_Proof
FMT_MTD.1/ADMIN	OT.ADMIN_Configuration
FMT_MTD.1/Key_Usage_Counter	OT.Key_Usage_Counter
FMT_MOF.1/GP	OT.Data_Integrity, OT.Sens_Data_Conf, OT.ADMIN_Configuration
FMT_MOF.1/AA	OT.AA_Proof, OT.Data_Int_AA
FPT_EMS.1	OT.AC_Pers, OT.Prot_Inf_Leak, OT.Configuration, OT.ADMIN_Configuration
FPT_FLS.1	OT.Prot_Inf_Leak, OT.Prot_Malfunction, OT.Configuration
FPT_PHP.3	OT.Data_Integrity, OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper, OT.Configuration
FPT_TST.1	OT.Prot_Inf_Leak, OT.Prot_Malfunction
FTP_ITC.1/PACE	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Tracing
FTP_ITC.1/MP	OT.Configuration

Table 22 SFRs and Security Objectives

9.3.3 Dependencies

9.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FAU_SAS.1	No Dependencies	
FCS_CKM.1/DH_PACE	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC
FCS_CKM.1/CA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.1/CA_DATA_GEN, FCS_CKM.1/GP
FCS_COP.1/PACE_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE, FCS_CKM.4

FCS_COP.1/PACE_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_COP.1/CA_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/SIG_VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/CA_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_RND.1	No Dependencies	
FCS_CKM.1/CAM	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/CAM
FCS_CKM.1/CA_DATA_GEN	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/SIG_VER
FCS_CKM.1/GP	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC
FCS_COP.1/CAM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/CAM
FCS_COP.1/GP_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/GP
FCS_COP.1/GP_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/GP
FCS_COP.1/GP_AUTH	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/GP
FCS_COP.1/GP_KEY_DEC	(FCS_CKM.1 or FDP_ITC.1 or	FCS_CKM.4, FCS_CKM.1/GP

	FDP_ITC.2) and (FCS_CKM.4)	
FCS_COP.1/AA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FDP_ITC.1/AA
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
FDP_RIP.1	No Dependencies	
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 (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/TRM, FTP_ITC.1/PACE
FDP_ACC.1/UPD_FILE	(FDP_ACF.1)	FDP_ACF.1/UPD_FILE
FDP_ACF.1/UPD_FILE	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/UPD_FILE
FDP_DAU.1/AA	No Dependencies	
FDP_ITC.1/AA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1/TRM
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/EAC	No Dependencies	
FIA_UAU.6/PACE	No Dependencies	
FIA_AFL.1/PACE	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_AFL.1/MP	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_API.1/CA	No Dependencies	
FIA_UAU.6/MP	No Dependencies	
FMT_SMF.1	No Dependencies	
FMT_SMR.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FMT_LIM.1	No Dependencies	
FMT_LIM.2	No Dependencies	

FMT_MTD.1/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/PA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CVCA_INI	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/DATE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CAPK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.3	(FMT_MTD.1)	FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD
FMT_MTD.1/PACE_PWD	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/LCS_PERS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/UPD_FILE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/SM_LVL_DG3_DG4	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/SM_LVL	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/AA_KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/AA_KEY_WRITE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/ADMIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/Key_Usage_Counter	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MOF.1/GP	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MOF.1/AA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE

FPT_EMS.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_PHP.3	No Dependencies	
FPT_TST.1	No Dependencies	
FTP_ITC.1/PACE	No Dependencies	
FTP_ITC.1/MP	No Dependencies	
FIA_API.1/TOE	No Dependencies	
FIA_API.1/CA	No Dependencies	
FMT_MTD.1/Initialize_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/Resume_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/Change_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/Unblock_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE

Table 23 SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FMT_MSA.3 of FDP_ACF.1/TRM is discarded. The access control TSF according to FDP_ACF.1/TRM uses security attributes that have been defined during personalisation, and that are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary.

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

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

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.3	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 24 SARs Dependencies

9.3.4 Rationale for the Security Assurance Requirements

The EAL5 was chosen to permit a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

9.3.5 AVA_VAN.5 Advanced methodical vulnerability analysis

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfill the security objectives OT.Chip_Auth_Proof.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 "Security architecture description"
- ADV_FSP.4 "Security-enforcing functional specification"
- ADV_TDS.3 "Basic modular design"
- ADV_IMP.1 "Implementation representation of the TSF"
- AGD_OPE.1 "Operational user guidance"
- AGD_PRE.1 "Preparative procedures"
- ATE_DPT.1 "Testing: basic design"

All of these are met or exceeded in the EAL5 assurance package

9.3.6 ALC_DVS.2 Sufficiency of security measures

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing especially for the secure handling of the MRTD's material.

The component ALC_DVS.2 augmented to EAL5 has no dependencies to other security requirements.

9.3.7 ALC_FLR.3 Systematic flaw remediation

The flaw remediation assurance improves a rigourous management for updating the TOE in the context of sensible market.

This assurance component has no dependencies.

10 TOE Summary Specification

10.1 TOE Summary Specification

The TOE provides the following Security Functions (TSF):

F.ACR - Access Control in Reading

This function controls access to read functions and enforces the security policy for data retrieval. Prior to any data retrieval, it authenticates the actor trying to access the data, and checks the access conditions are fulfilled as well as the life cycle state. It ensures that at any time, the following keys are never readable:

- Manufacturer Keys,
- Pre-personalisation Agent keys,
- Personalisation Agent keys,
- CA private key,
- PACE passwords,
- Active Authentication Keys.

It controls access to the Initialization and Pre-Personalisation data by allowing read access without authentication prior to delivery. After delivery, only the personalisation agent after authentication has read access to it.

Regarding the file structure:

In the Operational Use phase:

- The terminal can read user data, the Document Security Object, (EF.COM, EF.SOD, EF.DG1 to EF.DG16) only after PACE or EAC authentication and through a valid secure channel.

In the Production and preparation stage:

The Manufacturer can read the Initialization Data in Stage 2 "Production". The pre-personalisation agent and the Personalisation Agent can read only the random identifier in Stage 3 "Preparation" stored in the TOE. Other data-elements can only be read after they are authenticated by the TOE (using their authentication keys).

It ensures as well that no other part of the memory can be accessed at anytime.

F.ACW - Access Control in Writing

This function controls access to write functions (in NVM) and enforces the security policy for data writing. Prior to any data update, it authenticates the actor, and checks the access conditions are fulfilled as well as the life cycle state.

Regarding the file structure:

In the Operational Use phase:

It is not possible to create any files (system or data files). Furthermore, it is not possible to update any files (system or data files), except for the current date, the CVCA public key and the CVCA certificate which can be updated if the access conditions is verified by the subjects defined in FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

In the Production and preparation stage:

The Manufacturer can write all the Initialization and data for the Pre-personalisation. The Personalisation Agent can write through a valid secure channel all the data, PACE passwords, Chip Authentication Private Key, Active Authentication Keys and Country Verifying Certification Authority Public Key after it is authenticated by the TOE (using its authentication keys).

The Pre-Personalisation Agent can write through a valid secure channel data to be used by the personalisation agent (after it is authenticated by the TOE using its authentication keys). The Pre-personalisation agent is only active after delivery. The key that is written in the TOE for authentication purposes during manufacturing in meant for the pre-personalisation agent. the Pre-personalisation agent (which is seen as a sub-role of thep Personalisation agent) will refresh this key.

F.CLR_INFO - Clear Residual Information

This security function ensures clearing of sensitive information

- Authentication state is securely cleared in case an error is detected or a new authentication is attempted
- Authentication data related to GP authentication, PACE authentication and EAC is securely cleared to prevent reuse
- Session keys is securely erased in case an error is detected or the secure communication session is closed
- ephem-SK picc -PACE is securely erased
- PIN and PUK

F.CRYPTO - Cryptographic Support

This Security Function provides the following cryptographic features:

- Key Generation based on ECDH with key sizes 192 to 521 bits.
- Key generation based on DH with key sizes 1024, 1536 and 2048.
- Key generation for Triple-DES in CBC mode for 112 bits.
- Key generation for AES in CBC mode with key sizes 128, 192 and 256 bits.
- Secure messaging (encryption and decryption) using:
  - Triple DES in CBC mode (key size 112 bits).
  - AES in CBC mode (key sizes 128,192,256 bits).
- Secure messaging (message authentication code) using:
  - Retail MAC with key size 112 bits.
  - AES CMAC with key sizes 128,192 and 256 bits.
- GP Secure Messaging (encryption and decryption) using:
  - Triple-DES in CBC mode with key size 112 bits as defined in [FIPS_46_3].
  - AES with key sizes 128, 192 and 256 bits as defined in [NIST_800_38A].
- Digital signature creation using:
  - ECDSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 with key sizes 192 to 512 bits over prime field curves
  - RSA signature (CRT) with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 with key sizes 1024, 1536 and 2048.
- Digital signature verification using:

- ECDSA with SHA-1, SHA-224 and SHA-256 with key sizes 192 to 512 bits.
- RSA PKCS#1v1.5 with SHA-1, SHA-256 and SHA-512 with key sizes 1024, 1536 and 2048.
- RSA PKCS#1-PSS with SHA-1, SHA-256 and SHA-512 with key sizes 1024, 1536 and 2048.

o GP Secure Messaging (message authentication code) using:
- Retail MAC with key size 112 bits as defined in [ISO_9797_1].
- AES CMAC with key sizes 128, 192 and 256 bits as defined in [NIST_800_38B].

o Random number generation that meets the requirement the average Shannon entropy per internal random bit exceeds 0.994.

o Symmetric Authentication - encryption and decryption using:
- Full 3DES MAC with key size 112 bits as defined in [ISO_9797_1].
- AES CMAC with key sizes 128, 192 and 256 bits as defined in [NIST_800_38B].

o Key decryption using:
- Triple-DES in ECB mode with key size 112 bits as defined in [FIPS_46_3].
- AES in CBC mode with key sizes 128, 192 and 256 bits as defined in [FIPS_197].

o Chip Authentication Data Generation using DH, with key sizes 1024 to 2048 bits in steps of 512 bits.

o Chip Authentication Data Generation using ECDH, with key sizes 192 to 521 bits.

F.EAC - Extended Access Control

This TSF provides the Extended Access Control, authentication and session keys generation to be used by F.SM, as described in [TR-03110-3]. It also provides the following management functions:

o Maintain the roles: Document Verifier, CVCA, Domestic EIS, Foreign EIS

o Limit the ability to update the CVCA Public key and CVCA Certificate to the Country Verifying Certification Authority

o Limit the ability to update the date to CVCA, Document Verifier and Domestic Extended Inspection System.

F.PACE - Authentication using PACE

This TSF provides the Password Authenticated Connection Establishment Authentication (all mappings) and session keys generation to be used by F.SM, as described in [ICAO_9303].

In case the number of consecutive failed authentication attempts crosses the administrator defined number defined in FIA_AFL.1/PACE the TSF will slow down further authentication attempts.

Only the eDigitalIdentity document holder after successful authentication can

o resume the suspended PIN or PUK,

o change the PIN,

o unblock the blocked PIN using the PUK.

F.PERS - MRTD Personalisation

This security functionality ensures that the TOE, when delivered to the Personalisation Agent, provides and requires authentication for data exchange. This authentication is based

on a Triple DES and AES authentication mechanism. This security function is also responsible for management operations during personalisation phase. This function allows to:

- Manage symmetric authentication using Personalisation Agent keys,
- Configuration of the TOE
- Compute session keys to be used by F.SM,
- Load user data,
- Configure SM level for biometrical data access,
- Load Chip Authentication keys in encrypted form,
- Chip Authnetication Key Generation,
- Write Active Authentication Keys,
- Enable and disable TSF Active Authentication,
- Load of key data PACE in encrypted form,
- Configure BAC deactivation mechanism,
- Set TOE life cycle to Operational Use phase,
- Write the PIN and PUK,
- set the files that are allowed to be modified in phase 7,
- Write the Document Security Object (SO d),
- Write the initial CVCA Public Key, CVCA Certificate and Current Date.
- Configure the Key Usage Counter (optional),
- Configure the minimum key size for CA Key Renewal (optional).

In case the number of consecutive failed authentication attempts crosses 1 the TSF will slow down further authentication attempts.

F.PHY - Physical Protection

This Security Function protects the TOE against physical attacks, so that the integrity and confidentiality of the TOE is ensured, including keys, user data, configuration data and TOE life cycle. It detects physical tampering, responds automatically, and also controls the emanations sent out by the TOE.

This Security Function also limits any physical emanations from the TOE so as to prevent any information leakge via these emanations that might reveal or provide access to sensitive data.

Furthermore, it prevents deploying test features after TOE delivery.

F.PREP - MRTD Pre-personalisation

This security functionality ensures that the TOE, when delivered to the Manufacturer, provides and requires an authentication mechanism for data exchange. This authentication is based on Triple DES and AES symmetric authentication mechanism. This function allows to:

- Manage symmetric authentication using Pre-personalisation Agent keys,
- Compute session keys to be used by F.SM,
- Initialization of the TOE,
- Load Personalisation Agent keys in encrypted form,
- Store the Initialization and Pre-Personalisation data in audit records.

In case the number of consecutive failed authentication attempts crosses 1 the TSF will slow down further authentication attempts.

F.SM - Secure Messaging

This security functionality ensures the confidentiality, authenticity and integrity of the communication between the TOE and the interface device. In the operational phase, after a successful Authentication Procedure (i.e. PACE or CA), a secure channel is established. This security functionality also provides a Secure Messaging (SCP02 and SCP03) for the transmission of user data in Pre-personalisation and Personalisation phases. The protocols can be configured to protect the exchanges integrity and/or confidentiality. If an error occurs in the secure messaging layer or if the session is closed, the session keys are destroyed. This ensures protection against replay attacks as session keys are never reused. The level of security of the allowed secure messaging can now be restricted during perso for the USE phase according to the following increasing level:

- 3DES Secure messaging and above accepted
- AES 128 Secure messaging and above accepted
- AES 192 Secure messaging and above accepted
- AES 256 Secure messaging and above accepted

F.SS - Safe State Management

This security functionality ensures that the TOE gets back to a secure state when:

- a tearing occurs (during a copy of data in NVM).
- an error due to self test as defined in FPT_TST.1.
- any physical tampering is detected.

This security functionality ensures that if such a case occurs, the TOE either is switched in the state "kill card" or becomes mute.

F.STST - Self Test

This security function implements self test features through platform functionalities at reset as defined in FPT_TST.1 to ensure the integrity of the TSF and TSF data.

F.AA - Active Authentication

This security functionality ensures the Active Authentication is performed as described in [ICAO_9303] (if it is activated by the personaliser).

F.ADMIN - MRTD Administration

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 of the Chip Authentication key to be modified in USE phase,
- Change the CA key domain parameters used for the CA key generation process in user phase,
- Invalidate the primary 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

Class FAU Security Audit

FAU_SAS.1 is met by F.PREP - MRTD Pre-personalisation.

Class FCS Cryptographic Support

FCS_CKM.1/DH_PACE is met by F.PACE - Authentication using PACE that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support.

FCS_CKM.1/CA is met by F.EAC - Extended Access Control and F.PACE - Authentication using PACE that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support.

FCS_CKM.4 is met by F.CLR_INFO - Clear Residual Information and F.SM - Secure Messaging that destroys the session keys upon closure of a secure messaging session.

FCS_COP.1/PACE_ENC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support to maintain a secure messaging session as defined in the requirement.

FCS_COP.1/PACE_MAC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support to maintain a secure messaging session as defined in the requirement.

FCS_COP.1/CA_ENC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support to maintain a secure messaging session as defined in the requirement.

FCS_COP.1/SIG_VER is met by F.EAC - Extended Access Control that uses F.CRYPTO - Cryptographic Support to provide digital signature verification.

FCS_COP.1/CA_MAC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support to maintain a secure messaging session as defined in the requirement.

FCS_RND.1 is met by F.CRYPTO - Cryptographic Support.

Additional FCS SFR's Identified

FCS_CKM.1/CAM is met by F.PACE - Authentication using PACE that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support.

FCS_CKM.1/CA_DATA_GEN is met by F.PERS - MRTD Personalisation that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support.

FCS_CKM.1/GP is met by F.PERS - MRTD Personalisation and F.PREP - MRTD Pre-personalisation that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support.

FCS_COP.1/GP_ENC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support maintain a secure messaging session as defined in the requirement.

FCS_COP.1/GP_MAC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support maintain a secure messaging session as defined in the requirement.

FCS_COP.1/GP_AUTH is met by F.PREP - MRTD Pre-personalisation and F.PERS - MRTD Personalisation that use F.CRYPTO - Cryptographic Supportto perform Symmetric Authentication.

FCS_COP.1/GP_KEY_DEC is met by F.PREP - MRTD Pre-personalisation and F.PERS - MRTD Personalisation that use F.CRYPTO - Cryptographic Support to perform key decryption.

FCS_COP.1/AA is covered by F.AA - Active Authentication in association with F.CRYPTO - Cryptographic Support.

Class FDP User Data Protection

FDP_ACC.1/TRM is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanism provided by F.PACE - Authentication using PACE.

FDP_ACF.1/TRM is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanism provided by F.PACE - Authentication using PACE.

FDP_RIP.1 is met by F.CLR_INFO - Clear Residual Information that ensures keys are erased securely.

FDP_UCT.1/TRM is met by F.SM - Secure Messaging that ensures all user data is transmitted and received via a secure communication channel.

FDP_UIT.1/TRM is met by F.SM - Secure Messaging that ensures all user data is transmitted and received via a secure communication channel.

Additional FDP SFR's Identified

FDP_ACC.1/UPD_FILE is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current

authentication state using authentication mechanisms provided by F.EAC - Extended Access Control and F.PACE - Authentication using PACE using PACE and F.PERS - MRTD Personalisation.

FDP_ACF.1/UPD_FILE is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanisms provided by F.PACE - Authentication and F.EAC - Extended Access Control using PACE and F.PERS - MRTD Personalisation.

FDP_DAU.1/AA is met by F.AA - Active Authentication.

FDP_ITC.1/AA is met by F.ACW - Access Control in Writing that verifies the write access based on authentication provided by F.AA - Active Authentication.

Class FIA Identification and Authentication

FIA_UID.1/PACE is met by F.ACR - Access Control in Reading that manages access to data based on the current authentication state. It is also met by F.PACE - Authentication using PACE and F.EAC - Extended Access Control that provide PACE and Chip Authentication. It is met by F.PERS - MRTD Personalisation and F.PREP - MRTD Pre-personalisation for manufacturer and peronalization agent authentication. It is also met by F.SM - Secure Messaging that provides a secure messaging channel.

FIA_UAU.1/PACE is met by F.ACR - Access Control in Reading that manages access to data based on the current authentication state. It is also met by F.PACE - Authentication using PACE and F.EAC - Extended Access Control that provide PACE and Extended Access Control. It is met by F.PERS - MRTD Personalisation and F.PREP - MRTD Pre-personalisation for manufacturer and peronalization agent authentication. It is also met by F.SM - Secure Messaging that provides a secure messaging channel.

FIA_UAU.4/PACE is met by F.CLR_INFO - Clear Residual Information that ensures all authentication data is securely erased to prevent reuse.

FIA_UAU.5/PACE is met by F.PACE - Authentication using PACE that provides PACE Authentication. It is also met by F.EAC - Extended Access Control that provides Chip Authentication and Terminal Authentication as part of Extended Access Control. It is also

met by F.PERS - MRTD Personalisation and F.PREP - MRTD Pre-personalisation that provides symmetric authentication.

FIA_UAU.6/EAC is met by F.SM - Secure Messaging that ensures all messages are sent through secure messaging after chip and terminal authentication.

FIA_UAU.6/PACE is met by F.SM - Secure Messaging that ensures all messages are sent through secure messaging after PACE authentication.

FIA_AFL.1/PACE is met by F.PACE - Authentication using PACEthat handles the consecutive failed authentication attempts related to PACE.

Additional FIA SFRs identified as per ADDENDUM

FIA_API.1/TOE is met by F.PACE - Authentication using PACE that provides a means to identify the document holder via PACE Authentication.

Additional FIA SFR's Identified

FIA_AFL.1/MP is met by F.PERS - MRTD Personalisation and F.PREP - MRTD Pre-personalisation that ensures that after 3 unsuccessful symmetric authentication attempts the TOE increases the time taken to respond to a terminal challenge.

FIA_API.1/CA is met by F.EAC - Extended Access Control that provides Chip Authentication.

FIA_UAU.6/MP is met by F.SM - Secure Messaging that ensures all messages are sent through secure messaging after symmetric authentication.

Class FMT Security Management

FMT_SMF.1 is met by F.EAC - Extended Access Control and F.PACE - Authentication using PACE, F.PERS - MRTD Personalisation and F.PREP - MRTD Pre-personalisation that provide the required management functions and F.SM - Secure Messaging that ensures protection of incoming and outgoing user data via secure communication.

FMT_SMR.1/PACE is met by F.PACE - Authentication using PACE, F.EAC - Extended Access Control, F.PERS - MRTD Personalisation and F.PREP - MRTD Pre-personalisation. These

roles are maintained by means of the authentication states during the authentication mechanisms provided by the 3 security functions.

FMT_LIM.1 is met by F.PHY - Physical Protection and F.SS - Safe State Management that ensure that no data can be manipulated or revealed and the TSF assumes a safe state in case any illegal attempts to do so are detected.

FMT_LIM.2 is met by F.PHY - Physical Protection and F.SS - Safe State Management that ensure that no data can be manipulated or revealed and the TSF assumes a safe state in case any illegal attempts to do so are detected.

FMT_MTD.1/INI_ENA is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PREP - MRTD Pre-personalisation.

FMT_MTD.1/INI_DIS is met by F.ACR - Access Control in Reading that ensures access conditions are met by way of authentication through F.PREP - MRTD Pre-personalisation.

FMT_MTD.1/PA is met by F.PERS - MRTD Personalisation.

FMT_MTD.1/CVCA_INI is met by F.ACW - Access Control in Writing that controls write access based on authentication provided by F.PERS - MRTD Personalisation.

FMT_MTD.1/CVCA_UPD is met by F.ACW - Access Control in Writing that controls write access based on authentication provided by F.EAC - Extended Access Control.

FMT_MTD.1/DATE is met by F.ACW - Access Control in Writing that controls write access based on authentication provided by F.EAC - Extended Access Control.

FMT_MTD.1/CAPK is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PERS - MRTD Personalisation.

FMT_MTD.1/KEY_READ is met by F.ACR - Access Control in Reading that ensures the secret keys are never readable.

FMT_MTD.3 is met by F.EAC - Extended Access Control that implements terminal authentication.

Additional FMT SFR's Identified

FMT_MTD.1/PACE_PWD is met by F.PERS - MRTD Personalisation.

FMT_MTD.1/LCS_PERS is met by F.PERS - MRTD Personalisation that allows the personalisation agent after successful authentication to switch the lifecycle state from phase 6 to phase 7.

FMT_MTD.1/UPD_FILE is met by F.PERS - MRTD Personalisation that controls access conditions in F.ACW - Access Control in Writing to allow only the name set by the personalisation agent to be able to edit files in operational phase.

FMT_MTD.1/SM_LVL_DG3_DG4 is met by F.PERS - MRTD Personalisation that allows the personalisation agent to provide configure the secure messaging level required to access DG.3 and DG.4

FMT_MTD.1/SM_LVL is met by F.PERS - MRTD Personalisation in which the level of security of the allowed secure messaging can now be restricted during perso for the USE phase.

FMT_MTD.1/AA_KEY_READ is met by F.ACR - Access Control in Reading that ensures the secret keys are never readable

FMT_MTD.1/AA_KEY_WRITE is met by F.ACW - Access Control in Writing that controls write access for Active Authentication based on authentication provided by F.PERS - MRTD Personalisation.

FMT_MTD.1/ADMIN is met by F.ADMIN - MRTD Administration, that 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,
- Modify the Chip Authentication key parameters to be used during key generation in USE phase,
- Change the key parameters during the key generation process,
- Invalidate one of the Chip Authentication key in USE phase and to set the secondary key as being the primary key.

FMT_MTD.1/Key_Usage_Counter is met by F.PERS - MRTD Personalisation that allows the personalisation agent to configure 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. This Key Usage Counter is an optional parameter during the

creation of the key in PERSO phase and if not configured, the usage of the key will be unlimited.

FMT_MOF.1/GP is met by F.SM - Secure Messaging that provides secure messaging after authentication through F.PERS - MRTD Personalisation and F.PREP - MRTD Pre-personalisation.

FMT_MOF.1/AA is met by F.PERS - MRTD Personalisation.

Class FPT Protection of the Security Functions

FPT_EMS.1 is met by F.PHY - Physical Protection that prevents emanations beyond permissible limits to prevent any accidental revelation of data.

FPT_FLS.1 is met by F.SS - Safe State Management that ensures a safe state is maintained.

FPT_PHP.3 is met by F.PHY - Physical Protection that protects the TOE against any phycial probing or tampering by using F.SS - Safe State Management in case any physical manipulation is detected.

FPT_TST.1 is met by F.STST - Self Test that performs self tests to ensure integrity of the TSF

Class FTP Trusted Path/Channels

FTP_ITC.1/PACE is met by F.SM - Secure Messaging that establishes a secure channel for communication as defined in F.EAC - Extended Access Control and F.PACE - Authentication using PACE.

Additional FTP SFR's Identified

FTP_ITC.1/MP is met by F.SM - Secure Messaging that establishes a secure channel for communication for loading of keys as defined in F.PERS - MRTD Personalisation and F.PREP - MRTD Pre-personalisation.

Additional SFRs as per Addendum

FIA_API.1/TOE is met by F.PACE - Authentication using PACE that provides a means to identify the document holder via PACE Authentication

FMT_MTD.1/Initialize_PIN is met by F.PERS - MRTD Personalization.

FMT_MTD.1/Resume_PIN is met by F.PACE - Authentication using PACE.

FMT_MTD.1/Change_PIN is met by F.PACE - Authentication using PACE.

FMT_MTD.1/Unblock_PIN is met by F.PACE - Authentication using PACE.

10.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FAU_SAS.1	F.PREP - MRTD Pre-personalisation
FCS_CKM.1/DH_PACE	F.PACE - Authentication using PACE, F.CRYPTO - Cryptographic Support
FCS_CKM.1/CA	F.EAC - Extended Access Control, F.CRYPTO - Cryptographic Support, F.PACE - Authentication using PACE
FCS_CKM.4	F.SM - Secure Messaging, F.CLR_INFO - Clear Residual Information
FCS_COP.1/PACE_ENC	F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support
FCS_COP.1/PACE_MAC	F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support
FCS_COP.1/CA_ENC	F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support
FCS_COP.1/SIG_VER	F.EAC - Extended Access Control, F.CRYPTO - Cryptographic Support
FCS_COP.1/CA_MAC	F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support
FCS_RND.1	F.CRYPTO - Cryptographic Support
FCS_CKM.1/CAM	F.CRYPTO - Cryptographic Support, F.PACE - Authentication using PACE
FCS_CKM.1/CA_DATA_GEN	F.PERS - MRTD Personalisation, F.CRYPTO - Cryptographic Support
FCS_CKM.1/GP	F.PERS - MRTD Personalisation, F.PREP - MRTD Pre-personalisation, F.CRYPTO - Cryptographic Support
FCS_COP.1/CAM	F.CRYPTO - Cryptographic Support, F.PACE - Authentication using PACE
FCS_COP.1/GP_ENC	F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support
FCS_COP.1/GP_MAC	F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support
FCS_COP.1/GP_AUTH	F.PERS - MRTD Personalisation, F.PREP - MRTD Pre-personalisation, F.CRYPTO - Cryptographic Support

Security Functional Requirements	TOE Summary Specification
FCS_COP.1/GP_KEY_DEC	F.PERS - MRTD Personalisation, F.CRYPTO - Cryptographic Support, F.PREP - MRTD Pre-personalisation
FCS_COP.1/AA	F.CRYPTO - Cryptographic Support, F.AA - Active Authentication
FDP_ACC.1/TRM	F.ACR - Access Control in Reading, F.ACW - Access Control in Writing, F.PACE - Authentication using PACE
FDP_ACF.1/TRM	F.ACR - Access Control in Reading, F.ACW - Access Control in Writing, F.PACE - Authentication using PACE
FDP_RIP.1	F.CLR_INFO - Clear Residual Information
FDP_UCT.1/TRM	F.SM - Secure Messaging
FDP_UIT.1/TRM	F.SM - Secure Messaging
FDP_ACC.1/UPD_FILE	F.ACR - Access Control in Reading, F.ACW - Access Control in Writing, F.PERS - MRTD Personalisation, F.EAC - Extended Access Control, F.PACE - Authentication using PACE
FDP_ACF.1/UPD_FILE	F.ACR - Access Control in Reading, F.ACW - Access Control in Writing, F.PERS - MRTD Personalisation, F.EAC - Extended Access Control, F.PACE - Authentication using PACE
FDP_DAU.1/AA	F.AA - Active Authentication
FDP_ITC.1/AA	F.ACW - Access Control in Writing, F.AA - Active Authentication
FIA_UID.1/PACE	F.EAC - Extended Access Control, F.PACE - Authentication using PACE, F.SM - Secure Messaging, F.PERS - MRTD Personalisation, F.PREP - MRTD Pre-personalisation, F.ACR - Access Control in Reading
FIA_UAU.1/PACE	F.ACR - Access Control in Reading, F.SM - Secure Messaging, F.EAC - Extended Access Control, F.PACE - Authentication using PACE, F.PERS - MRTD Personalisation, F.PREP - MRTD Pre-personalisation
FIA_UAU.4/PACE	F.CLR_INFO - Clear Residual Information
FIA_UAU.5/PACE	F.EAC - Extended Access Control, F.PACE - Authentication using PACE, F.PERS - MRTD Personalisation, F.PREP - MRTD Pre-personalisation
FIA_UAU.6/EAC	F.SM - Secure Messaging
FIA_UAU.6/PACE	F.SM - Secure Messaging

Security Functional Requirements	TOE Summary Specification
FIA_AFL.1/PACE	F.PACE - Authentication using PACE
FIA_AFL.1/MP	F.PERS - MRTD Personalisation, F.PREP - MRTD Pre-personalisation
FIA_API.1/CA	F.EAC - Extended Access Control
FIA_API.1/TOE	F.PACE - Authentication using PACE
FIA_UAU.6/MP	F.SM - Secure Messaging
FMT_SMF.1	F.PERS - MRTD Personalisation, F.PREP - MRTD Pre-personalisation, F.EAC - Extended Access Control, F.SM - Secure Messaging, F.PACE - Authentication using PACE
FMT_SMR.1/PACE	F.PACE - Authentication using PACE, F.PERS - MRTD Personalisation, F.PREP - MRTD Pre-personalisation, F.EAC - Extended Access Control
FMT_LIM.1	F.PHY - Physical Protection, F.SS - Safe State Management
FMT_LIM.2	F.PHY - Physical Protection, F.SS - Safe State Management
FMT_MTD.1/INI_ENA	F.ACW - Access Control in Writing, F.PREP - MRTD Pre-personalisation
FMT_MTD.1/INI_DIS	F.ACR - Access Control in Reading, F.PREP - MRTD Pre-personalisation
FMT_MTD.1/PA	F.PERS - MRTD Personalisation
FMT_MTD.1/CVCA_INI	F.ACW - Access Control in Writing, F.PERS - MRTD Personalisation
FMT_MTD.1/CVCA_UPD	F.EAC - Extended Access Control, F.ACW - Access Control in Writing
FMT_MTD.1/DATE	F.EAC - Extended Access Control, F.ACW - Access Control in Writing
FMT_MTD.1/CAPK	F.PERS - MRTD Personalisation, F.ACW - Access Control in Writing
FMT_MTD.1/KEY_READ	F.ACR - Access Control in Reading
FMT_MTD.3	F.EAC - Extended Access Control
FMT_MTD.1/PACE_PWD	F.PERS - MRTD Personalisation
FMT_MTD.1/LCS_PERS	F.PERS - MRTD Personalisation
FMT_MTD.1/UPD_FILE	F.ACW - Access Control in Writing, F.PERS - MRTD Personalisation
FMT_MTD.1/SM_LVL_DG3_DG4	F.PERS - MRTD Personalisation
FMT_MTD.1/SM_LVL	F.PERS - MRTD Personalisation

Security Functional Requirements	TOE Summary Specification
FMT_MTD.1/AA_KEY_READ	F.ACR - Access Control in Reading
FMT_MTD.1/AA_KEY_WRITE	F.ACW - Access Control in Writing, F.PERS - MRTD Personalisation
FMT_MTD.1/ADMIN	F.ADMIN - MRTD Administration
FMT_MTD.1/Key_Usage_Counter	F.PERS - MRTD Personalisation
FMT_MOF.1/GP	F.SM - Secure Messaging, F.PERS - MRTD Personalisation, F.PREP - MRTD Pre-personalisation
FMT_MOF.1/AA	F.PERS - MRTD Personalisation
FPT_EMS.1	F.PHY - Physical Protection
FPT_FLS.1	F.SS - Safe State Management
FPT_PHP.3	F.PHY - Physical Protection, F.SS - Safe State Management
FPT_TST.1	F.STST - Self Test
FTP_ITC.1/PACE	F.SM - Secure Messaging, F.PACE - Authentication using PACE, F.EAC - Extended Access Control
FTP_ITC.1/MP	F.PERS - MRTD Personalisation, F.PREP - MRTD Pre-personalisation, F.SM - Secure Messaging
FMT_MTD.1/Initialize_PIN	F.PERS - MRTD Personalization
FMT_MTD.1/Resume_PIN	F.PACE - Authentication using PACE
FMT_MTD.1/Change_PIN	F.PACE - Authentication using PACE
FMT_MTD.1/Unblock_PIN	F.PACE - Authentication using PACE

Table 25 SFRs and TSS - Coverage