IDEMIA

TnD v5.1 on ID-One Cosmo X (PACE/EAC1/Polymorphic eMRTD/LDS2 configuration)

Public Security Target

About IDEMIA

IDEMIA, the global leader in trusted identities for an increasingly digital world, with the ambition to empower citizens and consumers alike to interact, pay, connect, travel and vote in ways that are now possible in a connected environment.

Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, we reinvent the way we think, produce, use and protect this asset, whether for individuals or for objects. We ensure privacy and trust as well as guarantee secure, authenticated and verifiable transactions for international clients from Financial, Telecom, Identity, Security and IoT sectors.

With close to €3bn in revenues, IDEMIA is the result of the merger between OT (Oberthur Technologies) and Safran Identity & Security (Morpho). IDEMIA counts 14,000 employees of more than 80 nationalities and serves clients in 180 countries.

For more information, visit www.idemia.com / Follow @IdemiaGroup on Twitter

APPROVAL

	COMPANY	NAME	FUNCTION
Established by:	IDEMIA	Nicolas LOKIEC	CERTIFICATION Project Manager
Authorized by:	IDEMIA	Sarra MESTIRI	IDEMIA CERTIFICATION Manager

DOCUMENT EVOLUTION

Date	Version	Author	Revision
15/07/2021	Ed 1	Prem KUMAR	Sanitized version created for Public Issue.
29/07/2021	Ed 2	Prem KUMAR	Sanitized version created for public issue after incorporating Certifier feedback.
11/08/2021	Ed 3	Prem KUMAR	Sanitized version created for public issue after removing [ST-IC] from References section (2.3) of this Public ST as [PTF-ST] already refers to it.
23/03/2023	Ed 4	Nicolas LOKIEC	Update for new references: [AGD_OPE], [AGD_PRE], [PTF-ST] and [PTF-CERT].

Table of contents

Table of figures

Table of tables

1 Security Target Introduction

1.1 ST Identification

Title	TnD v5.1 on ID-One Cosmo X (PACE/EAC1/Polymorphic eMRTD/LDS2 configuration) Public Security Target
ST Identification	FQR 550 0247 Ed 4
CC Version	3.1 Revision 5
Assurance Level	EAL5 augmented with ALC_DVS.2 and AVA_VAN.5
ITSEF	Brightsight
Certification Body	NSCIB
Compliant to Protection Profiles	Protection Profile Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP) BSI-CC-PP-0056-V2-2012, Version 1.3.2, 5th December 2012 [EAC-PP-V2] Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-MA-01, Version 1.01, 22 July 2014, BSI [PACE-PP].

1.2 TOE Reference

TOE Commercial Name	TnD v5.1 on ID-One Cosmo X (PACE/EAC1/Polymorphic eMRTD/LDS2 configuration)
Applet Code Versions (SAAAAR Code)	See **TOE Configurations** table below
Applet Internal Versions	See **Applet Internal Versions** table below
Platform Name	ID-One Cosmo X
Platform Certificate	[PTF-CERT]
Platform Identification	SAAAAR Code: 093363
IC Certificate Reference	BSI_DSZ-CC-1107-V3-2022

The following table defines the TOE configurations, depending on the source code compilation and build options:

Configurations	Description of the configurations	Content of the config (package/cap files)	
Config 1	TnD Applet without support for MOC	SAAAAR + version + Config of TnD Java Applet on Cosmo X {config 1}	203621FF 05010000 **0101**
		SAAAAR + version + config of Common Package {Cosmo X build} {Config 1}	417641FF 01000000 **0201**
Config 2	TnD Applet with support for MOC	SAAAAR + version + config of TnD Java Applet on Cosmo X {config 2}	203621FF 05010000 **0201**
		SAAAAR + version + config of Common Package {Cosmo X build} {Config 2}	417641FF 01000000 **0301**

Table 1 TOE Configurations

Note:
In the table above a "SAAAAR code" is denoted by first 4 bytes, a "version" by the next 2 bytes and a "config" ID by the last 2 bytes.

The "SAAAAR" is the product configuration item number within IDEMIA and is uniquely defined as:

S	IDEMIA Site code	1 byte
AAAA	Article number	4 bytes
R	Software Release number	1 byte

Applet Internal Versions of above Configurations are as follows:

Configurations	Returned value of DF67
Config 1	00 00 02 08 01 01 00 08
Config 2	00 00 02 08 01 04 00 07

Table 2 Applet Internal Versions

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-03110-1].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a travel document and a terminal as required by [TR-03110-1], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SO_D and (iv) Terminal Authentication v.1. 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.
Active Authentication	Security mechanism defined in [ICAO-9303]. Option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
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 MRTDs chip to store the Initialisation Data and Pre-personalisation Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
Basic Access Control	Security mechanism defined in [ICAO-9303] by which means the MTRD'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 travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorised by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.
Biographical data (bio data).	The personalised details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa.
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD'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.

Term	Definition
Certificate chain	A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means.
Country Signing CA Certificate (C_{CSCA})	Self-signed certificate of the Country Signing CA Public Key ($K_{Pu\ CSCA}$) issued by CSCA stored in the inspection system.
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO-9303], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-1].
Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [TR-03110-1]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organizational entity within this ST. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO-9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-1].
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.

Term	Definition
Document Details Data	Data printed on and electronically stored in the travel 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 MRTD'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 MRTD's chip. It may carry the Document Signer Certificate (CDS). [ICAO-9303]
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [TR-03110-1] and [ICAO-9303]. This role is usually delegated to a Personalisation Agent.
Document Verifier (DV)	An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, see [TR-03110-1]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this ST. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy) [1] [2]
Eavesdropper	A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD'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]
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 travel document (MRTD).

[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
	See [TR-03110-1]. [PP-EAC] definition Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes the file structure implementing the LDS [ICAO-9303], the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and the TSF Data including the definition the authentication data but except the authentication data itself.
Extended Access Control	Security mechanism identified in [ICAO-9303] by which means the MTRD'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 MRTD 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 MRTDs. [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.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to

Term	Definition
	represent himself or herself as another person for the purpose of using that person's document.
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO-9303]
Initialisation	Process of writing Initialisation Data (see below) to the TOE (TOE life-cycle, Phase 2 Manufacturing, Step 3).
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveller (the MRTD 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 MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO-9303]]
Issuing State	The Country issuing the MRTD. [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 MRTD's chip.
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 travel document	Data of the travel document holder stored according to the Logical Data Structure [ICAO-9303] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) personal data of the travel document holder the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), the digitized portraits (EF.DG2), the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and the other data according to LDS (EF.DG5 to EF.DG16).

Term	Definition
	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 MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, 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 travel document in a form that can be read and verified by machine. [ICAO-9303]
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [TR-03110-1]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD'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

Term	Definition
	as read from the MRZ, see [ICAO-9303] part 11 or a user PIN or PUK as specified in [TR-03110-3]
Polymorphic Authentication Terminal / Service	The terminal or authentication web service that is authorized to retrieve the Polymorphic ID attributes form a Polymorphic eMRTD using standard ICAO and EAC1 ePassport protocols (PACE, CAv1, TAv1) and the Polymorphic Authentication (PMA)protocol to retrieve the PP, PI and CPI data. A Polymorphic Authentication Terminal/Service: • implements the terminal part of the PACEv2 with PIN, PA, CAv1 and TAv1 protocols configured in accordance with ICAO DOC9303 and TR-03110 v2.10 and the Polymorphic Authentication protocol (PMA). • performs the Advanced Inspection Procedure as a precondition to gain access to the randomized polymorphic user data (PI, PP and optional CPI) by executing the PMA protocol. The Polymorphic Authentication Terminal/Service must pass PACE with the correct user PIN and successful CAv1/TAv1 in order to be able to execute the PMA protocol successfully. performs the Polymorphic Authentication protocol (PMA) to retrieve the randomized polymorphic user data (PI, PP and optional CPI) and the non-card unique identifiable meta data.
Polymorphic Authentication System	The complete set of sub systems in the polymorphic authentication infrastructure, required to perform user authentication with privacy protection based on (randomized) Polymorphic ID attributes: • Polymorphic Authentication Service • (Central) Key Management Authority • (optional) Polymorphic eMRTD Status Service Polymorphic Service Provider
Polymorphic document holder	The owner of a Polymorphic eMRTD, that contains his Polymorphic ID attributes.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the "Enrolment" (cf. paragraph 1.7.4.3, TOE life-cycle, Phase 3, Step 6).
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: ICAO eMRTD (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [TR-03110-1],

Term	Definition
	(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). Polymorphic eMRTD (i) establishing the identity of the polymorphic document holder for requesting the Polymorphic ID attributes, (ii) Requesting the required Polymorphic eMRTD ID attributes from the central Key Management authority, (iii) writing Polymorphic ID attributes, Polymorphic LDS data as defined in [PCA-eMRTD], (iv) writing the TSF data as defined in [PCA-eMRTD], (v) signing the Document Security Object defined in [ICAO-9303] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
Personalisation Data	A set of data incl. individual-related data (biographic and biometric data) of the travel document holder, dedicated document details data and dedicated initial TSF data (incl. the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing.
Personalisation Agent Authentication Information	TSF data used for authentication proof and verification of the Personalisation Agent.
Personalisation Agent Key	Symmetric cryptographic key or key set (MAC, ENC) used by the Personalisation Agent to prove his identity and get access to the logical travel document and by the MRTD'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 (FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM for PACE CAM).
Physical part of the travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) biographical data, data of the machine-readable zone, photographic image and other data.
Pre-personalisation	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (TOE life-cycle, Phase 2, Step 5)
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalised MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It

Term	Definition
	contains (but is not limited to) the Personalisation Agent Key Pair and Chip Life-Cycle Production data (CPLC data).
Pre-personalised travel document's chip	Travel document's chip equipped with a unique identifier.
Receiving State	The Country to which the MRTD 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 travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Skimming	Imitation of the inspection system to read the logical MRTD 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 travel 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 eMRTDs	This section describes an inspection procedure designed for eMRTDs containing one or more applications besides the eMRTD application ("LDS2-documents"): [LDS2_TR] Annex A2.
Terminal	A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE. Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel 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.

Term	Definition
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
Travel document	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO-9303] (there "Machine readable travel document").
Travel document (electronic)	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: *ePassport*.
Travel Document Holder	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document.
Travel document's Chip	A contact based / contactless integrated circuit chip complying with ISO/IEC 14443 [15] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO-9303], sec III.
Traveller	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [CC-1]).
Unpersonalised travel document	The travel document that contains the travel document chip holding only Initialisation Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.
User data	All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [5] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE. 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 [CC-1]). 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 [CC-2]).
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
CC	Common Criteria
BIS	Basic Inspection System
BIS-PACE	Basic Inspection System with PACE
CA	Chip Authentication
CAN	Card Access Number
CLFDB	Ciphered Load File Data Block
PS	Personalisation System
DBI	Digital Blurring of Images
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DF	Dedicated File
DH	Diffie Hellman
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EF	Elementary File
FID	File identifier
GP	Global Platform
IC	Integrated Chip
ICC	Integrated Chip card
ICCSN	Integrated Circuit Card Serial Number.
IFD	Interface Device
MAC	Message Authentication code
MF	Master File
MRZ	Machine readable zone
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
PT	Personalisation Terminal
RF	Radio Frequency
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
RSA CRT	Rivest Shamir Adleman – Chinese Remainder Theorem
SAI	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
TSP	TOE Security Policy (defined by the current document)

2.3 References

Reference	Description
[AGD_OPE]	FQR 220 1580 Ed 2 - TnD v5.1 on ID-One Cosmo X - Operational User Guidance (AGD_OPE)
[AGD_PRE]	FQR 220 1579 Ed 4 - TnD v5.1 on ID-One Cosmo X - Preparative Procedures (AGD_PRE)
[BAC-PP]	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
[EAC-PP]	EAC- Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0056 v1.10 25th march 2009
[EAC-PP-V2]	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
[EACv2-PP]	Common Criteria Protection Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110, BSI-CC-PP-0086, Version 1.01, May 20th, 2015, BSI
[PACE-PP]	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
[CC-1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017. CCMB-2017-04-001.
[CC-2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-002.
[CC-3]	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.
[ICAO-9303]	International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – 7th edition, 2015
[PCA-eMRTD]	Polymorphic eMRTD Specification. V2.1. 03-04-2018. IDEMIA.
[LDS2_TR]	TECHNICAL REPORT LDS2 – Protocols Version 0.8 04-27- 2017
[9303-10_LDS2]	TR Logical Data Structure (LDS) for Storage of Data in the Contactless IC - Doc 9303-10 LDS 2 – New Applications, v21, 10-11-2018.
[LDS2_PKI]	TR LDS2-PKI, v1.1, March 2019 ((Preliminary Publication), ICAO
[TR-03110-1]	Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012 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 2.10, 20.03.2012 by BSI
[TR-03110-3]	TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3: Common Specifications, version 2.10, 2012-03-07 by BSI

Reference	Description
[ISO14443]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2016
[ISO15946-2]	ISO/IEC15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.
[ISO15946-3]	ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002
[ISO18013-3]	ISO/IEC 18013-3: Information technology — Personal identification — ISO-compliant driving licence. Part 3: Access control, authentication and integrity validation, 2009-03-01 Including ISO/CEI 18013-3/AC1:2011, TECHNICAL CORRIGENDUM 1, Published 2011-12-01
[ISO7816]	ISO/IEC 7816: Identification cards — Integrated circuit cards.
[ISO9796-2]	ISO/IEC 9796-2: 2002, Information Technology - Security Techniques - Digital Signature Schemes giving message recovery - Part 2: Integer factorization based mechanisms
[ISO11770-2]	ISO/IEC 11770-2. Information Technology – Security techniques – Key management – part 2: Mechanisms using symmetric techniques, 1996
[JCAPI]	Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5. May 2015.
[PP-PL]	Java Card System - Open Configuration Protection Profile, Version 3.0.5, BSI-CC-PP-0099-2017
[PTF-ST]	Security Target Lite ID-ONE COSMO X, FQR 110 9730 Ed 8
[PTF-CERT]	ANSSI-CC-2021/29-S01-V2
[NIST-180-4]	NIST. FIPS 180-4, Secure Hash Standard, February 2011.
[NIST-186-3]	NIST. Digital Signature Standard (DSS), FIPS 186-3, 2009
[NIST-800-38B]	NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, 2005
[RFC-5639]	Lochter, Manfred; Merkle, Johannes. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, 2010
[RSA-PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[ANSSI-FRP256V1]	Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français NOR: PRMD1123151V (Le 18 avril 2012)- ANSSI
[DH]	Rescorla, Eric, RFC 2631: Diffie-Hellman key agreement method, 1999
[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.
[TR-03111]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, 17.04.2009
[ANSI_X9.31]	"Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)" ANSI X9.31-1998, American Bankers Association
[IEEE_1363]	IEEE Std 1363a-2004 Standard Specification of Public-Key Cryptography

3 TOE overview and description

3.1 TOE Overview

The TOE is a composite product that consist of an IDEMIA applet named TnD v5.1 and its supporting "Common" library package on top of the COSMO X Global Platform Java Card 3.0.5 operating system and Infineon SLC37 contact/contactless smart card security controller in **PACE/EAC1/Polymorphic eMRTD/LDS2 configuration**.

It supports the ICAO and TR-3110-1 and -3 defined protocols for EAC1 (Chip Authentication v1 and Terminal Authentication v1), PACE (Generic Mapping (GM), Integrated Mapping (IM) and Chip Authentication Mapping (CAM)), Active Authentication (AA) and LDS2 protocol extensions for EAC1 and PACE. In addition, the TOE supports Polymorphic Authentication protocol (PMA) for privacy-protected authentication with polymorphic ID attributes.

For compliancy with the protection profiles claimed in this security target, the PACE and EAC1 protocols MUST be configured on the TOE for each configured ID document application mentioned below.

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:

- ICAO/EAC eMRTD, including LDS2 Travel records (stamps), Visa records and Additional biometrics in accordance with ICAO [ICAO-9303] and [LDS2_TR] specifications,
- Polymorphic eMRTD according to Dutch national specification and
- EU/ISO Driving Licence compliant to ISO/IEC 18013 or ISO/IEC TR 19446.

The Polymorphic eMRTD application is in compliance with the Polymorphic eMRTD Specification of the Dutch National Office of Identity Data (written by IDEMIA). This ensures authentication to an authentication service at eIDAS High assurance level, without revealing privacy sensitive ID attributes the authentication service provider. This is accomplished by the TOE's Polymorphic Authentication (PMA) protocol, which randomizes Polymorphic Pseudonym, Identity and Complementary ID attributes.

The TOE may also be used as an ISO Driving Licence (IDL) compliant to ISO/IEC 18013 or ISO/IEC TR 19446, as both eMRTD and IDL applications share the same protocols and data structure organization.

The TnD v5.1 application embeds other secure functionalities (e.g. BAC and EAC in combination with BAC), which are not in the scope of this evaluation, but are covered in the scope of other evaluated configurations of this product shown in Table 3 below.

This ST considers the TnD v5.1 application in the **PACE/EAC1/Polymorphic eMRTD/LDS2 configuration**.

Configuration	**PP Conformity**	**Extensions to the PP**
1. EAC	PP0056v1 (EAC)	- Active Authentication (AA) - Restart secure messaging AES128, AES192 and AES256 secure messaging (in addition to 3DES) after CAv1 - Digital Blurring of Images (DBI)
2. PACE/EAC1/Polymorphic eMRTD/LDS2	**PP 0068 (PACE)**	- **ICAO LDS2 protocol extensions for TAv1, PACE and CAv1**

Configuration	PP Conformity	Extensions to the PP
	PP0056v2 (ICAO application, EAC with PACE)	- **Polymorphic eMRTD extensions for PMA and PACE** - **Active Authentication (AA)** - **PACE-CAM** - **BAC de-activation** - **Digital Blurring of Images (DBI)**
3. BAC	PP 0055 (BAC)	- Active Authentication (AA) - Chip Authentication v1 (CAv1) - Restart secure messaging AES128, AES192 and AES256 secure messaging (in addition to 3DES) after CAv1

Table 3 Different evaluated configurations of the TnD application

Note
For interoperability reasons, an eMRTD will most likely support BAC, PACE and EAC. The three TOE configurations mentioned above cover the security level of the TOE depending on the inspection procedure executed by the Inspection System/Advanced Inspection System:

- If the Inspection System reads MRTD data after having performed BAC + EAC, the security of the MRTD will be covered by the security evaluation of the TOE described in the ST claiming compliance to [EAC-PP].
- If the Inspection System reads MRTD data after having performed PACE + EAC, the security of the MRTD will be covered by the security evaluation of the TOE described in this ST, claiming compliance to [EAC-PP-V2] and [PACE-PP].
- If the Inspection System 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 [BAC-PP].

3.2 TOE Description

The TOE in the PACE/EAC1/Polymorphic/LDS2 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 and PACE-CAM;
  - Secure import and/or on-chip generation of the AA key pair;
  - life-cycle phase switching to operational phase;

- In operational phase:
  - PACE mapping types Generic Mapping (GM), Integrated Mapping (IM) and Chip Authentication Mapping (CAM)*;
    Note*: The availability of PACE-CAM depends on platform configuration;
  - PACE passwords: MRZ, CAN, PIN and PUK;

- PACE PIN/PUK suspend/resume mechanism according to [TR-03110-2] in case of TOE communication over the contactless interface;
- PIN/PUK verify and PIN reset;
- EAC1: 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 EAC1: access control to DG3 and DG4 based on the effective authorization established during TAv1;
- After EAC1: Polymorphic Authentication;
- LDS2 protocol extensions for PACE, TAv1 and CAv1 and EAC1 access control to LDS2 applications (Travel records, Visa records and Additional Biometrics);
- Automatic BAC phasing out;
- Digital Blurring of Images (DBI).

Note:
TnD v5.1 applet supports Match on Card (MoC) functionality, which is used to support the DBI deactivation. MoC as a security feature is not within the scope of this Security Target, though may be configured without impacting the security of the TOE.

3.2.1 Physical scope

From physical/hardware point of view, 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 because it does not alter nor modify any security functions of the TOE.

The TOE may be used in several form factors, like wafer, chip modules on a reel, chip modules embedded in ID3 passport booklets or ID3 holder pages, chip modules embedded in ID1 cards, chip modules embedded in antenna inlays, etc.

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.

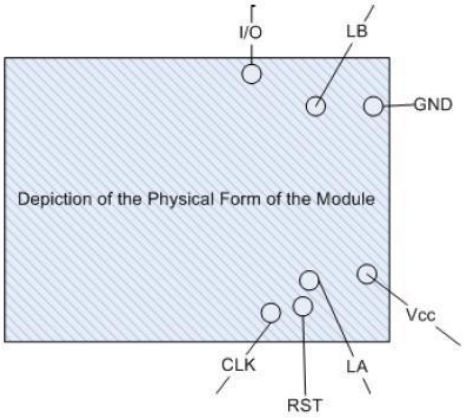

Figure 1 Physical Form

The contactless ports (LA and LB) of the module require a connection to an antenna. The other ports are required for connection to the contact plate of the contact chip module. The chip module's electrical interfaces are according to [ISO7816] and [ISO14443] interface specifications for respectively contact and contactless connections to card reader devices.

Port	Description	Logical Interface Type
VCC, GND	ISO 7816: Supply voltage	Power (not available in contactless-only configurations)
RST	ISO 7816: Reset	Control in (not available in contactless-only configurations)
CLK	ISO 7816: Clock	Control in (not available in contactless-only configurations)
I/O	ISO 7816: Input/ Output	Control in, Data in, Data out, Status out (not available in contactless-only configurations)
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out (Not available in Contact-only configurations)

Table 4 TOE physical ports and interfaces

3.2.2 Logical Scope

The Target of Evaluation (TOE), addressed by the this security target, is an electronic travel document representing a contactless/contact based smart card or passport, programmed according to the Logical data structure (LDS) and authentication protocols specified in [ICAO-9303], [9303-10_LDS2], [LDS2_TR], [TR-03110-1], [TR-03110-3] and [PCA-eMRTD]. The TOE supports:

- Password Authenticated Connection Establishment (PACE) with the following mapping modes:
  - Generic Mapping (GM),
  - Integrated Mapping (IM) and
  - Chip Authentication Mapping (CAM)
- EAC1 protocols
  - Chip Authentication v1 (CAv1) and
  - Terminal Authentication v1 (TAv1)
- Active Authentication (AA) and
- Polymorphic eMRTD extensions
  - Polymorphic Authentication protocol (PMA) for privacy-protected authentication with polymorphic ID attributes.
  - PACE PIN and PUK passwords in addition to ICAO defined MRZ and CAN;
  - PACE PIN/PUK suspend/resume mechanism according to [TR-03110-2] in case of TOE communication over the contactless interface.
  - PIN/PUK verify and PIN reset functionality;
- LDS2 protocol extensions for EAC1 and PACE providing:
  - CV certificate extensions for TAv1
  - PACE extension in accordance with [TR-03110-3] to return the eMRTD's EAC trust point information required for TAv1.
- BAC phasing out
- Digital Blurring of Images (DBI)

In accordance with [EAC-PP-V2] and [PACE-PP] and the communication between terminal and chip SHALL be established and protected by the Password Authenticated Connection Establishment (PACE) protocol.

The Polymorphic eMRTD extensions present on the TOE enable secure authentication with enhanced privacy protection features. It provides the ID document holder the possibility to authenticate towards

a service provider at eIDAS High assurance level in a non-traceable and non-linkable manner thanks to usage of Polymorphic Pseudonyms and other Polymorphic ID attributes. This is accomplished by the TOE's Polymorphic Authentication (PMA) protocol, which randomizes Polymorphic Pseudonym, Identity and Complementary ID attributes.

The ICAO LDS2 protocol and Logical Data Structure extensions are available in the TOE for supporting secure access and storage Electronic visas, electronic travel stamps or additional biometrics like fingerprint or an iris scan.

The TnD v5.1 on ID-One Cosmo X TOE consists of:

- The MRTD's chip circuitry and the IC dedicated software;
- The IC embedded software being the "ID-One Cosmo X platform" consisting of
    - Java Card virtual machine, ensuring language-level security;
    - Java Card runtime environment, providing additional security features for Java card technology enabled devices;
    - Java card API, providing access to card's resources for the Applet;
    - Global Platform Card Manager, responsible for management of Applets on the card.
    - Crypto Library.
- TnD v5.1 Applet along with its Common (library) Package loaded in non-volatile (FLASH) memory*;
- The associated guidance documentation in [AGD_PRE] and [AGD_OPE];
- The Personalisation Agent Key set (see [AGD_PRE]).

* In the remaining part of this Security Target, we refer "TnD v5.1 Applet along with its Common (library) Package" as "TnD v5.1 Application".

A schematic overview of the TOE's logical architecture is shown in Figure 1 below.

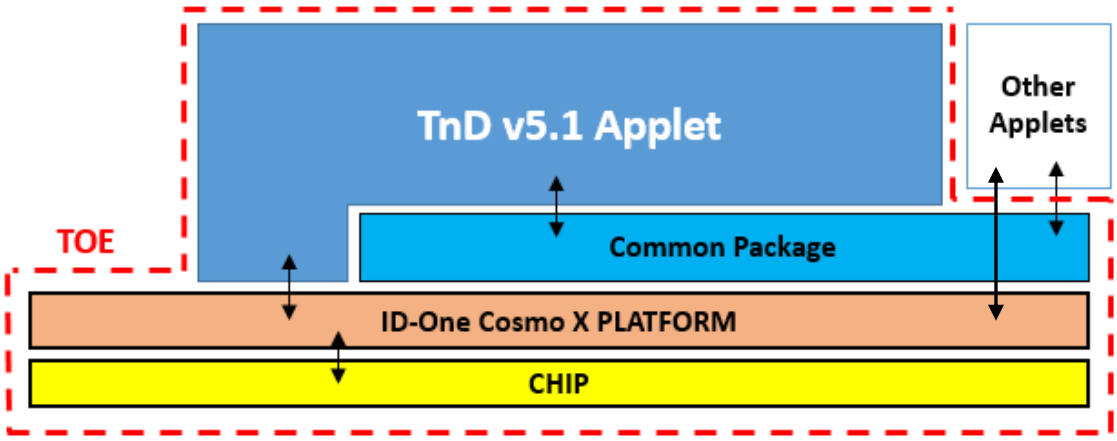

Figure 2 TOE's logical architecture

The TOE is a composition of the TnD v5.1 applet plus Common Package and the ID-One Cosmo X platform, which has been certified by the French certification body ANSSI.

The following guidance documents will be provided with the TOE:

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

Table 5 TOE Guidance

This ST Lite will also be provided along with above-mentioned documents.

The above-mentioned guidance documents will be delivered by email in PGP signed and encrypted format.

Platform related guidance documents are mentioned in [PTF-ST].

Section 4, "Life Cycle" in this ST provides for more details about the TOE delivery for the different options.

3.3 Required Non-TOE hardware/software/firmware

The TOE does not require any explicit non-TOE hardware, software or firmware to perform its claimed security features. The TOE comprises the chip, the complete operating system and the TnD v5.1 application. Note that for an ICAO compliant ID document, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete travel document. Nevertheless, these parts are not critical for the security of the TOE.
In order to powerup the TOE and to communicate with it, a card reader is required.

3.4 TOE usage and security features for operational use

3.4.1 TOE usage

Depending on its configuration during pre-personalisation and personalisation, the TOE can be used as:

- ICAO/EAC eMRTD including Travel records (stamps), Visa records and Additional biometrics,
- Polymorphic eMRTD and
- EU/ISO Driving Licence.

The ICAO/EAC eMRTD, Polymorphic eMRTD and Driver Licence are installed as a separate application instances of the TnD v5.1 applet, each having its own dedicated application identifier and personalisation. The following TOE configurations are covered within the scope of this Security Target:

Configuration at Personalisation	ICAO/EAC with PACE eMRTD	Polymorphic eMRTD	LDS2	Driver licence
1	present	-	-	-
2	present	present		-
3	present	present	present	-
4	present	-	present	-
5	-	-	-	present
6	-	present	-	present

Configuration at Personalisation	ICAO/EAC with PACE eMRTD	Polymorphic eMRTD	LDS2	Driver licence
7	-	present	-	-

Table 6 TOE Configurations during Personalisation

The authentication protocols PACEv2, Chip authentication (CAv1), Active Authentication and Terminal Authentication (TAv1) specified in [ICAO-9303] and [TR-03110] have also been referred to in ISO18013 for EU driving licences. The BAP-1 protocol defined in ISO18013 is equal to Basic Access Protocol (BAC) defined in [ICAO-9303]. As to the logical data structure, the ISO18013 uses the same concept of Passive Authentication defined in [ICAO-9303], but specifies different ISO7816-4 elementary file identifiers for storing the ICAO defined content of DG3, DG4 and DG15.
When an Issuing state is using the product as an ISO compliant Driving licence, the following name mapping of roles, definitions, data groups and protocol is applicable within the scope of this security target:

MRTD	ISO Driving License
MRTD	IDL
ICAO	ISO/IEC
ICAO 9303	ISO/IEC 18013 or ISO/IEC TR 19446
BAC	BAP-1
DG3	DG7
DG4	DG8
DG15	DG13
MRZ	MRZ or SAI (Scanning Area Identifier)
Traveller	Holder

Table 7 eMRTD and IDL Terminology

Note
Iin the remaining parts of this document, the word "MRTD" SHOULD be understood either as an MRTD in the sense of ICAO or a driving license compliant to ISO/IEC 18013 or ISO/IEC TR 19446 depending on the targeted usage envisioned by the issuer.

A State or Organization issues MRTDs to be used by the holder for international travel. The traveller 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 traveller 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 travel 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.

This security target addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. Also it addresses the Chip Authentication Version 1 described in [TR-03110] as an alternative to the Active Authentication stated in [ICAO-9303].

During the pre-personalisation and personalisation, the Personalisation Agent, once authenticated, gets the rights (access control) for (1) reading and writing data,(2) instantiating the application, and (4) writing of personalisation data. The Personalisation Agent can so create the file structure (MF / ADF) required for this configuration.

The DBI feature is used as an additional layer of security during personalization. When the DBI Activation process is performed, the biometric image of the card holder shall be corrupted/blurred. After personalization, a specific terminal that has a de-blurring access rights will be used to deactivate or revert the image to its original state. If this step is not performed, this means that the proper personalization up to issuance procedures were not followed. The photo will remain blurred which will be noticeable when reading the contents of the document. This will alert the agencies that the document has been compromised.

3.4.2 TOE Security Features

3.4.2.1 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 realized with the INTERNAL AUTHENTICATE command. The key and algorithms supported are the following:

RSA ISO/IEC 9796-2 with a key length of 1536, 1792, 2048, 2560, 3072, 3584 and 4096 bits and hashing algorithm of SHA1 or SHA2 (i.e. SHA224, SHA256, SHA384 and SHA512).

ECDSA over prime field curves with hashing algorithm of SHA1 or SHA2 and the key sizes 192 to 521.

3.4.2.2 Basic Access Control (BAC)

The protocol for Basic Access Control is specified by [BAC-PP]. 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 in the MRZ (for MRTD), 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 8 BAC Configuration

3.4.2.3 Terminal Authentication

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.

3.4.2.4 Chip Authentication 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 v1 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 restarts secure messaging with new agreed 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.

3.4.2.5 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.

The PACE protocol is executed by issuing the following sequence of 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	SHA1
PACE–ECDH–GM– AES–128	Generic	AES	16	CBC/CMAC	CMAC	SHA1
PACE–ECDH–GM– AES–192	Generic	AES	24	CBC/CMAC	CMAC	SHA256
PACE–ECDH–GM– AES–256	Generic	AES	32	CBC/CMAC	CMAC	SHA256
PACE–ECDH–IM– 3DES	Integrated	3DES 2Key	16	CBC/Retail MAC	Retail MAC	SHA1
PACE–ECDH–IM– AES–128	Integrated	AES	16	CBC/CMAC	CMAC	SHA1
PACE–ECDH–IM– AES–192	Integrated	AES	24	CBC/CMAC	CMAC	SHA256
PACE–ECDH–IM– AES–256	Integrated	AES	32	CBC/CMAC	CMAC	SHA256
PACE–ECDH–CAM– AES–128	Chip Authentication	AES	16	CBC/CMAC	CMAC	SHA1
PACE–ECDH–CAM– AES–192	Chip Authentication	AES	24	CBC/CMAC	CMAC	SHA256
PACE–ECDH–CAM– AES–256	Chip Authentication	AES	32	CBC/CMAC	CMAC	SHA256
PACE–DH–GM– 3DES	Generic	3DES 2Key	16	CBC/Retail MAC	Retail MAC	SHA1
PACE–DH–GM– AES–128	Generic	AES	16	CBC/CMAC	CMAC	SHA1
PACE–DH–GM– AES–192	Generic	AES	24	CBC/CMAC	CMAC	SHA256
PACE–DH–GM– AES–256	Generic	AES	32	CBC/CMAC	CMAC	SHA256
PACE–DH–IM– 3DES	Integrated	3DES 2Key	16	CBC/Retail MAC	Retail MAC	SHA1
PACE–DH–IM– AES–128	Integrated	AES	16	CBC/CMAC	CMAC	SHA1
PACE–DH–IM– AES–192	Integrated	AES	24	CBC/CMAC	CMAC	SHA256
PACE–DH–IM– AES–256	Integrated	AES	32	CBC/CMAC	CMAC	SHA256

Table 9 PACE Configuration

3.4.2.6 Extended Access Control v1 (EAC1)

EAC is an authentication protocol based on a PKI infrastructure. It further ensures that the IS is authorized to read and/or update data stored in the applet. This authentication mechanism generates a strong secure messaging session through the step of Chip Authentication.

This mechanism is realized by the following steps:

1. Chip Authentication v1 (CAv1)

Chip Authentication v1 is achieved by using a MANAGE SECURITY ENVIRONMENT – SET – Key Agreement Template (MSE SET KAT) command
or
by using a MANAGE SECURITY ENVIRONMENT – SET – Authentication Template (MSE SET AT) command followed by GENERAL AUTHENTICATE command.

The Chip Authentication mechanism enables the authentication of the chip by using an authenticated DH scheme. It may be realized in two ways:

- Classical DH (DH El Gamal) with key length of 2048 bits
- DH over Elliptic curves over prime fields (ECDH) with the key length supported by the underlying Java Card platform (minimum key size 192 bits).

2. CV Certificate Chain verification

CV certificate chain verification is established by executing a series of MANAGE SECURITY ENVIRONMENT – SET – Digital Signature Template (MSE SET DST) and PERFORM SECURITY OPERATION – Verify Certificate (PSO VERIFY) commands.

The chain is done to extract a key from the IS certificate, the key which will be used in the Terminal Authentication.

3. Terminal Authentication v1 (TAv1)

Terminal Authentication is achieved by using an EXTERNAL AUTHENTICATE command.

The Terminal Authentication mechanism is an authentication of the IS based on a classical challenge/response scheme. The signature scheme may be:
- ECDSA SHA-1, ECDSA SHA-224, ECDSA SHA-256, ECDSA SHA-384, or ECDSA SHA-512 on elliptic curves over prime field with key length supported by the underlying Java Card platform (key sizes 192 bits to 521 bits).
- RSA SHA-1, SHA-256, or SHA-512 (PKCS#1 v1.5 or PKCS#1 v2.1 - PSS) with a key length of 1280, 1536, 1792, 2048, 2560, 3072, 3584 and 4096 bits.

3.4.2.7 PACE-CAM

The Chip Authentication Mapping is a new mapping mode of PACE. It extends Generic Mapping and integrates Chip Authentication into the PACE protocol. This mapping combines PACE and Chip Authentication into one protocol PACE-CAM, which allows faster execution than the separate protocols (i.e. PACE + CA).

3.4.2.8 Polymorphic eMRTD

In addition to an ICAO/EAC eMRTD functionality, the TOE supports Polymorphic eMRTD extensions that can be configured using the same applet during personalisation. The TOE's Polymorphic eMRTD extensions enable secure authentication with enhanced privacy protection features. The Polymorphic extensions provide the holder the possibility to authenticate towards a service provider using an

authentication service in a non-traceable and non-linkable manner thanks to usage of Polymorphic ID attributes.

The Polymorphic extensions are used to configure a Polymorphic eMRTD as stand alone application instance or next to an ICAO/EAC eMRTD/Driving application licence instance having its own application identifier during personalisation.

The Polymorphic eMRTD uses the same ICAO and EAC1 protocols like PACEv2, Chip Authentication v1 (CAv1) and Terminal Authentication (v1) as defined in [ICAO-9303], [TR-03110-1] and [TR-03110-3]. The TOE's Polymorphic eMRTD extensions provide the following features:

- Secure storage of the Polymorphic ID attributes during personalisation of the TOE.
- Polymorphic Authentication Protocol (PMA) for authenticated access with user consent, randomization and secure readout of the Polymorphic ID attributes, in combination with PACEv2 and EAC1 eMRTD protocols.
- PACEv2 protocol extended with PIN and PUK passwords, to enforce user authentication (document holder verification) in compliance with [TR-03101-3].

For Polymorphic eMRTD, the PACE protocol is configured with PIN and PUK passwords in compliance with [TR-03110-3] during personalisation. Only PACE-GM and PACE-IM are configurable for a Polymorphic eMRTD.

The Active Authentication protocol shall not be configured for a polymorphic eMRTD.

The logical data structure consists only of EF.CVCA, DG14 and EF.SOD. In order to assure a sufficient level of privacy during authentication the CAv1 private key and EF.SOD are shared amoung a sufficient high number of personalised Polymorphic eMRTDs, i.e. the logical data structure does not contain any unique identifiable data.

3.4.2.9 LDS2 eMRTD

In addition to an ICAO/EAC eMRTD LDS functionality, the TOE supports ICAO LDS2 extensions for PACE, Chip Authentication v1 and Terminal Authentication v1 and EAC1 access control to three (new) LDS2 applications. The CAv1 and TAv1 authentication protocols can now be executed now at MF level and the PACE protocol has extended functionality to return the eMRTD's EAC trust point information required for TAv1. TAv1 functionality is extended to support card verifiable CV certificates with LDS2 certificate extensions. LDS2 specific ISO7816 command APDUs are present in order to perform file and record management of LDS2 application data.

The logical data structure is extended at MF level with three new (optional) Application Dedicated Files (ADF), one for Travel Records (stamps), one for Visas records and one for Additional biometrics.

An LDS2 compliant eMRTD may support one, several or all of these applications. The logical data structure and protocol extensions for PACE, CAv1 and TAv1 are specified in [9303-10_LDS2] and [LDS2_TR] repectively. The records integrates the Signature by LDS2 Signer and LDS2-TS Signer Certificate Reference. This new file structure allows the writing of data after personalisation and allows for States to add additional travel information. For access to applications the IC requires the execution of PACE.

The LDS2 application is written to the contactless IC of an eMRTD, by the Issuing State or organization at the time of personalisation. Before LDS2 terminal application of another State can write LDS2 data into an LDS2 application, it must have the proper LDS2 authorization right from the Issuing State or organization configured in its CV certificate. Each LDS2 data object is digitally signed by an LDS2 Signer of the writing State and subsequently written to the LDS2 application.

The authenticity and integrity of the data (representing the stamps, the visas and biometrics) is protected by the creation and verification of digital signatures over the LDS2 data objects.

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].

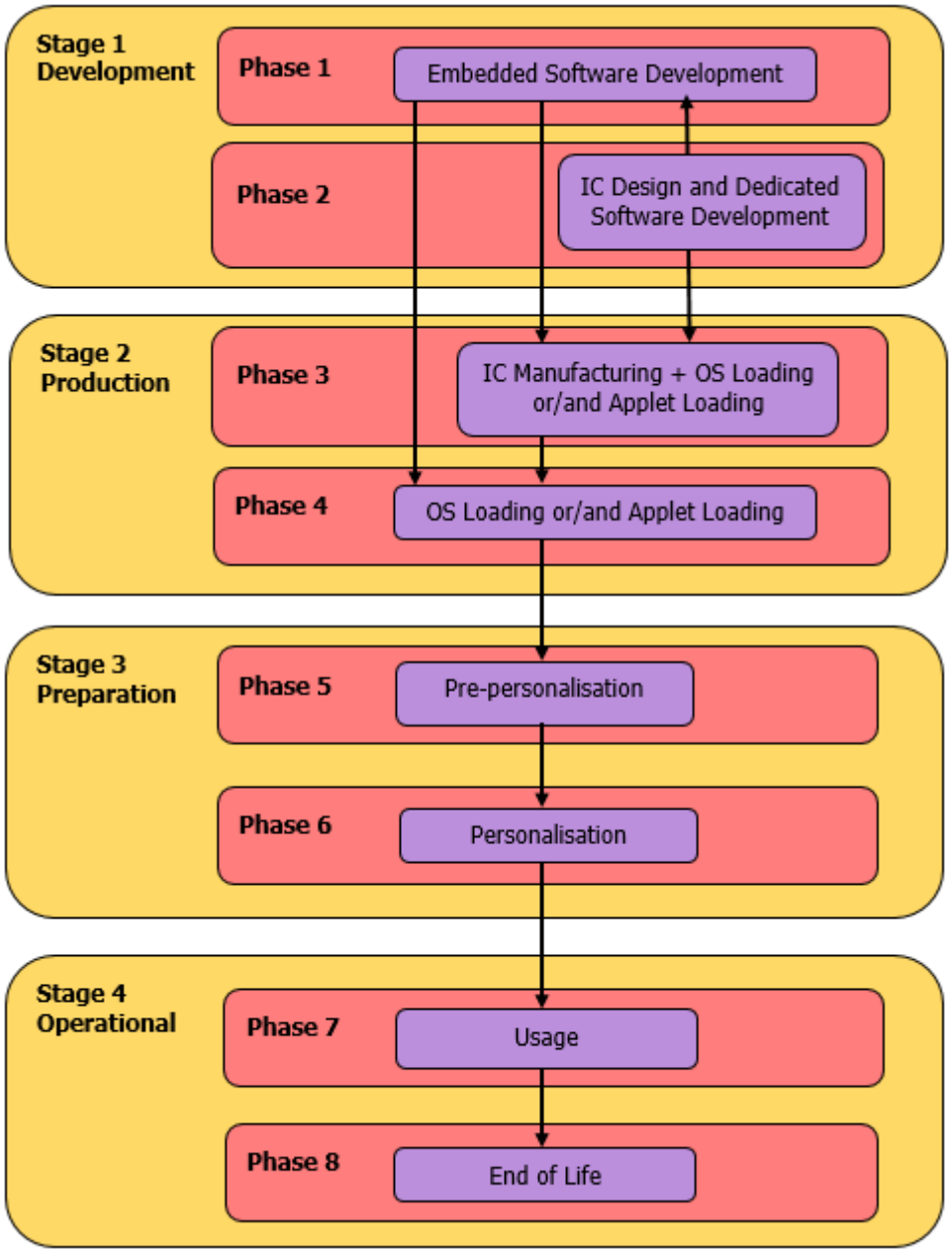

Figure 3 Life cycle Overview

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 TnD v5.1 Application)
- 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 TnD v5.1 Application).

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
TnD v5.1 Applet Developer	IDEMIA	MANILA, JAKARTA,COURBEVOIE and PESSAC R&D sites	ALC
Embedded Software Developer (Java Card Open Platform)	IDEMIA	Platform Developer Refer to [PTF-ST]	ALC
Redaction and Review of Documents	IDEMIA	NOIDA and HAARLEM R&D site	ALC
IC Developer	INFINEON	IC Manufacturer Refer to [PTF-ST]	ALC

4.2 Production Environment

In this environment, the following two phases take place:

- Phase 3: IC Manufacturing
- Phase 4: ID-One Cosmo X Operating System loading and TnD v5.1 Application loading (TnD v5.1 applet and its Common package)

The TnD v5.1 Applet run time code and its Common Package are 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].**

(Option 1) Image Loading audited IC Manufacturer site

FLASH image containing both the "Cosmo X" Java Card Platform OS along with the TnD v5.1 Application is securely delivered directly from the software developer (IDEMIA R&D Audited Site) to the **IC Manufacturer** (Infineon CC Audited Site) to be loaded into FLASH memory. The FLASH image is always encrypted. Decryption is performed by the FLASH loader application inside the IC. The IC loader application is preconfigured with the FLASH decryption (and Authentication) key the during IC wafer initialisation by the IC Manufacturer.

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 Java Card Platform OS + TnD 5.1 Applet + Common package by the IC Manufacturer has completed.

Package	Actor for FLASH image loading	Site For FLASH image loading	Covered by CC
FLASH image containing Java Card Platform OS + TnD v5.1 Applet and Common package	IC Manufacturer	**IC Manufacturer CC Audited Production Plants specified in [PTF-ST]**	**ALC**

Table 10 Option 1: Both Platform and Applet packages are loaded at IC Manufacturer Site

(Option 2) Image loading at IDEMIA and External sites

FLASH image containing both Cosmo X Platform along with TnD v5.1 Applet and Common package is securely delivered directly from the software developer (IDEMIA R&D Audited Site) for loading to **CC Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen or Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

TOE Delivery point:

- If loading of Java Card Platform package + TnD v5.1 Applet run time code including its Common Package (as described below) is performed in Audited IDEMIA Production Sites, then TOE delivery is considered at the end of Phase 4.

- If loading of Java Card Platform package + + TnD v5.1 Applet run time code including its Common Package (as described below) is performed in Non-Audited IDEMIA Production Sites or External Sites, then TOE delivery is considered after Phase 4.

Package	Actor for FLASH image loading	Site for FLASH image loading	Covered by CC
FLASH image containing the Java Card Platform OS + TnD v5.1 Applet and Common package	IDEMIA Authorized Entity or External Authorized Agent	**CC Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD

Table 11 Option 2: Both Platform and Applet packages are loaded at CC Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites

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

With the Cosmo X Platform already loaded (i.e. present) on the chip, the following options (**3a or 3b (i) or 3b (ii) or 3c**) can be chosen for loading the TnD v5.1 applet and its Common Package.

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

The TnD v5.1 Applet with its Common package along with the TOE's guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

Loading of the TnD v5.1 Applet and its Common package on top of the already present COSMO X 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 TnD v5.1 Applet with its Common package on top of already loaded Java Card Platform package (as described below) is done in a CC Audited IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of the TnD v5.1 Applet with its Common package on top of already loaded Java Card Platform package (as described below) is done in Non-Audited IDEMIA Production Sites or External Sites then, TOE delivery is considered after phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
TnD v5.1 Applet and Common package loaded through GP mechanism using CLFDB Key	IDEMIA Authorized Entity or External Authorized Agent	**Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD

Table 12 Option 3(a): Platform package is loaded at IC Manufacturer Site and Applet package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites through GP Mechanism

(Option 3b) Applet loading using the IDEMIA Resident Application

(i) TnD v5.1 Application with Common package along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

TnD v5.1 applet and its Common package are securely loaded via LSK on top of the present COSMO X Java Card OS in any of these sites. This loading is accomplished by using the IDEMIA "Resident Application" of the COSMO X OS

(ii) The DUMP package (including TnD v5.1 Application with Common package data) with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

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

TOE Delivery points:

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

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

<table>
<tr><th>Package</th><th>Actor</th><th>Site</th><th>Covered by</th></tr>
<tr><td>Image containing only Java Card Platform OS</td><td>IC Manufacturer</td><td>IC Manufacturer Production Plants Refer to [PTF-CERT]</td><td>ALC</td></tr>
<tr><td>3b (i)
TnD v5.1 Applet and Common package loaded through Resident Application using LSK format</td><td>IDEMIA Authorized Entity
or
External Authorized Agent</td><td rowspan="2">Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)
or
Non-Audited IDEMIA Sites
or
External Sites</td><td rowspan="2">ALC
or
AGD</td></tr>
<tr><td>3b (ii)
DUMP PACKAGE Ciphered format [DSK Secret Live Key]</td><td>IDEMIA Authorized Entity</td></tr>
</table>

Table 13 Platform package is loaded at IC Manufacturer Site and 3b (i) Applet package is loaded through resident application using LSK format and 3b (ii) DUMP Package is loaded through resident application using DSK Secret Live Key - at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites

(Option 3c) Applet loading in plain (unprotected) format using GP
TnD v5.1 Application with Common package along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **CC Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava).

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

TOE Delivery points:

- The loading of TnD v5.1 applet and Common package on top of already loaded Java Card Platform package is done in plain (unprotected) format in Common Criteria Audited IDEMIA Production Sites. The TOE delivery is considered at the end of Phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
TnD v5.1 Applet and Common package in Plain Format	IDEMIA Authorized Entity	CC Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)	ALC

Table 14 Option 3(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at Audited IDEMIA Sites only

(Option 4) Platform and Applet loaded by IDEMIA or 3rd party
Only Cosmo X Platform is securely delivered directly from the software developer (IDEMIA R&D Audited Site) for loading to **CC Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen or Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

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

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

(Option 4a) Applet loading using GP CLFDB mechanism
TnD v5.1 Applet and Common package along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited 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 IDEMIA Production Sites** or **Non-Audited IDEMIA Sites** or **External Sites**.

TOE Delivery points:

- If loading of the TnD v5.1 Applet and Common package on top of already loaded Java Card Platform package (as described below) is done in CC Audited IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of the TnD v5.1 Applet and Common package onto the already loaded Java Card Platform OS package (as described below) is done in Non-Audited IDEMIA Production Sites or External Sites then, TOE delivery is considered after Phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IDEMIA Authorized Entity or External Authorized Agent	**Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD
TnD v5.1 Applet and Common package loaded through GP mechanism using CLFDB Key	IDEMIA Authorized Entity or External Authorized Agent	**Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD

Table 15 Option 4(a): Platform package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites and Applet package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites through GP Mechanism

(Option 4b) Applet loading using the IDEMIA Resident Application

(i) TnD v5.1 Application with Common package along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

Secure loading of TnD v5.1 applet and its Common package is done via LSK on top of the present COSMO X Java Card OS (already loaded by **Audited IDEMIA Production Sites** or **Non-Audited IDEMIA Sites** or **External Sites)** in any of these sites. This loading is accomplished by using the IDEMIA "Resident Application" of the COSMO X OS

(ii) DUMP package (including the TnD v5.1 Applet and Common package data) with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

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

TOE Delivery points:

- If loading of Applet package /DUMP Package on top of already loaded Java Card Platform package (as described below) is done in Audited IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.
- If loading of Applet package /DUMP Package on top of already loaded Java Card Platform package (as described below) is done in Non-Audited IDEMIA Production Sites or External Sites then, TOE delivery is considered after Phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IDEMIA Authorized Entity or External Authorized Agent	**Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD
4b (i) TnD v5.1 Applet and Common package loaded through Resident Application using LSK format	IDEMIA Authorized Entity or External Authorized Agent	**Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD
4b (ii) DUMP PACKAGE Ciphered format [DSK Secret Live Key]	IDEMIA Authorized Entity		

Table 16 Platform package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites and Options 4b(i) Applet package is loaded through Resident

application using LSK format and and 4b(ii) DUMP Package is loaded through resident application using DSK Secret Live Key - at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites

(Option 4c) Applet loading in plain (unprotected) format using GP
TnD v5.1 Application with Common package along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava).

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

TOE Delivery points:

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

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IDEMIA Authorized Entity or External Authorized Agent	**CC Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD
TnD v5.1 Applet and Common package in Plain Format	IDEMIA Authorized Entity	**CC Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)**	**ALC**

Table 17 Option 4(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at CC Audited IDEMIA 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 TnD v5.1 applet 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 [PTF-ST].

4.4 Operational Environment

Phase 7: Use Phase

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

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

This phase is covered by [AGD_OPE] tasks of the TOE and Guidance tasks of [PTF-ST].

5 Conformance Claims

5.1 CC Conformance Claim

This security target claims conformance to the Common Criteria version 3.1, revision 5 ([CC-2] and [CC-3]).

The conformance to the Common Criteria 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"

Table 18 Conformance Rationale

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

Application note

Not all key sizes specified in this security target have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". In order to be protected against attackers with a "high attack potential", sufficiently large cryptographic key sizes SHALL be configured for this TOE. References can be found in national and international document standards. Further details have been specified in the TOE's guidance documentation [AGD_PRE].

5.2 PP Claim

This security target (ST) claims strict conformance to:

- Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP) BSI-CC-PP-0056-V2-2012, Version 1.3.2, 5th December 2012 [EAC-PP-V2].
- 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 [PACE-PP].

The [EAC-PP-V2] claims strict conformance to the PACE Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011, Version 1.0, 2nd November 2011, BSI.

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

5.3 Package Claim

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

5.4 PP Conformance Rationale

This ST claims strict conformance to [EAC-PP-V2]. According to hints in [EAC-PP-V2] parts of the [PACE-PP] have been included into this ST. A detailed justification is given in the following.

5.4.1 Main aspects

- The TOE description is based on the TOE definition and TOE usage of [EAC-PP-V2]. It was enhanced by product specific details.
- All definitions of the security problem definition in [EAC-PP-V2] have been taken exactly from the protection profile in the same wording.
- All security objectives have been taken exactly from [EAC-PP-V2] in the same wording.
- The part of extended components definition has been taken originally from [EAC-PP-V2].
- All SFRs for the TOE have been taken originally from the [EAC-PP-V2] added by according iterations, selections and assignments.
- The security assurance requirements (SARs) have been taken originally from the [EAC-PP-V2]. The requirements are shifted to those of EAL 5+.

5.4.2 Overview of differences between the PP and the ST

a) The Active Authentication has been added to the TOE. For that:

- One assumption has been added to cover Active Authentication during personalisation: **A.Pers_Agent_AA**
- One security objective for the TOE has been added: **OT.AA_Proof.**
- Two security objectives for the environment have been added: **OE.Auth_Key_MRTD** and **OE.AA_MRTD**. These additions to the original objectives of the PP do not contradict with any other objective nor mitigate a threat (or part of a threat) meant to be addressed by security objectives for the TOE in the PP.
- Following security functional requirements have been added:
  - **FCS_COP.1/AA**
  - **FIA_API.1/AA**
  - **FMT_MTD.1/AAPK**
  - **FCS_CKM.1/AA**

b) **OT.BAC_Expiration** has been added to support Automatic deactivation of BAC protocol. The following additional SFRs have been defined for the same:

- **FMT_MOF.1/BAC_EXP**
- **FMT_MTD.1/BAC_EXP**

c) **OT.DBI** has been added to restrict the access to the plain image data of particular EF(s). Enabling the feature will cause the image data to be corrupted during the reading of the file contents until the blurring is removed by an authorized terminal. The following additional SFRs have been defined for the same:

- **FMT_MTD.1/Activate_DBI**
- **FMT_MTD.1/Deactivate_DBI**
- **FMT_MTD.1/DBI_Terminal**

d) The additional functionality of Password Authenticated Connection Establishment with Chip Authentication Mapping (PACE-CAM) has been added to the TOE. It possesses the same security requirements as the PACE functionality, which means that the same security problem definition is applicable for PACE-CAM. **OT.Chip_Auth_Proof_PACE_CAM** has been added.

The following additional SFRs have been defined for PACE-CAM:

- **FIA_UID.1/PACE_CAM**
- **FIA_UAU.1/PACE_CAM**
- **FIA_UAU.4/PACE_CAM**
- **FIA_UAU.5/PACE_CAM**
- **FIA_UAU.6/PACE_CAM**

e) The additional functionality of the Polymorphic eMRTD extensions has been added to the TOE with: (i) additional security problem definition; (ii) additional security objectives; (iii) additional SFRs. Notice that many SFRs are included from the [EACv2-PP].

f) The additional functionality of the LDS2 extension has been added to the TOE with: (i) additional security problem definition; (ii) additional security objectives; (iii) additional SFRs. LDS2 for access control is based on EAC1 [TR-03110-1], and translated in this ST with the conformity to [EAC-PP-V2]. Also for LDS2 data integrity protection, no new definition is added but *Application Notes* reminds that user data mentioned in security definitions include the user data of additional applications Records Travel, Visas Records and Additional Biometrics Records. Indeed, as these additional applications are under the same Master File (MF) than the eMRTD application, user data are considered as a whole wherever possible.

6 Security Problem Definition

6.1 Assets

The assets to be protected by the TOE include the User Data on the travel document's chip, user data transferred between the TOE and the terminal, and travel document tracing data from PACE PP [PACE-PP], chapter 3.1, claimed by [EAC-PP-V2]:

6.1.1 Primary Assets travel document

6.1.1.1 User data stored on the TOE

All data (being not authentication data) stored in the context of the ePassport application of the travel document 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 [BAC-PP].

The generic security properties to be maintained by the current security policy are: confidentiality, integrity and authenticity

6.1.1.2 User data transferred between the TOE and the terminal connected

The terminal connected is an authority represented by Basic Inspection System with PACE.

All data (being not authentication data) being transferred in the context of the ePassport application of the travel document as defined in [ICAO-9303] part 11 between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-9303] part 11). User data can be received and sent.

The generic security properties to be maintained by the current security policy are: Confidentiality, integrity and authenticity.

6.1.1.3 Travel document tracing data

Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.
The generic security property to be maintained by the current security policy is: Unavailability

6.1.2 Secondary Assets travel document

6.1.2.1 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 authorized subjects only.

The property to be maintained by the current security policy is: Availability

6.1.2.2 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 [BAC-PP].
The property to be maintained by the current security policy is: Availability

6.1.2.3 TOE internal secret cryptographic keys

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

The properties to be maintained by the current security policy are: Confidentiality, integrity

6.1.2.4 TOE internal non-secret cryptographic material

Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SO_D containing digital signature) used by the TOE in order to enforce its security functionality.
The properties to be maintained by the current security policy are: Integrity, authenticity

6.1.2.5 Travel document communication establishment authorisation data

Restricted-reveal able authorization information for a human user being used for verification of the authorisation attempts as authorized user (PACE password). These data are stored in the TOE and are not to be send to it.
The properties to be maintained by the current security policy are: Confidentiality, integrity

All primary assets represent User Data in the sense of the CC. The secondary assets represent TSF and TSF-data in the sense of the CC, see [PACE-PP]. The secondary assets also have to be protected by the TOE in order to achieve a sufficient protection of the primary assets.

6.1.3 Additional Assets

6.1.3.1 Logical travel document sensitive User Data

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

6.1.3.2 Authenticity of the travel document chip

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

6.1.4 Assets related to Polymorphic eMRTD

6.1.4.1 Polymorphic eMRTD sensitive User Data stored on the TOE

Sensitive Polymorphic eMRTD user data stored on the TOE:

- Polymorphic representation of the user's main unique identification data (PI) (e.g. Social Security Number, etc.)
- Polymorphic representation of the Pseudonym (PP) derived from the user's main unique identification data
- Polymorphic representation of the user's Complementary Polymorphic Identification data (CPI) (ie. other identification attributes like e.g. the user's name, etc.).

Security Properties: Confidentiality, Integrity

Application Note: This asset is an extension of the asset 'Logical travel document sensitive User Data' defined in [EAC-PP-V2].

6.1.4.2 Secret Polymorphic eMRTD Document Holder Authentication Data

Secret authentication information for the Polymorphic eMRTD document holder being used for verification of the authentication attempts as authorized Polymorphic eMRTD document holder (sent PACE passwords, e.g. CAN or PIN/PUK). Security Properties: Confidentiality, Integrity

6.1.4.3 Polymorphic eMRTD User Data transferred between the TOE and the Terminal

Output data (randomized PI, PP and optional CPI), with the exception of authentication data, that are transferred during usage of the application of the Polymorphic eMRTD document between the TOE and Polymorphic authenticated terminals/Services. The TOE must ensure the Privacy, Integrity and Authenticity of the randomized polymorphic PI, PP and optional CPI data during their transmission to Terminal/Authentication Service connected after the PACE (with PIN), CAv1, TAv1 and the Polymorphic Authentication protocol (PMA) have been executed successfully. Security Properties: Confidentiality, Privacy, Integrity, Authenticity.

Application Note: This asset is an extension of the asset 'user data transferred between the TOE and the terminal connected' defined in [PACE-PP] and [EAC-PP-V2]. As for confidentiality, note that even though not each transferred data element represents a secret, [TR-03110-2] requires confidentiality of all transferred data by secure messaging, employing the encrypt-then-authenticate approach.

6.1.5 Assets related to LDS2

Three applications can be configured; three associated user groups of assets are defined: the Travel Records, the Visas Records and Additional Biometrics Records. The sensitive User Data defined hereafter are considered as User Data in this document.

6.1.5.1 Applications travel document sensitive User Data

This asset includes:

- Entry and Exit records user data from the Travel Records application already stored in the TOE.
- Visa user data from Visa Records application already stored in the TOE.
- Additional Sensitive biometric data from the Additional Biometrics application already stored in the TOE.

The generic security properties to be maintained by the current security policy are: Confidentiality, Integrity, Authenticity

Application Note: This asset is an extension of the asset "Logical travel document sensitive User Data" defined in [EAC-PP-V2].

6.1.5.2 Applications User Data transferred between the TOE and the Terminal

All LDS2 data being transferred in the context of the LDS2 ePassport applications (Entry and Exit records, Visas records), with the exception of authentication data, that are transferred during usage of the application of the eMRTD document between the TOE and authenticated terminals/Services. Security Properties: Confidentiality, Integrity, Authenticity

Application Note: This asset is an extension of the asset 'user data transferred between the TOE and the terminal connected' defined in [PACE-PP] and [EAC-PP-V2]. As for confidentiality, note that even though not each transferred data element represents a secret, [TR-03110-2] requires confidentiality of all transferred data by secure messaging, employing the encrypt-then-authenticate approach. The Additional Biometrics records can't be appended in eMRTD in operational user phase, just written directly if dedicated file.

6.1.5.3 Document Signer (DS)

An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [ICAO-9303]. This role is usually delegated to a Personalisation Agent.

6.2 Users / Subjects

6.2.1 Subjects listed in PP PACE

This ST considers the following external entities and subjects from [PACE-PP] chapter 3.1:

6.2.1.1 Travel document holder

Definition A person for whom the travel document Issuer has personalised the travel document. This entity is commensurate with 'MRTD Holder' in [BAC-PP]. Please note that a travel document holder can also be an attacker (s. below).

6.2.1.2 Travel document presenter

A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [BAC-PP]. Please note that a travel document presenter can also be an attacker (s. below)

6.2.1.3 Terminal

A terminal is any technical system communicating with the TOE either through the contact interface or through the contactless interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated ('Terminal' is used by the travel document presenter). This entity is commensurate with 'Terminal' in [BAC-PP].

6.2.1.4 Basic Inspection System with BIS-PACE

A technical system being used by an inspecting authority and verifying the travel document presenter as the travel Document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication.

6.2.1.5 Document Signer (DS)

An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [ICAO-9303]. This role is usually delegated to a Personalisation Agent.

6.2.1.6 Country Signing Certification Authority (CSCA)

An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel document 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.

6.2.1.7 Personalisation Agent

An organization acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities:

1. establishing the identity of the travel document holder for the biographic data in the travel document,
2. enrolling the biometric reference data of the travel document holder,
3. writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO-9303],
4. writing the document details data,
5. writing the initial TSF data,
6. signing the Document Security Object defined in [ICAO-9303](in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. This entity is commensurate with 'Personalisation agent' in [BAC-PP].

6.2.1.8 Manufacturer

Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [BAC-PP].

6.2.1.9 Attacker

A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most high attack potential. Please note that the attacker might 'capture' any subject role recognised by the TOE. This external entity is commensurate with 'Attacker' in [BAC-PP].

Additionally to this definition, the definition of an attacker is refined as follows: A threat agent trying

1. to manipulate the logical travel document without authorization,
2. to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4),
3. to forge a genuine travel document or
4. to trace a travel document.

6.2.1.10 Additional Subjects

Furthermore, this ST considers the following additional subjects from [EAC-PP-V2]:

6.2.1.11 Country Verifying Certification Authority

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 travel 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.

6.2.1.12 Document Verifier

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 travel document in the limits provided by the issuing States or Organisations in the form of the Document Verifier Certificates.

6.2.1.13 Inspection system (IS)

A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder.
The Extended Inspection System (EIS) performs the Advanced Inspection Procedure and therefore

1. contains a terminal for the communication with the travel document's chip,
2. implements the terminals part of PACE and/or BAC;
3. gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information.
4. implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [TR-03110-1] and
5. 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 Subjects related to Polymorphic eMRTD

6.2.2.1 Polymorphic Authentication Terminal/Service

A Polymorphic Authentication Terminal/Service used by the Polymorphic eMRTD document holder to perform (anonymous) polymorphic authentication process steps:

1. verifying the user as Polymorphic eMRTD document holder by verifying the user's PIN PACE password as part of the PACE protocol
2. examining a Polymorphic eMRTD document presented by the user and verifying its authenticity by Passive Authentication (PA) (signature verification of DG14 using SO_D)
3. Performing Chip Authentication (CAv1) and Terminal Authentication (TAv1)
4. checking the Polymorphic eMRTD document validity status by using the PP and meta data provided by the TOE during the execution of the Polymorphic Authentication protocol (PMA).

A Polymorphic Authentication Terminal/Service:

1. implements the terminal part of the PACEv2 with PIN, PA, CAv1 and TAv1 protocols configured in accordance with ICAO DOC9303 and TR-03110 v2.10 and the Polymorphic Authentication protocol (PMA).
2. performs the Advanced Inspection Procedure as a precondition to gain access to the randomized polymorphic user data (PI, PP and optional CPI) by executing the PMA protocol. The Polymorphic Authentication Terminal/Service must pass PACE with the correct user PIN and successful CAv1/TAv1 in order to be able to execute the PMA protocol successfully.
3. performs the Polymorphic Authentication protocol (PMA) to retrieve the randomized polymorphic user data (PI, PP and optional CPI) and the non-card unique identifiable meta data.

Application Note: This subject is an extension of the subject 'Personalisation Agent' defined in [PACE-PP].

6.2.2.2 Polymorphic Personalisation Agent

An organization acting on behalf of the Polymorphic eMRTD document issuer that personalises the Polymorphic eMRTD document for the Polymorphic eMRTD document holder. Personalisation includes some or all of the following activities:

1. Retrieve Polymorphic Identity (PI), Polymorphic Pseudonym (PP) and optionally the user's Complementary Polymorphic Identification data (CPI) from the central Key Management Authority of the Polymorphic Authentication Framework, based on the unique identifiable user identity attribute and optional other identification attributes that require privacy protection,
2. Storage of PI, PP and optional CPI data of the Polymorphic eMRTD document holder. Configuration of polymorphic eMRTD PIN, PUK and CAN as PACE passwords and into secure data authentication objects,
3. write document non-card unique identifiable meta data (i. e. document type, scheme version, issuer, etc.),
4. writing the initial TSF data and
5. sign the Document Security Object according to [ICAO-9303] and [TR-03110-3]) in the role of DS.

Note that the role personalisation agent may be distributed among several institutions according to the operational policy of the Polymorphic eMRTD document issuer.

Application Note: This subject is an extension of the subject 'Personalisation Agent' defined in [PACE-PP].

6.2.2.3 Polymorphic Country Verifying Certification Authority

The Country Verifying Certification Authority (CVCA) for the Polymorphic eMRTD authentication framework enforces the privacy policy of the issuing State or Organisation with respect to the protection of Polymorphic eMRTD data stored in the Polymorphic eMRTD document. The CVCA represents the country specific root of the PKI of Polymorphic Authentication Terminals/services 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 see TR-03110-3, v2.10 [TR-03110-3].

Application Note: This subject is an extension of the subject 'Country Verifying Certification Authority' defined in [EAC-PP-V2].

6.2.2.4 Polymorphic Document Verifier

An organization issuing terminal certificates. The DV is a Certificate Authority, authorized by the corresponding CVCA to issue certificates for Polymorphic Authentication terminals/services, see TR-03110-3, v2.10 [TR-03110-3]. The Document Verifier (DV) enforces the privacy policy of the Organisation with respect to the protection of Polymorphic eMRTD data to be handled by Polymorphic Authentication Terminals/services. The Document Verifier manages the authorization of the Polymorphic Authentication Terminals/services for the user data of the Polymorphic eMRTD in the limits provided by the issuing States or Organisations in the form of the Document Verifier Certificates.

Application Note: This subject is an extension of the subject 'Document Verifier' defined in [EAC-PP-V2].

6.2.2.5 Polymorphic Attacker

Additionally to the definition from PACE PP [PACE-PP] and EAC PP [EAC-PP-V2], the definition of an attacker is refined as followed: A threat agent trying (i) to manipulate the Polymorphic eMRTD document without authorization, (ii) to read sensitive Polymorphic eMRTD data (i.e. PP/PI/CPI and PIN/PUK), (iii) to forge a genuine Polymorphic eMRTD document, or (iv) to compromise the privacy of the Polymorphic eMRTD user Data (i.e.randomized PP/PI and optional CPI).

Application Note: This subject is an extension of the subject 'Attacker' defined in [EAC-PP-V2].

6.2.2.6 Polymorphic eMRTD Document Holder

A person for whom the Polymorphic eMRTD document Issuer has personalised the Polymorphic eMRTD document. Please note that a Polymorphic eMRTD document holder can also be an attacker.

Application Note: This subject is an extension of the subject 'Travel Document Holder' defined in [PACE-PP].

6.2.3 Subjects related to LDS2

6.2.3.1 LDS2 subjects Application Note 1:

CSCA issuing Document Signer certificates for the ICAO eMRTD application also issues certificates for LDS2 signers.
The CSCA issues certificates to LDS2 Signer for one or more of the LDS2 data types. The CSCA issues a single CRL that covers revocation notices for all types of certificates it issues including CSCA Certificates, Document Signers, Master List Signers, Deviation List Signers and LDS2 Signer Certificates.

6.2.3.2 LDS2 subjects Application Note 2:

Country Verifying CA (CVCA): Each issuing State or organization that allows LDS2 data to be added to its eMRTDs MUST set up a single CVCA. This CVCA is a Certification Authority (CA) that is the trust anchor for the authorization PKI of that State or organization and covers both access to DG3 and DG4 in the ICAO application and the user data in the LDS2 applications. The CVCA may be a stand-alone entity or it may be integrated with the CSCA of that same State or organization. However, even if co-located, the CVCA MUST use a different key pair than that of the CSCA. The CVCA determines the access rights that will be granted to all Document Verifiers (DV), foreign and domestic and issues certificates containing the individual authorizations to each of those DVs.

6.2.3.3 LDS2 subjects Application Note 3:

Terminal/Inspection System (IS): Within the context of the authorization PKI, a terminal is the entity that accesses the contactless IC of an eMRTD and writes a digitally signed LDS2 data object, or reads an LDS2 data object. The terminal MUST have an authorization certificate issued to it, from its local DV that grants the required authorization. The terminal is also referred to as an Inspection System. The inspection procedure designed for eMRTDs containing one or more LDS2 applications besides the eMRTD application ("LDS2-documents") is used see [LDS2_TR] Annex A2.
The inspection system for LDS and for LDS2 could be the same machine but the inspection system shall include the LDS2 characteristics described in [9303-10_LDS2] ,[LDS2_PKI] and [LDS2_TR]. In particular, at least one private key and the corresponding Terminal Certificate must be embedded in Terminal.

6.2.3.4 LDS2 subjects Application Note 4:

Document Verifier (DV): As defined in [EAC-PP-V2], the Document Verifier has also its role for LDS2 PKI. For LDS2, the DV issues IS certificates with extension: Certificate holder authorizations for each LDS2 application are encoded in CV-certificate extensions (one extension per application).The LDS2 DV now issues IS certificate that contain the authorization rights for accessing the LDS2 applications as defined in [9303-10_LDS2].

6.2.3.5 LDS2 Attacker

Additionally to the definition from PACE PP [PACE-PP] and EAC PP [EAC-PP-V2], the definition of an attacker is refined as followed:
A threat agent trying:
(i) to manipulate the LDS2 User Data (Visa, Stamps and additional biometric data) without authorization,
(ii) to read, delete, write or append LDS2 record data,

Application Note: This subject is an extension of the subject 'Attacker' defined in [EAC-PP-V2].

All primary assets represent User Data in the sense of the CC. The secondary assets represent TSF and TSF-data in the sense of the CC, see [PACE-PP]. The secondary assets also have to be protected by the TOE in order to achieve a sufficient protection of the primary assets.

6.3 Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the TOE method of use in the operational environment and the assets stored in or protected by the TOE. Threats to be averted by the TOE and its environment.

6.3.1 Threats listed in PP PACE

6.3.1.1 T.Skimming

Skimming travel document / Capturing Card-Terminal Communication
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 travel document data.

6.3.1.2 T.Eavesdropping

Eavesdropping on the communication between the TOE and the PACE terminal
Adverse action: An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE 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 travel document data.

6.3.1.3 T.Tracing

Tracing travel document
Adverse action: An attacker tries to gather TOE tracing data (i.e. to trace the movement of the travel 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 travel document holder.

6.3.1.4 T.Forgery

Forgery of Data
Adverse action: An attacker fraudulently alters the User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS-PACE or EIS-PACE by means of changed travel 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 travel document.

6.3.1.5 T.Abuse-Func

Abuse of Functionality
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 travel document holder.
Threat agent: having high attack potential, being in possession of one or more legitimate travel documents.

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

6.3.1.6 T.Information_Leakage

Information Leakage from travel document
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 travel document

6.3.1.7 T.Phys-Tamper

Physical Tampering
Adverse action: An attacker may perform physical probing of the travel 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 travel document in order to alter (i) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the travel document.
Threat agent: having high attack potential, being in possession of one or more legitimate travel documents.
Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document.

6.3.1.8 T.Malfunction

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

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

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

6.3.2 Additional Threats

6.3.2.1 T.Read_Sensitive_Data

Read the sensitive biometric reference data

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel 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 travel 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 travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.

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

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

6.3.2.2 T.Counterfeit

Counterfeit of travel document chip data

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

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

Asset: authenticity of user data stored on the TOE.

6.3.2.3 T. BAC_breaking

Adverse action: An attacker manages to break the BAC protocol using cryptanalysis means and powerful computation capacity leading to threaten (1) the non traceability and (2) confidentiality of data. The attacker is able to intercept and record a log of BAC transaction during inspection at a border control. Then using computation capacity, he is able to perform reverse engineering over the logs, to break the protocol within a few minutes or less and get (1) the MRZ value, and (2) the log of plain text exchanged between the MRTD and the inspection system. This leads the attacker to (1) get the holder information and use it, and (2) trace the holder in real time.
Threat agent: having high attack potential, being able to intercept transaction with MRTDs.
Asset: confidentiality of data read from the MRTD, traceability of the MRTD

6.3.3 Threats related to Polymorphic eMRTD

The table below provides a mapping giving the Threats related to the polymorphic eMRTD and Threats from PACE PP [PACE-PP] and EAC PP [EAC-PP-V2]:

Threats related to the polymorphic eMRTD	Threats from PACE PP	Threats from EAC PP
T.Sensitive_Polymorphic_Data	T.Skimming	T.Read_Sensitive_Data
T.Forgery_Polymorphic	T.Forgery	
T.Eavesdropping_Polymorphic	T.Eavesdropping	
T.Compromise_Privacy_Poly		

6.3.3.1 T.Sensitive_Polymorphic_Data

Read the sensitive Polymorphic eMRTD data

Adverse action: An attacker tries to gain the sensitive Polymorphic eMRTD data stored on the TOE through the communication interface of the Polymorphic eMRTD document's chip.

Threat agent: Attacker with attack potential high

Asset: confidentiality of polymorphic sensitive user data stored on the TOE (i.e. PI/PP/CPI data and PIN/PUK)

Application Note: This Threat is an extension of the Threat 'T.Read_Sensitive_Data' defined in [EAC-PP-V2] and the threat T.Skimming from [PACE-PP].

6.3.3.2 T.Forgery_Polymorphic

Forgery of Polymorphic Data

Adverse action: An attacker fraudulently alters the PI/PP/CPI and/or PIN/PUK data stored on the Polymorphic eMRTD document.

Threat agent: having high attack potential

Asset: Integrity of Sensitive polymorphic User Data stored on the TOE (i.e. PI/PP/CPI data and PIN/PUK).

Application Note: T.Forgery from [PACE-PP] is extended here to Polymorphic Authentication Terminal/Service target that is outsmarted by the attacker.

6.3.3.3 T.Compromise_Privacy_Poly

Compromise Polymorphic eMRTD document Holder privacy

Adverse action: A non-authorized person with high-privileges over the system or application (administrator) could try to access the randomized PI, PP and optional CPI data of the Polymorphic

eMRTD document Holder in order to link and trace the Holder sessions or the identification during the Polymorphic Authentication.

An external attacker could try to access the randomized PI, PP and optional CPI data of the Polymorphic eMRTD document Holder in order to link and trace the Holder sessions or the identification during the Polymorphic Authentication.

Threat agent: Attacker with attack potential high

Asset: confidentiality, authenticity and privacy of the Polymorphic eMRTD user Data (randomized PI, PP and optional CPI).

Application Note: This Threat has been added to this ST for attacks on the confidentiality and privacy of randomized PI, PP and optional CPI data during the Polymorphic Authentication. This addition does not conflict with the strict conformance to PACE PP [PACE-PP] and EAC PP [EAC-PP-V2].

6.3.3.4 T.Eavesdropping_Polymorphic

Eavesdropping on the communication between the TOE and the Polymorphic terminal/Authentication Service

Adverse action: An attacker is listening to the communication between the polymorphic eMRTD document and the Polymorphic terminal/Authentication Service connected in order to gain the *user data transferred between the TOE and the terminal (randomized PI, PP and optional CPI)*.

Threat agent: having high attack potential

Asset: Privacy and confidentiality of eMRTD polymorphic user data (randomized PI, PP and optional CPI)

Application Note: T.Eavesdropping from the PACE PP [PACE-PP] is extended here by the Polymorphic terminal/Authentication Service.

6.3.4 Additional threats related to LDS2

The LDS2 extends the LDS file systems and keep the same LDS threats for the LDS2 assets. . The same policy for condentiality, integrity and authenticity is required.

6.3.4.1 T.Read_LDS2_Sensitive_Data

Read the sensitive reference data of LDS2 additional applications

Adverse action: An attacker tries to gain the sensitive Entry/Exit data (Travel Record Application), Visa data and Additional Biometric reference data through the communication interface of the travel document's chip.

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

Asset: confidentiality of logical travel document sensitive user data (i.e. Entry/Exit data (Travel Record Application), Visa data and Additional Biometric reference)

Application Note: This Threat is an extension of the Threat 'T.Read_Sensitive_Data' defined in [EAC-PP-V2] and the threat T.Skimming from [PACE-PP].

6.3.4.2 T.Forgery_LDS2_Sensitive_Data

Forgery of LDS2 Data

Adverse action: An attacker fraudulently alters the reference data of LDS2 sensitive applications.

Threat agent: having high attack potential

Asset: Integrity and authenticity of logical travel document sensitive user data (i.e. Entry/Exit data (Travel Record Application), Visa data and Additional Biometric reference)

6.4 Organisational Security Policies

The TOE shall comply to the following organization security policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1 [CC-1], sec. 3.2).

6.4.1 OSP listed in PP PACE

6.4.1.1 P.Manufact

Manufacturing of the travel document's chip

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

6.4.1.2 P.Pre-Operational

Pre-operational handling of the travel document

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

6.4.1.3 P.Card_PKI

PKI for Passive Authentication (issuing branch)

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

6.4.1.4 P.Trustworthy_PKI

Trustworthiness of 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 travel document.

6.4.1.5 P.Terminal

Abilities and trustworthiness of terminals
The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:

1. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [ICAO-9303].
2. They shall implement the terminal parts of the PACE protocol [ICAO-9303] part 11, of the Passive Authentication [ICAO-9303] and use them in this order. 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 travel 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 the PP [PACE-PP].

6.4.2 Additional OSPs from PP EAC

6.4.2.1 P.Sensitive_Data

Privacy of sensitive biometric reference data
The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organization 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 travel 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.

6.4.2.2 P.Personalisation

Personalisation of the travel document by issuing State or Organisation only
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 travel document with respect to the travel document holder. The personalisation of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.

6.4.3 OSPs related to Polymorphic eMRTD

The table below provides a mapping giving the OSPs related to the polymorphic eMRTD and OSPs from PACE PP [PACE-PP] and EAC PP [EAC-PP-V2]:

OSPs related to the polymorphic eMRTD	OSPs from PACE PP	OSPs from EAC PP
P.Polymorphic_Data		P.Sensitive_Data
P.Polymorphic_Authentication_Terminal	P.Terminal	
P.Pre-Operational_Polymorphic	P.Pre-Operational	
P.Personalisation_Polymorphic		P.Personalisation

6.4.3.1 P.Polymorphic_Data

Polymorphic eMRTD User data

The polymorphic randomized PI, PP and optional CPI data are ElGamal encrypted private personal identication attributes of the polymorphic eMRTD document holder. Encryption is performed by central Key Management Authority by using its system public keys. The Polymorphic eMRTD User data can only be read by Authentication Service(s)/Terminal(s), which are authorized for this access at the time the polymorphic eMRTD document is presented to the Authentication Service/Terminal. The polymorphic eMRTD document's chip shall protect the confidentiality, privacy, authenticity and integrity of the Polymorphic eMRTD User data (PI, PP and/or CPI) during transmission to the Polymorphic Authentication Service/Terminal after successful PACE (with PIN), CAv1, TAv1 and Polymorphic (PMA) authentication.
Nobody is able to read/change/delete the sensitive polymorphic PI, PP and CPI data stored inside the chip.

Application Note: This OSP is an extension of the OSP 'P.Sensitive_Data' defined in [EAC-PP-V2].

6.4.3.2 P.Polymorphic_Authentication_Terminal

Terminals/Services that intend to be Polymorphic Authentication Terminals/Services must implement the respective terminal part of the protocols required to execute PACE with PIN, PA, CAv1 and TAv1 authentications according to [TR-03110] and the Polymorphic Authentication protocol (PMA). Authentication terminals store static private keys and card verifiable IS certificates for TAv1 and CVCA and CSCA cerificates and generate ephemeral keys and nonces to support all required above mentioned protocols (PACE, PA, CAv1, TAv1 and PMA).

Application Note: P.Terminal from [PACE-PP] is extended here to Polymorphic Authentication Terminal/Service target.

6.4.3.3 P.Pre-Operational_Polymorphic

Pre-operational handling of the polymorphic eMRTD document

1) The polymorphic eMRTD document Issuer issues the polymorphic eMRTD document and approves it using the terminals and authentication services complying with all applicable laws and regulations.
2) The polymorphic eMRTD document Issuer guarantees correctness of the PI/PP/CPI data stored in the TOE.
3) The polymorphic eMRTD document Issuer uses only such TOE's technical components (IC) which enable traceability of the polymorphic eMRTD documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase.
4) If the polymorphic eMRTD document Issuer authorises a Personalisation Agent to personalise the polymorphic eMRTD document for polymorphic eMRTD document holders, the polymorphic eMRTD document Issuer has to ensure that the Personalisation Agent acts in accordance with the polymorphic eMRTD document Issuer's policy.
5) The Polymorphic eMRTD document issuer shall ensure that the PP/PI/CPI data are generated and stored securely in the Polymorphic eMRTD document.
6) The Polymorphic eMRTD document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication v1. For this aim, the Polymorphic eMRTD document issuer shall run a Country Verifying Certification Authority. The PKI shall fulfill the requirements and rules of the corresponding certificate policy. The Polymorphic eMRTD document issuer shall make the CVCA certificate available to the personalisation agent or the manufacturer.

Application Note: This OSP is an extension of the OSP 'P.Pre-Operational' defined in [PACE-PP].

6.4.3.4 P.Personalisation_Polymorphic

Personalisation of the polymorphic eMRTD document by issuing State or Organisation only

The issuing State or Organisation guarantees the correctness of the PI/PP/CPI data of the polymorphic eMRTD document with respect to the polymorphic eMRTD document holder. The personalisation of the polymorphic eMRTD document for the holder is performed by an agent authorized by the issuing State or Organisation only. The Polymorphic Personalisation Agent guarantees privacy, integrity, confidentiality and authenticity of the PI/PP/CPI data during the personalisation phase (loading of PI/PP/CPI data in the Polymorphic eMRTD document).

Application Note: This OSP is an extension of the OSP 'P.Personalisation' defined in [EAC-PP-V2].

6.4.4 Additional OSPs related to LDS2 ePassport

Organisational Security Policies for LDS2 extension are added to previous OSPs.

6.4.4.1 P.LDS2_Card_PKI

PKI for LDS2 extension

The LDS2 authorization PKI consists of the following entities:

- Country Verifying CAs (CVCAs)
- Document Verifiers (DVs)
- Terminals
- Single Point of Contact (SPOC)

Distribution and management of the authorization certificates between CVCAs in one State and DVs in other States is handled through a Single Point of Contact (SPOC) in each State.

The LDS2 digital signature PKI is specified as a set of enhancements to the X.509-based PKI used in LDS for Passive Authentication. The same CSCA that is used for LDS is also used for LDS2. The LDS CSCA issues LDS2 Signer Certificates.

LDS2 Signer certificates MUST comply with the certificate profiles. The LDS2 Digital Signature PKI consists of the following entities:
- Country Signing CA (CSCA),
- LDS2 Signers,

The LDS2 authorization PKI uses a different certificate structure (ISO 7816 card verifiable certificates) and therefore requires additional infrastructure components. The authorization PKI enables an eMRTD Issuing State or organization to authorize:
- the writing of LDS2 data objects to the contactless IC of their eMRTDs after issuance,
- read access to LDS2 data objects.

These read/write authorizations MAY be granted to foreign States at the discretion of the Issuing State or organization. Each Roles, Responsabilities, distribution and management of the authorization certificates for LDS2 PKI must be defined following [LDS2_PKI]. Distribution and management of the authorization certificates between CVCAs in one State and DVs in other States is handled through a Single Point of Contact (SPOC) in each State.

Each State that participates in the LDS2 authorization PKI must set up a single SPOC. This SPOC is the interface that is used for all communication between the CVCA of one State with the DVs in another State. Certificate requests and responses are communicated between the SPOCs of each State using the SPOC protocol.

Application Note: This OSP is an extension of the OSP 'P.Card_PKI' defined in [EAC-PP-V2].

6.4.4.2 P.LDS2_Personalisation

Personalisation of the travel document by issuing State or Organisation only
The issuing State or Organisation guarantees the correctness of the Travel Records data, Visa Records data, Additional Biometric data, the authenticity token (Signature) and other data of the logical travel document with respect to the travel document holder.
Issuer should pre-create a number of Additional Biometrics EFs. These EFs can be selected, written, updated and read with appropriate authorizations. At the end of personalisation, the last command of sequence permanently disable writing into the Additional Biometrics Elementary File.

The personalisation of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.

Application Note: Note that in operational phase, the issuing State or Organisation still guarantees the correctness and authenticity of the LDS2 Travel Records data, Visa Records data and Additional Biometric data provided to the LDS2 Terminals/Inspection systems acting on his behalf. Indeed, to read LSD2 or write LDS2 data the Terminal should have the dedicated authorization: see P.LDS2_Card_PKI and signing LDS2 objects.

6.4.4.3 P.LDS2_Sensitive_Data

Privacy of sensitive Travel, Visas and Additional Biometric reference data
The Entry/Exit data (Travel Record Application), Visa data and Additional Biometric reference data are sensitive private personal data of the travel document holder. The reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organization 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 travel 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.

Application Note: This OSP is an extension of the OSP 'P.Sensitive_Data' defined in [EAC-PP-V2].

6.5 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

6.5.1 Assumptions listed in PP PACE

6.5.1.1 A.Passive_Auth

PKI for Passive Authentication

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 travel 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 travel 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].

6.5.2 Assumptions listed in PP EAC

6.5.2.1 A.Insp_Sys

Inspection Systems for global interoperability

The Extended Inspection System (EIS) for global interoperability includes the Country Signing CA Public Key and implements the terminal part of PACE [ICAO-9303] part 11 and/or BAC [BAC-PP]. 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 travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 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.

6.5.2.2 A.Auth_PKI

PKI for Inspection Systems

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 travel document's chip.

6.5.3 Assumptions related to Active Authentication

6.5.3.1 A.Pers_Agent_AA

Personalisation of the MRTD's chip (Active Authentication)
The Personalisation Agent ensures the correctness of the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip.

6.5.4 Assumptions related to Polymorphic eMRTD

The table below provides a mapping giving the Assumptions related to the polymorphic eMRTD and Assumptions from PACE PP [PACE-PP] and EAC PP [EAC-PP-V2]:

As related to the polymorphic eMRTD	As from PACE PP	As from EAC PP
A.Auth_PKI_Polymorphic		A.Auth_PKI
A.Insp_Sys_Polymorphic		A.Insp_Sys
A.Polymorphic_Auth		

6.5.4.1 A.Polymorphic_Auth

It assumed that:

- All authentication infrastructure keys used by the central Key Management Authority for the polymorphic authentication infrastructure (generation and transformation of PP, PI and CPI) are generated, handled and stored securely.
- The PP/PI/CPI are generated securely by the central Key Management Authority of the polymorphic authentication infrastructure and stored securely in the eMRTD polymorphic chip during the personalisation phase.
- The TOE communicates only with Trustworthy Authentication Service/Terminal during the Polymorphic Authentication.
- The randomised PP, PI and CPI are securely received by Polymorphic Authentication Service/Terminal. The randomised PP, PI and CPI are transformed ("re-keyed") by the central Key Management Authority (i.e. ElGamal re-encryption of the randomized PP, PI and/or CPI using the public key of Service Provider, who is authorized to read the plain value of identifying user attributes included in the PP, PI or CPI). Identification by the identifying user attributes contained inside the PP, PI and CPI takes place at the Service Provider.

Application Note: This Assumption has been added to this ST for the polymorphic authentication infrastructure. This addition does not conflict with the strict conformance to PACE PP [PACE-PP] and EAC PP [EAC-PP-V2].

6.5.4.2 A.Auth_PKI_Polymorphic

PKI for Polymorphic eMRTD
It is assumed that:

- The issuing States or Organisations establish a dedicated CVCA, DVCA and IS PKI for the polymorphic eMRTD infrastructure.
- 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 for access to the PP, PI and (optional) CPI polymorphic user data. 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 Polymorphic Authentication Terminal/Service of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their Polymorphic eMRTD document's chip.
- The issuing State or Organisation establishs the necessary public key infrastructure in order to limit the access to Polymorphic data of Polymorphic eMRTD document holders to authorized Organisations. The Country Verifying Certification Authority of the issuing State or Organisation generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.
- The issuing State or Organisation establishs the necessary public key infrastructure in order to (i) generate the Polymorphic eMRTD document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data and (iii) support Polymorphic Authentication Terminals/Services to verify the authenticity of the Polymorphic eMRTD document's chip according to [TR-03110] used for genuine Polymorphic eMRTD document by certification of the Chip Authentication Public Key by means of the Document Security Object.
- The Polymorphic eMRTD document issuer establishes a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the Polymorphic eMRTD document issuer shall run a Country Verifying Certification Authority. The PKI shall fulfill the requirements and rules of the corresponding certificate policy. The Polymorphic eMRTD document issuer shall make the CVCA certificate available to the personalisation agent or the manufacturer.
- The polymorphic eMRTD document Issuer issues the polymorphic eMRTD document and approves it using the terminals and authentication services complying with all applicable laws and regulations.

Application Note: This Assumption is an extension of the Assumption 'A.Auth_PKI' defined in [EAC-PP-V2]. 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.

6.5.4.3 A.Insp_Sys_Polymorphic

Polymorphic Inspection Systems and authentication services

- Polymorphic Inspection Systems (Polymorphic Authentication Terminals/Services) ensure the confidentiality, Privacy, Authenticity and integrity of the polymorphic data read from the polymorphic eMRTD document (e.g. PACE PIN/PUK, integrity of PKI certificates, randomized PI, PP and optional CPI data, etc.), where it is necessary for a secure operation of the TOE.
- Polymorphic Inspection Systems will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.
- Polymorphic Inspection Systems examine the polymorphic eMRTD document presented by the polymorphic eMRTD document holder to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the polymorphic eMRTD document.
- Polymorphic Inspection Systems include the Country Signing CA Public Key and implement the respective terminal part of the protocols required to execute PACE with PIN, Passive

Authentication (PA), CAv1, TAv1 authentication according to [TR-03110-2] and Polymorphic Authentication (PMA). They are assumed to securely store static IS private keys and generate secure temporary session keys and nonces.

- The Document Verifier authorizes Polymorphic Inspection Systems by creation of Inspection System Certificates for access to polymorphic user data stored the polymorphic eMRTD document. An Polymorphic Inspection Systems authenticates itselve to the polymorphic eMRTD document's chip for getting access to the polymorphic data with its private Terminal Authentication key and corresponding Inspection System Certificate.

Application Note: This Assumption is an extension of the Assumption 'A.Insp_Sys' defined in [EAC-PP-V2]. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the PACE with PIN, CAv1 and TAv1 authentication.

6.5.5 Assumptions related to LDS2

The Assumptions previously defined are applicable for LDS2 extension and are completed by the following ones:

6.5.5.1 **A. Insp_Sys_LDS2**

For Inspection Systems for multi-application eMRTDs with LDS2 it is assumed that:

- LDS2 requires the terminal to perform PACE, CAv1 and TAv1 to be performed prior to the selection of the LDS2 applications present on the eMRTD.
- LDS2 requires the terminal to prove to the eMRTD contact or contactless IC that it is entitled to write or read LDS2 data objects into/from the LDS2 applications on the IC during TAv1.
- The LDS2 enabled terminal is equipped with at least one TAv1 private key and the corresponding Terminal Certificate, encoding the terminal's public key and LDS2 application specific access rights. After the terminal has proven knowledge of this private key, the eMRTD chip grants the terminal access to read or write LDS2 data as indicated in the Terminal Certificate.
- Data written after issuance of the eMRTD are not protected by the Document Security Object, which is signed by the issuer of the document. To verify the authenticity of LDS2 data written after issuance, the following steps will be performed by the LDS2 inspection system for each retrieved LDS2 data object:
    1. The Inspection System shall start Passive authentication with inspection process dedicated to LDS2 and for LDS2 data written after issuance of the eMRTD: see authentication of data in [LDS2_TR]

Application Note: This Assumption is an extension of the Assumption 'A.Insp_Sys' defined in [EAC-PP-V2]. 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 and Reading/writing data includes selection of the applications containing the files or records.

7 Security Objectives

7.1 Security Objectives for the TOE

7.1.1 Security Objectives listed in PP PACE

7.1.1.1 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 BIS-PACE) after the PACE Authentication.

7.1.1.2 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 BIS-PACE) 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).

7.1.1.3 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 BIS-PACE 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 BIS-PACE) after the PACE Authentication.

7.1.1.4 OT.Tracing

Tracing travel document
The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel 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 travel document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of travel 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.

7.1.1.5 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.

7.1.1.6 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 travel document

1. 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,
2. by forcing a malfunction of the TOE and/or
3. 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.

7.1.1.7 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 travel document's Embedded Software by means of

1. 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
2. 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),
3. manipulation of the hardware and its security functionality, as well as
4. controlled manipulation of memory contents (User Data, TSF-data) with a prior
5. reverse-engineering to understand the design and its properties and functionality.

7.1.1.8 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.

7.1.1.9 OT.Identification

Identification 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 travel document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

7.1.1.10 OT.AC_Pers

Personalisation of the Electronic Document
The TOE must ensure that the logical travel 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 travel 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 travel document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.

7.1.2 Additional Security Objectives from PP EAC

7.1.2.1 OT.Sens_Data_Conf

Confidentiality of sensitive biometric reference data

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 travel 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.

7.1.2.2 OT.Chip_Auth_Proof

Proof of the travel document's chip authenticity

The TOE must support the Inspection Systems to verify the identity and authenticity of the travel 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]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

Application Note: The OT.Chip_Auth_Proof implies the travel document's chip to have (i) a unique identity as given by the travel document's Document 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 travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [ICAO-9303] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

7.1.3 Security Objectives related to Polymorphic eMRTD

The table below provides a mapping giving the OTs related to the polymorphic eMRTD and OTs from PACE PP [PACE-PP] and EAC PP [EAC-PP-V2]:

OTs related to the polymorphic eMRTD	OTs from PACE PP	OTs from EAC PP
OT.Polymorphic_Data_Confidentiality	OT.Data_Confidentiality	OT.Sens_Data_Conf
OT.Polymorphic_Data_Integrity	OT.Data_Integrity	
OT.Polymorphic_Data_Authenticity	OT.Data_Authenticity	
OT.AC_Pers_Polymorphic	OT.AC_Pers	
OT.Polymorphic_Data_Privacy		

7.1.3.1 OT.Polymorphic_Data_Confidentiality

Confidentiality of eMRTD polymorphic data

The TOE must ensure the confidentiality of the sensitive static polymorphic eMRTD PI, PP and CPI user data stored on the TOE during personalisation by denying all read access to everybody. Only read access to the randomized representation of the polymorphic user data is possible and only granted to authorized and authenticated Polymorphic Authentication Terminals/Services.

The TOE must ensure the confidentiality of the eMRTD polymorphic User Data (randomized PI, PP and optional CPI) during their exchange between the TOE and the Polymorphic Authentication terminal/Service connected after successfully executing the sequence of PACE with PIN, PA, CAv1, TAv1 and PMA authentication.

Application Note: This OT is an extension of the OTs 'OT.Sens_Data_Conf' and 'OT.Data_Confidentiality' defined in [PACE-PP] and [EAC-PP-V2] respectively to ensure the confidentiality of the sensitive polymorphic eMRTD PI/PP/CPI data stored on the TOE and the randomized PI, PP and optional CPI exchanged with the connected Polymorphic Authentication Terminal/Service. This extension does not conflict with the strict conformance to PACE PP and EAC PP.

7.1.3.2 OT.Polymorphic_Data_Integrity

Integrity of eMRTD polymorphic data

The TOE must ensure the Integrity of the sensitive polymorphic eMRTD PI, PP and CPI data and PIN/PUK data stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying).

Application Note: This OT is an extension of the OT 'OT.Data_Integrity' defined in [PACE-PP] to ensure the integrity of the polymorphic eMRTD user data. This extension does not conflict with the strict conformance to PACE PP and EAC PP.

7.1.3.3 OT.Polymorphic_Data_Authenticity

Authenticity of eMRTD polymorphic data

The TOE must ensure the authenticity of the polymorphic eMRTD randomized PI, PP and optional CPI data during their exchange between the TOE and Terminal/Authentication Service connected after successfully executing the sequence of PACE with PIN, CAv1, TAv1 and PMA.

Application Note: This OT is an extension of the OT 'OT.Data_Authenticity' defined in [PACE-PP] to ensure the authenticity of the polymorphic eMRTD PI/PP/CPI data. This extension does not conflict with the strict conformance to PACE PP and EAC PP.

7.1.3.4 OT.Polymorphic_Data_Privacy

Privacy of eMRTD polymorphic user data

The TOE guarantees the privacy of the PI, PP and optional CPI user data by randomising the PI, PP and optional CPI user data during the polymorphic authentication (PMA), prior to returning it to the authorised Polymorphic Authentication Terminal/Service. This prevents the Authenication Service from being able to harvest any user or card unique identifiable data.

Application Note: This OT has been added to this ST to ensure and maintain the privacy of the polymorphic PI, PP and optional CPI user data during the Polymorphic Authentication (sequence of PACE with PIN, CAv1, TAv1 and PMA). This addition does not conflict with the strict conformance to PACE PP and EAC PP.

7.1.3.5 OT.AC_Pers_Polymorphic

Access Control for Personalisation of Polymorphic eMRTD document

The TOE must ensure that the Polymorphic eMRTD data PI/PP/CPI and PIN/PUK can be written by authorized Personalisation Agents only. The Polymorphic eMRTD PI/PP/CPI data must be written only during and cannot be changed after personalisation of the document.

Application Note: This OT is an extension of the OT 'OT.AC_Pers' defined in [PACE-PP] to ensure that the polymorphic eMRTD data PI/PP/CPI and PIN/PUK are written by authorized Personalisation Agents only. This extension does not conflict with the strict conformance to PACE PP and EAC PP.

7.1.4 Additional Security Objectives related to LDS2 extension

The table below provides a mapping giving the OTs related to the LDS2 extension and OTs from PACE PP [PACE-PP] and EAC PP [EAC-PP-V2]:

OTs related to the LDS2 eMRTD	OTs from PACE PP	OTs from EAC PP
OT.LDS2_Data_Confidentiality	OT.Data_Confidentiality	OT.Sens_Data_Conf
OT.AC_Pers_LDS2	OT.AC_Pers	

7.1.4.1 OT.LDS2_Data_Confidentiality

Confidentiality of multi application LDS2 user data

The TOE must ensure the confidentiality of the sensitive Entry/Exit data (Travel Record Application), Visa data and Additional Biometric reference data 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 travel document data during their transmission to the LDS2 Inspection System. The confidentiality of the sensitive LDS2 applications data (Entry/Exit data, Visa data and Additional Biometric data) shall be protected against attacks with high attack potential.

Application Note: This OT is an extension of the OTs 'OT.Sens_Data_Conf' and 'OT.Data_Confidentiality' defined in [PACE-PP] and [EAC-PP-V2] respectively to ensure the confidentiality of the sensitive LDS2 eMRTD PI/PP/CPI data stored on the TOE and data exchanged with the connected LDS2 Authentication Terminal/Service. This extension does not conflict with the strict conformance to PACE PP and EAC PP.

7.1.4.2 OT.AC_Pers_LDS2

Access Control for Personalisation of LDS2 eMRTD document

The TOE must ensure that the logical travel document data for additional applications in Elementary files of DF: Travel Records Application, Visa Records
Application Additional Biometrics Application according [9303-10_LDS2], the Document Security Object according to LDS [ICAO-9303] and the TSF data can be written by authorized Personalisation Agents only. The logical travel document data and the TSF data may be written only during and cannot be changed after personalisation of the document.
After personalisation Travel records, Visa Records can only be appended in their corresponding elementary files and Additional Biometrics Records can be written inside their dedicated EF.
For access to applications other than the ICAO eMRTD application (such as LDS2 applications), only the PACE protocol is allowed (not BAC) with CAv1-TAv1 authentication sequence.

Application Note: This OT is an extension of the OT 'OT.AC_Pers' defined in [PACE-PP] to ensure that

- Pre-issuance, at the step of personalisation, LDS2 applications and elementary files can be created and LDS2 data can be written by authorized Personalisation Agents only during personalisation and
- Post-issuance, LDS2 records can be appended by authorised LDS2 Inspection Systems/Terminals only.

This extension does not conflict with the strict conformance to PACE PP and EAC PP.

7.1.5 Additional Security Objectives for the TOE

7.1.5.1 OT.Chip_Auth_Proof_PACE_CAM

The TOE must support the terminals to verify the identity and authenticity of the electronic document's chip as issued by the identified issuing State or Organization by means of the PACE-Chip Authentication Mapping (PACE-CAM) as defined in [ICAO-9303]. The authenticity proof provided by electronic document's chip shall be protected against attacks with high attack potential.

7.1.5.2 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.

7.1.5.3 OT.BAC_Expiration

Automatic deactivation of BAC protocol

7.1.5.4 OT.DBI

The TOE shall support Digital Blurring of Images. The feature may be used to restrict the access to the plain image data of particular EF(s). Enabling the feature will cause the image data to be corrupted during the reading of the file contents until the blurring is removed by an authorized terminal.

7.2 Security Objectives for the Operational Environment

7.2.1 Issuing State or Organisation

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

7.2.1.1 OE.Legislative_Compliance

Issuing of the travel document

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

7.2.1.2 OE.Auth_Key_Travel_Document

Travel document Authentication Key

The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the travel 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 travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

7.2.1.3 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 travel 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.

7.2.2 Travel document Issuer and CVCA: travel document's PKI (issuing) branch

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

7.2.2.1 OE.Passive_Auth_Sign

Authentication of travel document by Signature
The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must

1. generate a cryptographically secure CSCA Key Pair,
2. ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and
3. 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

1. generate a cryptographically secure Document Signing Key Pair,
2. ensure the secrecy of the Document Signer Private Key,
3. hand over the Document Signer Public Key to the CSCA for certification,
4. sign Document Security Objects of genuine travel 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 travel document.

7.2.2.2 OE.Personalisation

Personalisation of travel document
The travel document Issuer must ensure that the Personalisation Agents acting on his behalf

1. establish the correct identity of the travel document holder and create the biographical data for the travel document,
2. enroll the biometric reference data of the travel document holder,
3. write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO-9303],
4. write the document details data,
5. write the initial TSF data,
6. sign the Document Security Object defined in [ICAO-9303] (in the role of a DS).

7.2.3 Terminal operator: Terminal's receiving branch

7.2.3.1 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 travel document holders as defined in [ICAO-9303].
2. The related terminals implement the terminal parts of the PACE protocol [ICAO_TR_SAC], of the Passive Authentication [ICAO_TR_SAC] (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 travel document (determination of the authenticity of data groups stored in the travel 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].

7.2.4 Travel document holder Obligations

7.2.4.1 OE.Travel_Document_Holder

Travel document holder Obligations
The travel 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.

7.2.5 Receiving State or Organisation

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

7.2.5.1 OE.Exam_Travel_Document

Examination of the physical part of the travel document
The inspection system of the receiving State or Organisation must examine the travel document presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel 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_TR_SAC] 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 travel document's chip.

7.2.5.2 OE.AA_MRTD

Active Authentication - Inspection Systems

An Active Authentication (Basic, General or Extended) Inspection system performs all the functions of the Basic, General and Extended Inspection System, and verifies the IC authenticity with an RSA or ECDSA signature generated by the MRTD (if available).

7.2.5.3 OE.Auth_Key_MRTD

MRTD Authentication Key

The issuing State or Organization has to establish the necessary public key infra-structure in order to (i) generate the MRTD's Active Authentication Key Pair, (ii) sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 (if generated) and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object.

7.2.5.4 OE.Prot_Logical_Travel_Document

Protection of data from the logical travel document
The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical travel 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.

7.2.5.5 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 travel document. The Extended Inspection System authenticates themselves to the travel document's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

7.2.6 OEs related to Polymorphic eMRTD

The table below provides a mapping giving the OEs related to the polymorphic eMRTD and OEs from PACE PP [PACE-PP] and EAC PP [EAC-PP-V2]:

OEs related to the polymorphic eMRTD	OEs from PACE PP	OEs from EAC PP
OE.Insp_Sys_Polymorphic	OE.Terminal	OE.Prot_Logical_Travel_Document, OE.Exam_Travel_Document, OE.Ext_Insp_Systems
OE.Authoriz_Polymorphic_Data	OE.Legislative_Compliance	OE.Authoriz_Sens_Data, OE.Auth_Key_Travel_Document
OE.Personalisation_Polymorphic	OE.Personalisation	OE.Authoriz_Sens_Data, OE.Auth_Key_Travel_Document
OE.Polymorphic_Auth		

OE.Polymorphic_Auth

- All authentication infrastructure keys used by the central Key Management Authority for the polymorphic authentication infrastructure (generation and transformation of PP, PI and CPI) are generated, handled and stored securely.
- The Issuer has to ensure that Polymorphic PP/PI/CPI user data is generated securely by the central Key Management Authority of the polymorphic authentication infrastructure and stored securely in the electronic document during the eMRTD personalisation phase.
- The TOE communicates only with a Trustworthy Authentication Service/Terminal during the Polymorphic eMRTD authentication process steps (i.e. during sequence of PACE with PIN, PA, CAv1, TAv1 and PMA).
- The authorized Polymorphic Authentication Service/Terminal has to ensure that the randomised PP, PI and optional CPI are securely received and transformed by the central Key Management Authority. This comprises:
- eMRTD document authentication by performing Passive Authentication (SOD and DG14) signature verification and Chip Authentication (CAv1), being part of the Polymorphic Authentication process steps (i.e. sequence of PACE with PIN, PA, CAv1, TAv1 and PMA).
- eMRTD document status validation by encryption of the randomized PP received from the TOE using the public key of the eMRTD document Status Service and sending this with the the coresponding meta-data obtained from the TOE to the eMRTD document Status Service.
- Transformation (re-keying): encryption of the randomized PP, PIP or CPI received from the TOE using the public key of the destination Service Provider.
- Transmiting the transformed (encrypted) PP, PIP or CPI to the destination Service provider.

Application Note: This OE has been added to this ST for the polymorphic authentication infrastructure. This addition does not conflict with the strict conformance to PACE PP [PACE-PP] and EAC PP [EAC-PP-V2].

7.2.6.1 OE.Authoriz_Polymorphic_Data

Authorization for Use of Polymorphic eMRTD User Data

- The issuing States or Organisations have to establish a dedicated (separated) CVCA, DVCA and IS PKI in the polymorphic eMRTD infrastructure.
- The Country Verifying Certification Authorities, the Document Verifier and Inspection Systems have to 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 have to sign the certificates of the Document Verifier and the Document Verifiers have to sign the certificates of the Inspection Systems. The issuing States or Organisations have to distribute the public keys of their Country Verifying Certification Authority to their Polymorphic eMRTD document's chip.
- The issuing State or Organisation have to establish the necessary public key infrastructure in order to limit the access to Polymorphic data of Polymorphic eMRTD document holders to authorized Organisations. The Country Verifying Certification Authority of the issuing State or Organisation has to generate card verifiable Document Verifier Certificates for the authorized Document Verifier only.
- The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the Polymorphic eMRTD document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data and (iii) support inspection systems to verify the authenticity of the Polymorphic eMRTD document's chip according to [TR-03110] and [ICAO-9303] used for genuine Polymorphic eMRTD document by certification of the Chip Authentication Public Key by means of the Document Security Object (SOD).
- The Polymorphic eMRTD document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the Polymorphic eMRTD document issuer shall run a Country Verifying Certification Authority. The PKI shall fulfill the requirements and rules of the corresponding certificate policy. The Polymorphic eMRTD document issuer shall make the CVCA certificate available to the personalisation agent or the manufacturer.
- The polymorphic eMRTD document Issuer must issue the polymorphic eMRTD document and approves it using the terminals and authentication services complying with all applicable laws and regulations.

Application Note: This OE is an extension of the OEs 'OE.Legislative_Compliance' from [PACE-PP] and 'OE.Auth_Key_Travel_Document', 'OE.Authoriz_Sens_Data' defined in [EAC-PP-V2].

7.2.6.2 OE.Insp_Sys_Polymorphic

Polymorphic Inspection Systems and authentication services

- Polymorphic inspection systems (Terminals) or authentication services must ensure the confidentiality, privacy, authenticity and integrity of the user cerdentials (PIN, PUK, CAN) and the polymorphic data read from the polymorphic eMRTD document (integrity of trusted certificate store with PKI CSCA and CVCA, DVCA certificates, randomized PI, PP and optional CPI polymorphic user data, etc.), where it is necessary for a secure operation of the TOE.
- The inspection system (Terminal/Authentication service) must prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.
- Inspection Systems that intend to be Polymorphic Authentication Terminals/Services must include the Country Signing CA Public Key and must implement the respective terminal part of the protocols required to execute the Passive Authentication, PACE with PIN, CAv1 and TAv1 according to [TR-03110] and the Polymorphic Authentication protocol (PMA), and store (static keys) or generate (temporary keys and nonces) the corresponding credentials.
- The Document Verifier must authorize Polymorphic Inspection Systems by creation of Inspection System Certificates for access to polymorphic data of the polymorphic eMRTD document. Polymorphic inspection systems must authenticate themselves to the polymorphic eMRTD

document's chip for access to the polymorphic data with its private Terminal Authentication Key and its Inspection System Certificate.

Application Note: This OE is an extension of the OE 'OE.Terminal' from [PACE-PP] and 'OE.Ext_Insp_Systems', 'OE.Prot_Logical_Travel_Document', 'OE.Exam_Travel_Document' defined in [EAC-PP-V2].

7.2.6.3 OE.Personalisation_Polymorphic

Personalisation of the polymorphic eMRTD document by the Personalisation Agent
The Personalisation Agent shall guarantee the correctness of the PI/PP/CPI data of the polymorphic eMRTD document with respect to the polymorphic eMRTD document holder. The personalisation of the polymorphic eMRTD document for the holder must be performed by an agent authorized by the issuing State or Organisation only. The Polymorphic Personalisation Agent shall guarantee privacy of the PI/PP/CPI data during the personalisation phase (loading of PI/PP/CPI data in the Polymorphic eMRTD document).

Application Note: This OE is an extension of the OE 'OE.Personalisation' from [PACE-PP].

7.2.7 Additional OEs related to LDS2 extension

The table below provides a mapping giving the OEs related to the LDS2 and OSs from PACE PP [PACE-PP] and EAC PP [EAC-PP-V2]:

OEs related to the LDS2	**OEs from PACE PP**	**OEs from EAC PP**
OE.Authoriz_Sens_LDS2_Data	OE.Legislative_Compliance	OE.Authoriz_Sens_Data, OE.Auth_Key_Travel_Document
OE.Personalisation_LDS2	OE.Personalisation	OE.Authoriz_Sens_Data, OE.Auth_Key_Travel_Document
OE.Passive_Auth_Sign_LDS2	OE.Passive_Auth_Sign	
OE.Ext_Insp_Systems_LDS2		OE.Ext_Insp_Systems

7.2.7.1 OE.Authoriz_Sens_LDS2_Data

Authorization for Use of LDS2 sensitive multi application Data
The issuing State or Organisation has to establish the necessary public key infrastructure according [LDS2_PKI] in order to limit the access to sensitive Travel Records, Visa Records and Additional Biometric data of travel 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.
The infrastructure is established in order to

1. generate the travel document's Chip Authentication Key Pair,
2. sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.CardSecurity (present under the MF) and
3. support LDS2 inspection systems of receiving States or Organisations to verify the travel document's chip authenticity used for genuine travel document by certification of the Chip Authentication Public Key by means of verifying the Signature of the DER encoded Content structure of the type SignedData in EF.CardSecurity as specified in [ICAO-9303] part 10.

Application Note: This OE is an extension of the OEs 'OE.Legislative_Compliance' from [PACE-PP] and 'OE.Auth_Key_Travel_Document', 'OE.Authoriz_Sens_Data' defined in [EAC-PP-V2].

7.2.7.2 OE.Passive_Auth_Sign_LDS2

Authentication of travel document by Signature.
This environment objective fully inherits OE.Passive_Auth_Sign and adds the following environment objectives to the Document Signer role:

A Document Signer acting in accordance with the CSCA policy must

1. sign SecurityInfo entries in EF.CardSecurity of genuine travel documents in a secure operational environment only.

The digital signature is calculated over all present SecurityInfo entries in EF.CardAccess specified by [9303-10_LDS2] (which includes CAv1 public key) and is included together with the SecurityInfo entries in a ContentInfo structure of type id-SignedData as specified in [TR-03110-3].

The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct EF.CardSecurity SecurityInfo entries to be stored on the travel document.

Application Note: This OE extension has been added to this ST for supporting LDS2. This addition does not conflict with the strict conformance to PACE PP [PACE-PP] and EAC PP [EAC-PP-V2].

7.2.7.3 OE.Ext_Insp_Systems_LDS2

Authorization of LDS2 Extended Inspection Systems
The Document Verifier of receiving States or Organisations authorizes LDS2 Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive LDS2 application data on the logical travel document. The LDS2 Extended Inspection Systems authenticate themselves to the travel document's chip for access to the sensitive LDS2 applications 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 [PACE-PP] in order to handle the Threat T.Read_LDS2_Sensitive_Data, the Organisational Security Policy P.LDS2_Sensitive_Data and the Assumption A.Insp_Sys_LDS2 as it specifies the pre-requisite for the Terminal.

Application Note: This OE extension has been added to this ST for supporting LDS2. This addition does not conflict with the strict conformance to PACE PP [PACE-PP] and EAC PP [EAC-PP-V2].

7.2.7.4 OE.Personalisation_LDS2

Personalisation of travel document
In addition to OE.Personalisation, the travel document Issuer must ensure that the Personalisation Agents acting on his behalf

- creates correct LDS2 applications with Application Identifiers (AID) specified in [9303-10_LDS2] for Visa records, travel records, additional biometrics and configure access rights
  1. based on only a succesfully accomplished PACE-CAv1-TAv1 authentication sequence and
  2. the LDS2 application specific role based access rights in certificate extensions of the CVCA, DVCA and IS CV certificates in accordance with [9303-10_LDS2],
- creates correct EF.DIR and EF.CardSecurity and configure its access rights in accordance with [9303-10_LDS2],
- signs the EF.CardSecurity SecurityInfo entries in the role of Document Signer as specified in [ICAO-9303] and signature according [TR-03110-3].
- [Optional] enroll and sign Additional biometric reference data of the travel document holder and store them in the LDS2 "Additional Biometric" application in the role of Additional Biometrics Signer.

Application Note: This OE extension has been added to this ST for the LDS2 Personalisation environment. This addition does not conflict with the strict conformance to PACE PP [PACE-PP] and EAC PP [EAC-PP-V2].

7.3 Security Objectives Rationale

7.3.1 Threats

7.3.1.1 Threats listed in PP PACE

T.Skimming

The threat T.Skimming 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, OT.Data_Authenticity and OT.Data_Confidentiality through the PACE authentication. The objective OE.Travel_Document_Holder ensures that a PACE session can only be established either by the travel document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

T.Eavesdropping

The threat T.Eavesdropping 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 through a trusted channel based on the PACE authentication

T.Tracing

The threat T.Tracing 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 (no gathering TOE tracing data) and OE.Travel_Document_Holder (the attacker does not a priori know the correct values of the shared passwords).

T.Forgery

The threat T.Forgery addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. The security objective OT.AC_Pers requires the TOE to limit the write access for the travel 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 and OT.Data_Authenticity, respectively. The objectives OT.Prot_Phys-Tamper and OT.Prot_Abuse-Func 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 and performing the Passive Authentication using the Document Security Object as aimed by OE.Passive_Auth_Sign will be able to effectively verify integrity and authenticity of the data received from the TOE.

The examination of the presented MRTD passport book according to OE.Exam_Travel_Document "Examination of the physical part of the travel document" shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the travel document.

T.Abuse-Func

The threat T.Abuse-Func addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the soft-coded security

functionality. The security objective OT.Prot_Abuse-Func ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

T.Information_Leakage

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

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

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.

7.3.1.2 Additional Threats

T.Read_Sensitive_Data

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"

T.Counterfeit

T.Counterfeir 'Counterfeit of travel document chip data' addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is thwarted by chip an identification and authenticity proof required by OT.Chip_Auth_Proof 'Proof of travel document's chip authentication' using an authentication key pair to be generated by the issuing State or Organisation. The chip can also be identified using OT.Chip_Auth_Proof_PACE_CAM that supports PACE-CAM and OT.AA_Proof that supports Active Authentication. 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 'Travel document Authentication Key'. According to OE.Exam_Travel_Document 'Examination of the physical part of the travel document' the General Inspection system has to perform the Chip Authentication Protocol Version 1 to verify the authenticity of the travel document's chip. Moreover, the Active Authentication Public Key has to be written into EF.DG15 as demanded by OE.Auth_Key_MRTD 'MRTD Authentication Key'. According to OE.AA_MRTD 'Active Authentication - Inspection Systems' the Inspection system has to perform the Active Authentication Protocol to verify the authenticity of the MRTD's chip.

The threat is also countered by OT.DBI that helps ensure that a counterfeit TOE is identified because of the digitally blurred images.

T. BAC_breaking

The threat T. BAC_breaking "BAC protocol is broken" addresses the attack aiming at breaking the BAC protocol. The protection of the TOE against this threat is addressed by security objective OT.BAC_Expiration "Automatic deactivation of BAC protocol" which is directly related to it. It prevents an attacker to perform offline dictionary attacks on transaction log, in order to preserve confidentiality of data and avoid citizen traceability.

7.3.1.3 Threats related to Polymorphic eMRTD

T.Sensitive_Polymorphic_Data

The threat **T.Sensitive_Polymorphic_Data** is countered by the following TOE-objectives:

- **OT.Polymorphic_Data_Confidentiality** requiring the confidentiality of the static sensitive polymorphic eMRTD PI, PP and CPI user data stored inside the TOE. Furthermore the confidentiality of the eMRTD polymorphic the randomized PI, PP and optional CPI User Data during their exchange is also required.
- **OT.Polymorphic_Data_Authenticity** requiring the authenticity of the polymorphic eMRTD randomized PI, PP and optional CPI user data during their exchange between the TOE and Terminal/Authentication Service.
- **OT.Polymorphic_Data_Privacy** requiring the privacy of the PI, PP and optional CPI user data during the polymorphic authentication process steps, including during the randomisation performed by the TOE as part of the PMA protocol.
- **OE.Authoriz_Polymorphic_Data** requiring the authorization for the use of Polymorphic eMRTD user data based on CVCA/DV/IS certificates issued by the issuing State, the Polymorphic eMRTD document issuer or Organisation.

T.Forgery_Polymorphic

The threat **T.Forgery_Polymorphic** addresses the fraudulent, complete or partial alteration of the Polymorppphic eMRTD User Data stored on the TOE. It is countered by the following TOE-objectives:

- **OT.Polymorphic_Data_Integrity** requiring the integrity of the sensitive polymorphic eMRTD PI, PP and CPI data.
- **OT.AC_Pers_Polymorphic** requiring that the Polymorphic eMRTD data PI/PP/CPI and PIN/PUK data can only be written by authorized Personalisation Agents only.
- **OT.Prot_Phys-Tamper** and **OT.Prot_Abuse-Func** contribute to protecting integrity of the polymorphic eMRTD user data stored on the TOE.

T.Compromise_Privacy_Poly

The threat **T.Compromise_Privacy_Poly** is countered by the following TOE-objectives:

- **OT.Polymorphic_Data_Privacy** requiring the privacy of the PI, PP and optional CPI user data during the polymorphic authentication process steps, including during the randomisation performed by the TOE as part of the PMA protocol.
- **OT.Polymorphic_Data_Confidentiality** requiring the confidentiality of the static sensitive polymorphic eMRTD PI, PP and CPI user data stored inside the TOE. Furthermore the

confidentiality of the eMRTD polymorphic the randomized PI, PP and optional CPI User Data during their exchange is also required.

T.Eavesdropping_Polymorphic

The threat **T.Eavesdropping_Polymorphic** is countered by the following TOE-objective:

- **OT.Polymorphic_Data_Confidentiality** requiring the confidentiality of the static sensitive polymorphic eMRTD PI, PP and CPI user data stored inside the TOE. Furthermore the confidentiality of the eMRTD polymorphic the randomized PI, PP and optional CPI User Data during their exchange is also required.

7.3.1.4 Additional threats related to LDS2

T.Read_LDS2_Sensitive_Data

The threat **T.Read_LDS2_Sensitive_Data** is countered by the following TOE-objective:

- **OT.LDS2_Data_Confidentiality** requiring the confidentiality of the sensitive Entry/Exit data (Travel Record Application), Visa data and Additional Biometric reference data stored inside the TOE. Furthermore the confidentiality of the same User Data during their exchange is also required.
- **OT.AC_Pers_LDS2** requiring the TSF data can be written by authorized Personalisation Agents only.
- **OE.Authoriz_Sens_LDS2_Data** requiring the authorization bases on Document Verifier certificates issued by the issuing State or Organisation for use of sensitive reference data.
- **OE.Ext_Insp_Systems_LDS2** requiring the Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive LDS2 data.

T.Forgery_LDS2_Sensitive_Data

The threat **T.Forgery_LDS2_Sensitive_Data** addresses the fraudulent, complete or partial alteration of the reference data of the LDS2 sensitive applications. It is countered by the following TOE-objectives:

- **OT.AC_Pers_LDS2** requiring that the Document Security Object can only be written by an authorized personalization agent (**OE.Personalisation_LDS2)** and any access to LDS2 application requires PACE, CA and TA.
- **OT.Prot_Phys-Tamper** and **OT.Prot_Abuse-Func** contribute to protecting integrity of the eMRTD user data stored on the TOE.
- The examination of the presented MRTD passport book according to **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the travel document.
- A terminal operator operating the terminal according to **OE.Terminal** and performing authentication as aimed by **OE.Passive_Auth_Sign_LDS2** will be able to effectively verify integrity and authenticity of the data received from the TOE.

- **OE.Ext_Insp_Systems_LDS2** requiring the Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive LDS2 data.

7.3.2 Organisational Security Policies

7.3.2.1 OSP listed in PP PACE

P.Manufact

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**.

P.Pre-Operational

is enforced by the following security objectives: OT.Identification is affine to the OSP's property 'traceability before the operational phase; OT.AC_Pers and OE.Personalisation together enforce the OSP's properties 'correctness of the User and the TSF-data stored' and 'authorisation of Personalisation Agents'; OE.Legislative_Compliance is affine to the OSP's property 'compliance with laws and regulations'.

P.Card_PKI

is enforced by establishing the issuing PKI branch as aimed by the objectives OE.Passive_Auth_Sign (for the Document Security Object).

P.Trustworthy_PKI

is enforced by OE.Passive_Auth_Sign (for CSCA, issuing PKI branch).

P.Terminal

'Abilities and trustworthiness of terminals' is countered by the security objective OE.Exam_Travel_Document additionally to the security objectives from PACE PP [PACE-PP]. OE.Exam_Travel_Document enforces the terminals to perform the terminal part of the PACE protocol.

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

7.3.2.2 Additional OSPs from PP EAC

P.Sensitive_Data

P.Sensitive_Data "Read the sensitive biometric reference data" is fulfilled 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".

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 travel document by the Personalisation Agent as

described in the security objective for the TOE environment OE.Personalisation "Personalisation of logical travel 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 travel document". Note the manufacturer equips the TOE with the Personalisation Agent Key(s) according to OT.Identification "Identification and Authentication of the TOE". The security objective OT.AC_Pers limits the management of TSF data and the management of TSF to the Personalisation Agent.

7.3.2.3 OSPs related to Polymorphic eMRTD

P.Polymorphic_Data

The OSP P.Polymorphic_Data is fulfilled by the following Objectives:

- **OT.Polymorphic_Data_Confidentiality** requiring the confidentiality of the static sensitive polymorphic eMRTD PI, PP and CPI user data stored inside the TOE. Furthermore the confidentiality of the eMRTD polymorphic the randomized PI, PP and optional CPI User Data during their exchange is also required.
- **OT.Polymorphic_Data_Privacy** requiring the privacy of the PI, PP and optional CPI user data during the polymorphic authentication process steps, including during the randomisation performed by the TOE as part of the PMA protocol.
- **OE.Authoriz_Polymorphic_Data** requiring the authorization for the use of Polymorphic eMRTD User Data bases on CVCA/DV/IS certificates issued by the issuing State, the Polymorphic eMRTD document issuer or Organisation.

P.Polymorphic_Authentication_Terminal

The OSP P.Polymorphic_Data is fulfilled by the following Objective:

- **OE.Insp_Sys_Polymorphic** requiring the Polymorphic inspection systems (Terminals) or authentication services to perform the terminal part of PACE with PIN, PA, CAv1, TAv1 and PMA.

P.Pre-Operational_Polymorphic

The OSP P.Pre-Operational_Polymorphic is fulfilled by the following Objectives:

- **OT.AC_Pers_Polymorphic** requiring that the Polymorphic eMRTD data PI/PP/CPI and PIN/PUK data can be written by authorized Personalisation Agents only.
- **OE.Insp_Sys_Polymorphic** requiring the Polymorphic inspection systems (Terminals) or authentication services to perform the terminal part of PACE with PIN, PA, CAv1, TAv1 and PMA protocols.
- **OE.Authoriz_Polymorphic_Data** requiring the authorization for the use of Polymorphic eMRTD User Data bases on CVCA/DV/IS certificates issued by the issuing State, the Polymorphic eMRTD document issuer or Organisation.
- **OE.Polymorphic_Auth** requiring the secure generation and storage of the authentication infrastructure keys and PP/PI/CPI data.
- **OE.Personalisation_Polymorphic** requiring that the Polymorphic Personalisation Agent guarantees the correctness and the privacy of the PI/PP/CPI data during the personalisation phase.

P.Personalisation_Polymorphic

The OSP P.Personalisation_Polymorphic is fulfilled by the following Objectives:

- **OT.AC_Pers_Polymorphic** requiring that the Polymorphic eMRTD data PI/PP/CPI and PIN/PUK data can be written by authorized Personalisation Agents only.
- **OE.Personalisation_Polymorphic** requiring that the Polymorphic Personalisation Agent guarantees the correctness and the privacy of the PI/PP/CPI data during the personalisation phase.

7.3.2.4 Additional OSPs related to LDS2

P.LDS2_Card_PKI

is enforced by

- **OE.Passive_Auth_Sign_LDS2** by establishing the issuing PKI branch (for the SignedData structure in EF.CardSecurity Security Object).

P.LDS2_Personalisation

is enforced by

- **OE.Personalisation_LDS2** addressing the enrolment of the logical travel document by the Personalisation Agent as described in the security objective. Note that OE.Personalisation_LDS2 is also completed by OT.AC_Pers_LDS2.
- **OT.AC_Pers_LDS2** addressing the access control for the user data and TSF data as described by the security objective. The security objective OT.AC_Pers_LDS2 limits the management of user and TSF data and the management of TSF to the Personalisation Agent. Also management of writing User Data is limited to the Personalisation Agent.
- **OT.Identification** addressing loading the TOE with the Personalisation Agent Key(s) by the manufacturer according to OT.Identification 'Identification and Authentication of the TOE'.

P.LDS2_Sensitive_Data

is enforced by

- **OT.LDS2_Data_Confidentiality** requiring the confidentiality of the sensitive Entry/Exit data (Travel Record Application), Visa data and Additional Biometric user data stored inside the TOE. Furthermore the confidentiality of the eMRTD Additional application User Data during their exchange is also required.
- **OE.Authoriz_Sens_LDS2_Data** requiring the authorization for the use of LDS2 eMRTD User Data bases on CVCA/DV/IS certificates issued by the issuing State, the eMRTD document issuer or Organisation.
- **OE.Ext_Insp_Systems_LDS2** requiring the Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive LDS2 data.

7.3.3 Assumptions

7.3.3.1 Assumptions listed in PP PACE

A.Passive_Auth

The Assumption A.Passive_Auth "PKI for Passive Authentication" is directly addressed by OE.Passive_Auth_Sign requiring the travel document issuer to establish a PKI for Passive Authentication, generating Document Signing private keys only for rightful organisations and requiring the Document Signer to sign exclusively correct Document Security Objects to be stored on travel document.

It is also covered by the security objective for the TOE environment OE.Passive_Auth_Sign "Authentication of travel document by Signature" from PACE PP 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 travel document".

7.3.3.2 Assumptions listed in PP EAC

A.Insp_Sys

The examination of the travel 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 travel document" which requires the inspection system to examine physically the travel 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 travel document's chip. The security objectives for the TOE environment OE.Prot_Logical_Travel_Document "Protection of data from the logical travel document" require the Inspection System to protect the logical travel 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.

7.3.3.3 Assumptions related to Active Authentication

A.Pers_Agent_AA

The assumption **A.Pers_Agent_AA** is directly covered by the security objective for the TOE environment **OE.Personalisation** including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

7.3.3.4 Assumptions related to Polymorphic eMRTD

A.Polymorphic_Auth

The assumption A.Polymorphic_Auth is directly covered by the following objective:

- **OE.Polymorphic_Auth** requiring the secure generation and storage of the authentication infrastructure keys and PP/PI/CPI data.

A.Auth_PKI_Polymorphic

The assumption A.Auth_PKI_Polymorphic is directly covered by the following objective:

- **OE.Authoriz_Polymorphic_Data** requiring the authorization for the use of Polymorphic eMRTD User Data bases on CVCA/DV/IS certificates issued by the issuing State, the Polymorphic eMRTD document issuer or Organisation.

A.Insp_Sys_Polymorphic

The assumption A.Insp_Sys_Polymorphic is directly covered by the following objective:

- **OE.Insp_Sys_Polymorphic** requiring the Polymorphic inspection systems (Terminals) or authentication services to perform the terminal part of PACE with PIN, PA, CAv1, TAv1 and PMA.

7.3.3.5 Assumptions related to LDS2

A. Insp_Sys_LDS2

The assumption A.Insp_Sys_LDS2 is covered by the following objective:

- **OE.Ext_Insp_Systems_LDS2** ensuring that the terminals are equipped to handle and perform PACE, CAv1 and TAv1.

7.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Skimming	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OE.Travel_Document_Holder	Rationale
T.Eavesdropping	OT.Data_Confidentiality	Rationale
T.Tracing	OT.Tracing, OE.Travel_Document_Holder	Rationale
T.Forgery	OT.Data_Integrity, OT.Data_Authenticity, OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper, OT.AC_Pers, OE.Passive_Auth_Sign, OE.Personalisation, OE.Terminal, OE.Exam_Travel_Document	Rationale
T.Abuse-Func	OT.Prot_Abuse-Func	Rationale
T.Information_Leakage	OT.Prot_Inf_Leak	Rationale
T.Phys-Tamper	OT.Prot_Phys-Tamper	Rationale
T.Malfunction	OT.Prot_Malfunction	Rationale
T.Read_Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Rationale
T.Counterfeit	OT.Chip_Auth_Proof, OT.Chip_Auth_Proof_PACE_CAM, OT.AA_Proof, OE.Auth_Key_Travel_Document, OE.Exam_Travel_Document, OE.AA_MRTD, OE.Auth_Key_MRTD, OT.DBI	Rationale
T.Sensitive_Polymorphic_Data	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Authenticity, OT.Polymorphic_Data_Privacy, OE.Authoriz_Polymorphic_Data	Rationale

T.Forgery_Polymorphic	OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper, OT.Polymorphic_Data_Integrity, OT.AC_Pers_Polymorphic	Rationale
T.Compromise_Privacy_Poly	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Privacy	Rationale
T.Eavesdropping_Polymorphic	OT.Polymorphic_Data_Confidentiality	Rationale
T.Read_LDS2_Sensitive_Data	OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2, OE.Authoriz_Sens_LDS2_Data, OE.Ext_Insp_Systems_LDS2	Rationale
T.Forgery_LDS2_Sensitive_Data	OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper, OT.AC_Pers_LDS2, OE.Exam_Travel_Document, OE.Passive_Auth_Sign_LDS2, OE.Personalisation_LDS2, OE.Ext_Insp_Systems_LDS2, OE.Terminal	Rationale
T. BAC_breaking	OT.BAC_Expiration	Rationale

Table 19 Threats and Security Objectives - Coverage

Security Objectives	Threats
OT.Data_Integrity	T.Skimming, T.Forgery
OT.Data_Authenticity	T.Skimming, T.Forgery
OT.Data_Confidentiality	T.Skimming, T.Eavesdropping
OT.Tracing	T.Tracing
OT.Prot_Abuse-Func	T.Forgery, T.Abuse-Func, T.Forgery_Polymorphic, T.Forgery_LDS2_Sensitive_Data
OT.Prot_Inf_Leak	T.Information_Leakage
OT.Prot_Phys-Tamper	T.Forgery, T.Phys-Tamper, T.Forgery_Polymorphic, T.Forgery_LDS2_Sensitive_Data
OT.Prot_Malfunction	T.Malfunction
OT.Identification	
OT.AC_Pers	T.Forgery
OT.Sens_Data_Conf	T.Read_Sensitive_Data
OT.Chip_Auth_Proof	T.Counterfeit
OT.Polymorphic_Data_Confidentiality	T.Sensitive_Polymorphic_Data , T.Compromise_Privacy_Poly , T.Eavesdropping_Polymorphic
OT.Polymorphic_Data_Integrity	T.Forgery_Polymorphic
OT.Polymorphic_Data_Authenticity	T.Sensitive_Polymorphic_Data
OT.Polymorphic_Data_Privacy	T.Sensitive_Polymorphic_Data , T.Compromise_Privacy_Poly
OT.AC_Pers_Polymorphic	T.Forgery_Polymorphic
OT.LDS2_Data_Confidentiality	T.Read_LDS2_Sensitive_Data
OT.AC_Pers_LDS2	T.Read_LDS2_Sensitive_Data, T.Forgery_LDS2_Sensitive_Data
OT.Chip_Auth_Proof_PACE_CAM	T.Counterfeit
OT.AA_Proof	T.Counterfeit
OT.BAC_Expiration	T. BAC_breaking

OT.DBI	T.Counterfeit
OE.Legislative_Compliance	
OE.Auth_Key_Travel_Document	T.Counterfeit
OE.Authoriz_Sens_Data	T.Read_Sensitive_Data
OE.Passive_Auth_Sign	T.Forgery
OE.Personalisation	T.Forgery
OE.Terminal	T.Forgery, T.Forgery_LDS2_Sensitive_Data
OE.Travel_Document_Holder	T.Skimming, T.Tracing
OE.Exam_Travel_Document	T.Forgery, T.Counterfeit , T.Forgery_LDS2_Sensitive_Data
OE.AA_MRTD	T.Counterfeit
OE.Auth_Key_MRTD	T.Counterfeit
OE.Prot_Logical_Travel_Document	
OE.Ext_Insp_Systems	T.Read_Sensitive_Data
OE.Polymorphic_Auth	
OE.Authoriz_Polymorphic_Data	T.Sensitive_Polymorphic_Data
OE.Insp_Sys_Polymorphic	
OE.Personalisation_Polymorphic	
OE.Authoriz_Sens_LDS2_Data	T.Read_LDS2_Sensitive_Data
OE.Passive_Auth_Sign_LDS2	T.Forgery_LDS2_Sensitive_Data
OE.Ext_Insp_Systems_LDS2	T.Read_LDS2_Sensitive_Data, T.Forgery_LDS2_Sensitive_Data
OE.Personalisation_LDS2	T.Forgery_LDS2_Sensitive_Data

Table 20 Security Objectives and Threats - Coverage

OSPs	Security Objectives	Rationale
P.Manufact	OT.Identification	Rationale
P.Pre-Operational	OT.Identification, OT.AC_Pers, OE.Personalisation, OE.Legislative_Compliance	Rationale
P.Card_PKI	OE.Passive_Auth_Sign	Rationale
P.Trustworthy_PKI	OE.Passive_Auth_Sign	Rationale
P.Terminal	OE.Terminal, OE.Exam_Travel_Document	Rationale
P.Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Rationale
P.Personalisation	OT.AC_Pers, OE.Personalisation, OT.Identification	Rationale
P.Polymorphic_Data	OT.Polymorphic_Data_Privacy, OT.Polymorphic_Data_Confidentiality, OE.Authoriz_Polymorphic_Data	Rationale
P.Polymorphic_Authentication_Terminal	OE.Insp_Sys_Polymorphic	Rationale
P.Pre-Operational_Polymorphic	OT.AC_Pers_Polymorphic, OE.Polymorphic_Auth, OE.Authoriz_Polymorphic_Data,	Rationale

	OE.Insp_Sys_Polymorphic, OE.Personalisation_Polymorphic	
P.Personalisation_Polymorphic	OT.AC_Pers_Polymorphic, OE.Personalisation_Polymorphic	Rationale
P.LDS2_Card_PKI	OE.Passive_Auth_Sign_LDS2	Rationale
P.LDS2_Personalisation	OT.Identification, OT.AC_Pers_LDS2, OE.Personalisation_LDS2	Rationale
P.LDS2_Sensitive_Data	OT.LDS2_Data_Confidentiality, OE.Authoriz_Sens_LDS2_Data, OE.Ext_Insp_Systems_LDS2	Rationale

Table 21 OSPs and Security Objectives - Coverage

Security Objectives	OSPs
OT.Data_Integrity	
OT.Data_Authenticity	
OT.Data_Confidentiality	
OT.Tracing	
OT.Prot_Abuse-Func	
OT.Prot_Inf_Leak	
OT.Prot_Phys-Tamper	
OT.Prot_Malfunction	
OT.Identification	P.Manufact , P.Pre-Operational, P.Personalisation, P.LDS2_Personalisation
OT.AC_Pers	P.Pre-Operational, P.Personalisation
OT.Sens_Data_Conf	P.Sensitive_Data
OT.Chip_Auth_Proof	
OT.Polymorphic_Data_Confidentiality	P.Polymorphic_Data
OT.Polymorphic_Data_Integrity	
OT.Polymorphic_Data_Authenticity	
OT.Polymorphic_Data_Privacy	P.Polymorphic_Data
OT.AC_Pers_Polymorphic	P.Pre-Operational_Polymorphic, P.Personalisation_Polymorphic
OT.LDS2_Data_Confidentiality	P.LDS2_Sensitive_Data
OT.AC_Pers_LDS2	P.LDS2_Personalisation
OT.Chip_Auth_Proof_PACE_CAM	
OT.AA_Proof	
OT.BAC_Expiration	
OT.DBI	
OE.Legislative_Compliance	P.Pre-Operational
OE.Auth_Key_Travel_Document	
OE.Authoriz_Sens_Data	P.Sensitive_Data
OE.Passive_Auth_Sign	P.Card_PKI, P.Trustworthy_PKI

OE.Personalisation	P.Pre-Operational, P.Personalisation
OE.Terminal	P.Terminal
OE.Travel_Document_Holder	
OE.Exam_Travel_Document	P.Terminal
OE.AA_MRTD	
OE.Auth_Key_MRTD	
OE.Prot_Logical_Travel_Document	
OE.Ext_Insp_Systems	P.Sensitive_Data
OE.Polymorphic_Auth	P.Pre-Operational_Polymorphic
OE.Authoriz_Polymorphic_Data	P.Polymorphic_Data, P.Pre-Operational_Polymorphic
OE.Insp_Sys_Polymorphic	P.Polymorphic_Authentication_Terminal, P.Pre-Operational_Polymorphic
OE.Personalisation_Polymorphic	P.Pre-Operational_Polymorphic, P.Personalisation_Polymorphic
OE.Authoriz_Sens_LDS2_Data	P.LDS2_Sensitive_Data
OE.Passive_Auth_Sign_LDS2	P.LDS2_Card_PKI
OE.Ext_Insp_Systems_LDS2	P.LDS2_Sensitive_Data
OE.Personalisation_LDS2	P.LDS2_Personalisation

Table 22 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.Passive_Auth	OE.Passive_Auth_Sign, OE.Exam_Travel_Document	Rationale
A.Insp_Sys	OE.Exam_Travel_Document, OE.Prot_Logical_Travel_Document	Rationale
A.Auth_PKI	OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Rationale
A.Pers_Agent_AA	OE.Personalisation	Rationale
A.Polymorphic_Auth	OE.Polymorphic_Auth	Rationale
A.Auth_PKI_Polymorphic	OE.Authoriz_Polymorphic_Data	Rationale
A.Insp_Sys_Polymorphic	OE.Insp_Sys_Polymorphic	Rationale
A. Insp_Sys_LDS2	OE.Ext_Insp_Systems_LDS2	Rationale

Table 23 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions
OE.Legislative_Compliance	
OE.Auth_Key_Travel_Document	
OE.Authoriz_Sens_Data	A.Auth_PKI
OE.Passive_Auth_Sign	A.Passive_Auth
OE.Personalisation	A.Pers_Agent_AA
OE.Terminal	

OE.Travel_Document_Holder	
OE.Exam_Travel_Document	A.Passive_Auth, A.Insp_Sys
OE.AA_MRTD	
OE.Auth_Key_MRTD	
OE.Prot_Logical_Travel_Document	A.Insp_Sys
OE.Ext_Insp_Systems	A.Auth_PKI
OE.Polymorphic_Auth	A.Polymorphic_Auth
OE.Authoriz_Polymorphic_Data	A.Auth_PKI_Polymorphic
OE.Insp_Sys_Polymorphic	A.Insp_Sys_Polymorphic
OE.Personalisation_Polymorphic	
OE.Authoriz_Sens_LDS2_Data	
OE.Passive_Auth_Sign_LDS2	
OE.Ext_Insp_Systems_LDS2	A. Insp_Sys_LDS2
OE.Personalisation_LDS2	

Table 24 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 SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE?s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

8.1.1.2 Extended Components

8.1.1.2.1.1 Extended Component FPT_EMS.1

8.1.1.2.1.2 Description

This family defines requirements to mitigate intelligible emanations. 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.

8.1.1.2.1.3 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]**.

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]**.

8.1.2 Extended Family FIA_API - Authentication Proof of Identity

8.1.2.1 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.

8.1.2.2 Extended Components

8.1.2.2.1.1 Extended Component FIA_API.1

8.1.2.2.1.2 Description

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

8.1.2.2.1.3 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*]**.

8.1.3 Extended Family FMT_LIM - Limited capabilities

8.1.3.1 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.

8.1.3.2 Extended Components

8.1.3.2.1.1 Extended Component FMT_LIM.2

8.1.3.2.1.2 Definition

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 **[assignment: Limited capability and availability policy]**

8.1.3.2.1.3 Extended Component FMT_LIM.1

8.1.3.2.1.4 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]**

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:

8.1.4.2 Extended Components

8.1.4.2.1.1 Extended Component FAU_SAS.1

8.1.4.2.1.2 Description

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

8.1.4.2.1.3 Definition

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.

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

8.1.5.2.1.1 Extended Component FCS_RND.1

8.1.5.2.1.2 Description

Generation of random numbers requires that random numbers meet a defined quality metric.

8.1.5.2.1.3 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*]**.

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 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 FCS : Cryptographic Support

FCS_CKM.1/DH_PACE - Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Cryptographic Key Generation Algorithm]** and specified cryptographic key sizes **[Cryptographic Key Sizes]** that meet the following: **[Standards]**

Cryptographic Key Generation Algorithm	Cryptographic Key Sizes	Standards
PACE Protocol [ICAO-9303] based on the ECDH protocol compliant to [TR-03111] in combination with 112 bits 3DES or 128, 192 or 256 bits AES	192, 224, 256, 320, 384, 512 and 521 bits	[TR-03111]
PACE Protocol [ICAO-9303] based on the DH protocol compliant to [RSA-PKCS#3] in combination with 112 bits 3DES or 128, 192 or 256 bits AES	2048 bits	[TR-03110-1] and [RSA-PKCS#3]

FCS_CKM.1/CA - Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Cryptographic Key Generation Algorithm]** and specified cryptographic key sizes **[Cryptographic Key Sizes]** that meet the following: **[Standards]**

Cryptographic Key Generation Algorithm	Cryptographic Key Sizes	Standards
Chip Authentication Protocol Version 1 [TR-03110-1] based on the ECDH protocol	192, 224, 256, 320, 384, 512 and 521 bits	[TR-03111]

compliant to [TR-03111] in combination with 112 bits 3DES or 128, 192 or 256 bits AES		
Chip Authentication Protocol Version 1[TR-03110-1] based on the DH protocol compliant to [TR-03110-1] in combination with 112 bits 3DES or 128, 192 or 256 bits AES	**2048 bits**	**[TR-03110-1] and [RSA-PKCS#3]**

FCS_CKM.1/AA - Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Cryptographic Key Generation Algorithm]** and specified cryptographic key sizes **[Cryptographic Key Sizes]** that meet the following: **[Standards]**

Cryptographic Key Generation Algorithm	Cryptographic Key Sizes	Standards
ECC	**192, 224, 256, 320, 384, 512 and 521**	**[IEEE_1363]**
RSA	**1536, 1792, 2048, 2560, 3072, 3584 and 4096**	**[ANSI_X9.31]**

FCS_CKM.1/CAM - Cryptographic Key Generation

FCS_CKM.1.1 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, 224, 256, 320, 384, 512 and 521 bits in combination with 112 bits 3DES or 128, 192 or 256 bits AES** that meet the following: **[ICAO-9303]**.

FCS_CKM.1/POLY - Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECC** and specified cryptographic key sizes **320, 384 and 512 bits** that meet the following: **ECC Brainpool domain parameters [RFC-5639]**.

Application Note: The TOE generates the ephemeral key random k for as part of the Polymorphic Authentication protocol. This key is used for the randomization process of PI, PP and optional CPI required by FCS_COP.1/POLY. The TOE shall destroy this key in accordance with FCS_CKM.4 after successful randomization process of PI, PP and optional CPI.

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 **physically overwriting the keys** that meets the following: **none**.

FCS_COP.1/AA - Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **[cryptographic operation]** in accordance with a specified cryptographic algorithm **[algorithm]** and cryptographic key sizes **[key sizes]** that meet the following: **[standards]**

Cryptographic Operation	Cryptographic Algorithm	Cryptographic Key Sizes(bits)	Standard
Digital Signature Creation	**ECDSA**	**192 to 521 over prime field curves**	**[ISO_9796-2], [RSA-PKCS#3], [FIPS_180_2] and [X.92]**
Digital Signature Creation	**RSA signature**	**1536, 1792, 2048, 2560, 3072, 3584 and 4096**	**[ISO_9796-2]**

FCS_COP.1/CAM - Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **the PACE-CAM protocol** in accordance with a specified cryptographic algorithm **PACE-CAM** and cryptographic key sizes **192 to 521 bits** that meet the following: **[ICAO-9303]**.

FCS_COP.1/CA_MAC - Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **[Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[Cryptographic Algorithm]** and cryptographic key sizes **[Cryptographic Key Sizes]** that meet the following: **[Standards]**

Cryptographic Operation	Cryptographic Algorithm	Key Sizes	Standards
secure messaging message authentication code	**3DES Retail-MAC**	**112 bits**	**[ICAO-9303]**
secure messaging message authentication code	**AES CMAC**	**128, 192 and 256 bits**	**[NIST-800-38B]**

FCS_COP.1/CA_ENC - Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **[Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[Cryptographic Algorithm]** and cryptographic key sizes **[Key Sizes]** that meet the following: **[Standards]**

Cryptographic Operation	Cryptographic Algorithm	Key Sizes	Standards
secure messaging encryption and decryption	**3DES in CBC mode**	**112**	**[TR-03110-1]**
secure messaging encryption and decryption	**AES in CBC mode**	**128, 192 and 256**	**[TR-03110-1]**

FCS_COP.1/PACE_ENC - Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **[Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[Cryptographic Algorithm]** and cryptographic key sizes **[Key Sizes]** that meet the following: **[Standards]**

Cryptographic Operation	Cryptographic Algorithm	Key Sizes	Standards
secure messaging encryption and decryption	**3DES in CBC mode**	**112**	**[ICAO-9303] part 11**
secure messaging encryption and decryption	**AES in CBC mode**	**128, 192 and 256**	**[ICAO-9303] part 11**

FCS_COP.1/PACE_MAC - Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **[Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[Cryptographic Algorithm]** and cryptographic key sizes **[Key Sizes]** that meet the following: **[Standards]**

Cryptographic Operation	Cryptographic Algorithm	Key Sizes	Standards
secure messaging message authentication code	**3DES Retail-MAC**	**112 bits**	**[ICAO-9303] part 11**
secure messaging message authentication code	**AES CMAC**	**128, 192 and 256 bits**	**[ICAO-9303] part 11**

FCS_COP.1/SIG_VER - Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **[Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[Cryptographic Algorithm]** and cryptographic key sizes **[Key Sizes]** that meet the following: **[Standards]**

Cryptographic Operation	Cryptographic Algorithm	Key Sizes	Standards
digital signature verification	**ECDSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512**	**192, 224, 256, 320, 384, 512 and 521 bits**	**ISO15946-2 specified in [ISO15946-2]**
digital signature verification	**RSA with SHA-1, SHA-256 and SHA-512**	**1280, 1536, 1792, 2048, 2560, 3072, 3584 and 4096 bits**	**PKCS#1 v1.5 and PKCS#1-PSS**

FCS_COP.1/POLY - Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **PI, PP and optional CPI randomization** in accordance with a specified cryptographic algorithm **ECC** and cryptographic key sizes **320, 384, and 512 bits** that meet the following: **ECC Brainpool domain parameters [RFC-5639]**.

Application Note: In order to assure privacy for the Polymorphic eMRTD document holder, a randomization of the PI, PP and optional CPI is performed by the Polymorphic eMRTD application. The randomization of a PI/PP and optional CPI prevent these encrypted identity attributes as well as the user from being linkable by the Authentication Service to a Service Provider. It changes (i.e. 'randomizes') the PI, PP and optional CPI representations while preserving their original values.

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 deterministic random number generation specified by FCS_RNG.1 Quality metric for random numbers of [PTF-ST]**.

9.1.3 FDP : User Data Protection

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:

1. **Session Keys (immediately after closing related communication session),**
2. **the ephemeral private key ephem-SKpicc-PACE (by having generated a DH shared secret K)**
3. **none.**

FDP_UCT.1/TRM - Basic Data Exchange Confidentiality

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

FDP_UIT.1/TRM - Data Exchange Integrity

FDP_UIT.1.1 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 The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.

FDP_ACC.1/TRM - Subset Access Control

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

FDP_ACF.1/TRM - Security Attribute Based Access Control

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

1. **Subjects:**
   a. **Terminal,**
   b. **BIS-PACE,**
   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 travel document,**
   b. **data in EF.DG3 of the logical travel document,**

c. **data in EF.DG4 of the logical travel document,**
d. **all TOE intrinsic secret cryptographic keys stored in the travel document.**

3. **Security attributes:**
   a. **PACE Authentication**
   b. **Terminal Authentication v.1**
   c. **Authorisation of the Terminal.**

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

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

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

1. **Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.**
2. **Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document.**
3. **Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) 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 (Iris) 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.**

FDP_ACC.1/POLY - Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the **Polymorphic Access Control SFP** on **terminals gaining access to:**

- **the polymorphic eMRTD document data (DG14 and EF.SOD),**
- **the sensitive Polymorphic PI/PP/CPI user data,**
- **the PIN/PUK verification and management functions.**

Application Note: This SFR is an extension of the SFR 'FDP_ACC.1/TRM' defined in [EAC-PP-V2] to cover the secret Polymorphic eMRTD document holder authentication data, e.g. PIN and/or PUK and the sensitive polymorphic user data. This extension does not conflict with the strict conformance to PACE PP and EAC PP.

FDP_ACF.1/POLY - Security Attribute Based Access Control

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

1. **Subjects:**
    - **Polymorphic Authentication Terminal/Service**
    - **Personalisation Agent terminal**

2. **Objects:**
    - **polymorphic eMRTD document data in EF.DG14 and EF.SOD,**
    - **secret polymorphic eMRTD document holder authentication data (PIN/PUK),**
    - **sensitive polymorphic user data PI, PP and CPI,**
    - **all TOE intrinsic secret cryptographic keys stored in the travel document.**

3. **Security attributes:**
    - **PACE Authentication**
    - **Chip Authentication v.1**
    - **Terminal Authentication v.1**
    - **Authorisation of the Terminal**

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

- **only an authenticated personalisation agent terminal is allowed to write all objects specified in FDP_ACF.1.1/POLY**
- **only a Polymorphic Authentication Terminal/Service is allowed to read the polymorphic eMRTD document data in EF.DG14 and EF.SOD only after PACE Authentication has been successfully accomplished, independent of the used PACE password credential.**
- **A Polymorphic Authentication Terminal/Service, is only allowed to read the sensitive polymorphic user data PI, PP and CPI (specified in FDP_ACF.1.1/POLY) in case the following conditions have been satisfied:**
    1. **Either one of the following protocol scenarios has been successfully executed:**
        - **PACE Authentication (with user PIN) - CAv1 - TAv1**
        - **PACE Authentication (with CAN) - VERIFY(PIN) - CAv1 - TAv1**
    2. **The TAv1 terminal certificate specifies the appropriate access rights to receive the requested PP, PI op CPI value.**
    3. **PIN User consent constraint has been satisfied, i.e. the PP, PI or CPI value has not been read before within the same PACE secure messaging session.**
- **A Polymorphic Authentication Terminal/Service is granted access to VERIFY(PIN/PUK) and PIN Management functionality (Resume PIN, Change PIN and Unblock PIN), if the Polymorphic eMRTD Document Holder has been authenticated successfully in accordance with to FIA_UAU.1.1/POLY.**

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

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

1. **A Polymorphic Authentication Terminal/Service is denied access to the VERIFY(PIN/PUK) and PIN Management functionality (Resume PIN, Change PIN and Unblock PIN), in case Chip Authentication v1 (CAv1) has been performed successfully within the same PACE secure messaging session.**

2. **Any terminal not being authenticated as a personalisation agent terminal is not allowed to write, to modify or store any of the objects specified in FDP_ACF.1.1/POLY.**
3. **Terminals not using secure messaging are not allowed to read, to write, to modify or use any data stored on the document (i.e. objects specified in FDP_ACF.1.1/POLY).**
4. **Nobody is allowed to read, write and modify the data object 2.d) specified in FDP_ACF.1.1/POLY.**
5. **Terminals authenticated as CVCA or as DV are not allowed to read PI, PP and CPI data.**

FDP_RIP.1/POLY - 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 **allocation of the resource to and deallocation of the resource from** the following objects:

1. **secret Polymorphic eMRTD document holder authentication data, e.g. PIN and/or PUK (when their temporarily stored values are not used any more),**
2. **the randomized PI, PP and optional CPI,**
3. **the ephemeral (random) secret key k, used for the randomisation during the execution of the Polymorphic Authentication protocol.**

Application Note: This SFR is an extension of the SFR 'FDP_RIP.1' defined in [PACE-PP] to cover the Polymorphic eMRTD document holder authentication data, e.g. PIN and/or PUK, the randomized PI/PP and optional CPI user data, and the ephemeral secret key k as part of the Polymorphic Authentication protocol. This extension does not conflict with the strict conformance to PACE PP and EAC PP.

FDP_ACC.1/LDS2 - Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the **LDS2 SFP** on **terminals gaining access to additional LDS2 applications**.

FDP_ACF.1/LDS2 - Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the **LDS2 SFP** to objects based on the following:

1. **Subjects:**
   - **EIS**
2. **Objects:**
   - **Data for the additional LDS2 Applications**

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

- **Only a user authorized by a valid certificate with the appropriate APPEND authorization together with PACE, followed by Chip Authentication and Terminal Authentication is allowed to append to LDS2 record files.**
- **Only a user authorized by a valid certificate with the appropriate READ authorization together with PACE, followed by Chip Authentication and Terminal Authentication is allowed to read LDS2 application data.**

- **Only a user authorized by a valid certificate with the appropriate WRITE authorization together with PACE, followed by Chip Authentication and Terminal Authentication is allowed to write inside LDS2 application data.**

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **The TOE shall not allow any user to modify or delete data in exisiting additional LDS2 applications after personalisation phase**.

9.1.4 FIA : Identification and Authentication

FIA_UID.1/PACE_CAM - Timing Of Identification

FIA_UID.1.1 The TSF shall allow **additionally to FIA_UID.1/PACE**

1. carrying out the PACE CAM protocol according to [ICAO-9303] part 11

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

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

FIA_UAU.1/PACE_CAM - Timing Of Authentication

FIA_UAU.1.1 The TSF shall allow **additionally to FIA_UAU.1/PACE**

1. carrying out the PACE CAM protocol according to [ICAO-9303] part 11

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

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

FIA_UAU.4/PACE_CAM - Single-Use Authentication Mechanisms

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

1. PACE CAM Protocol according to [ICAO-9303] part 11 in addition to FIA_UAU.4/PACE.

FIA_UAU.5/PACE_CAM - Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide

1. PACE CAM Protocol according to [ICAO-9303] part 11

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **following rules: The same rules from FIA_UAU.5.2/PACE applies with the PACE CAM protocol.** .

FIA_UAU.6/PACE_CAM - Re-Authenticating

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

FIA_AFL.1/PACE - Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when **3** unsuccessful authentication attempts occur related to **authentication attempts using the PACE password as shared password.**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **wait a linear increasing time, starting at a minimum of 1s, before the next authentication attempt can be performed.**

Application Note: Note here, the PACE password could be a MRZ or CAN.

FIA_UID.1/PACE - Timing Of Identification

FIA_UID.1.1 The TSF shall allow

1. **to establish the communication channel,**
2. **carrying out the PACE Protocol (MRZ or CAN) according to [ICAO-9303] part 11,**
3. **to read the Initialisation Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,**
4. **to carry out the Chip Authentication Protocol v.1 according to [TR-03110-1],**
5. **to carry out the Terminal Authentication Protocol v.1 according to [TR-03110-1],**
6. **None**

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

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

FIA_UAU.1/PACE - Timing Of Authentication

FIA_UAU.1.1 The TSF shall allow

1. **to establish the communication channel,**
2. **carrying out the PACE Protocol (MRZ or CAN) according to [ICAO-9303] part 11,**
3. **to read the Initialisation Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,**
4. **to identify themselves by selection of the authentication key ,**
5. **to carry out the Chip Authentication Protocol v.1 according to [TR-03110-1],**
6. **to carry out the Terminal Authentication Protocol v.1 according to [TR-03110-1],**
7. **None**

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

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

FIA_UAU.4/PACE - Single-Use Authentication Mechanisms

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

1. **PACE Protocol according to [ICAO-9303] part 11**
2. **Authentication Mechanism based on Triple-DES and AES**
3. **Terminal Authentication Protocol Version 1 according to [TR-03110-1].**

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 The TSF shall provide

1. **PACE Protocol according to [ICAO-9303] part 11**
2. **Passive Authentication according to [ICAO-9303]**
3. **Secure messaging in MAC-ENC mode according to [ICAO-9303] part 11**
4. **Symmetric Authentication Mechanism based on Triple-DES and AES**
5. **Terminal Authentication Protocol Version 1 according to [TR-03110-1]**

to support user authentication.

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

1. **Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.**
2. **The TOE accepts the authentication attempt from the Personalisation Agent by means of GP authentication.**
3. **After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.**
4. **The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1**
5. **None.**

FIA_UAU.6/PACE - Re-Authenticating

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

FIA_API.1/AA - Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a **Active Authentication Protocol according to [ICAO-9303]** to prove the identity of the **TOE**.

FIA_API.1/CA - Authentication Proof of Identity

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

FIA_AFL.1/PINPUK - Authentication Failure Handling

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

1. **PACE using PIN/PUK**
2. **Verify PIN/PUK**

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

FIA_UID.1/POLY - Timing Of Identification

FIA_UID.1.1 The TSF shall allow **the steps specified in FIA_UAU.1/PACE, where step 2 is replaced by:**

- **to carry out the PACE protocol according to [TR-03110] of FIA_UID.1/PACE with either PIN or PUK as a password,**

or

- **to carry out the PACE protocol according to [ICAO-9303] with CAN as a password followed by VERIFY with PIN/PUK according to [PCA-eMRTD],**

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

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

FIA_UAU.1/POLY - Timing Of Authentication

FIA_UAU.1.1 The TSF shall allow **the steps specified in FIA_UAU.1/PACE, where step 2 is replaced by:**

- **to carry out the PACE protocol according to [TR-03110] of FIA_UID.1/PACE with either PIN or PUK as a password,**

or

- **to carry out the PACE protocol according to [ICAO-9303] with CAN as a password followed by VERIFY with PIN/PUK according to [PCA-eMRTD],**

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

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

FIA_UAU.4/POLY - Single-Use Authentication Mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to **in addition to FIA_UAU.4/PACE.**

1. **PACE with PIN/PUK Protocol according to [TR-03110],**
2. **Polymorphic Authentication Protocol (PMA).**

FIA_UAU.5/POLY - Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide **in addition to FIA_UAU.5.1/PACE,**

1. **PACE with PIN/PUK Protocol according to [TR-03110],**
2. **Chip Authentication Protocol v.1 according to [TR-03110],**
3. **Polymorphic Authentication Protocol(PMA),**

to support user authentication.

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

1. **Having successfully executed the polymorphic authentication protocol (PMA) after a PACE with PIN, CAv1 and TAv1, the TOE returns the randomised PI, PP or CPI values.**

FIA_UAU.6/POLY - Re-Authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the PACE with PIN/PUK, CAv1, TAv1 and PMA shall be verified as being sent by an authorized Polymorphic Authentication Terminal/Service**.

FIA_UAU.6/EAC - Re-Authenticating

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

9.1.5 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:

1. **Initialization,**
2. **Pre-personalisation,**
3. **Personalisation,**
4. **Configuration,**
5. **Resume and Unblock the PIN and PUK,**
6. **Basic Access Control expiration,**
7. **Activate and deactivate DBI.**

Application Note: This SFR is an extension of the SFR 'FMT_SMF.1' defined in [PACE-PP]. It is here refined by including mechanisms for PIN management (Resume and unblock the PIN and PUK). This extension does not conflict with the strict conformance to PACE PP and EAC PP.

FMT_SMR.1/PACE - Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles

1. **Personalisation Agent,**
2. **Terminal,**
3. **PACE authenticated BIS-PACE**
4. **Country Verifying Certificate Authority,**
5. **Document Verifier,**
6. **Domestic Extended Inspection System,**
7. **Foreign Extended Inspection System,**
8. **Manufacturer.**

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

Application Note: This SFR also applies to the refinement of the role Manufacturer.

FMT_MOF.1/BAC_EXP - Management Of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **enable** the functions **deactivation of BAC protocol** to **Country Verifying Certification Authority and Domestic Document Verifier once the current date in the TOE has reached or passed the value set by FMT_MTD.1/BAC_EXP**.

Application Note: The BAC is automatically deactivated by the TOE once the authenticated subject (CVCA or Domestic Document Verifier) has updated the current date of the TOE with a date that reaches or passes the reference date configured by FMT_MTD.1/BAC_EXP

FMT_MTD.1/BAC_EXP - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **set** the **BAC expiry date** to **personalisation agent**.

Application Note: By default, BAC expiration feature is not activated.

FMT_MTD.1/INI_ENA - Management Of Tsf Data

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

FMT_MTD.1/CVCA_INI - Management Of Tsf Data

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

1. **initial Country Verifying Certification Authority Public Key,**
2. **initial Country Verifying Certification Authority Certificate,**
3. **Initial Current Date,**
4. **none**

to **the Personalisation Agent**.

FMT_MTD.1/CVCA_UPD - Management Of Tsf Data

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

1. **Country Verifying Certification Authority Public Key,**
2. **Country Verifying Certification Authority Certificate**

to **Country Verifying Certification Authority**.

FMT_MTD.1/AAPK - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **load or create** the **Active Authentication private key** to **the personalisation agent**.

FMT_MTD.1/DATE - Management Of Tsf Data

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

1. **Document Verifier**
2. **Domestic Extended Inspection System**

FMT_MTD.1/PA - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **write** the **document Security Object (SO_D)** to **the Personalisation Agent**.

FMT_MTD.1/KEY_READ - Management Of Tsf Data

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

1. **PACE passwords,**
2. **Manufacturer Keys,**
3. **Pre-personalisation Agent Keys,**
4. **Personalisation Agent Keys,**
5. **Chip Authentication Private Key,**
6. **the ephemeral secret ephemeral key k used to randomize the PI/PP and/or the CPI data as part of the Polymorphic Authentication protocol**

to **none**.

Application Note: This SFR covers the definition in EAC PP [EAC-PP-V2] and extends it by 6. the ephemeral private key K as part of the Polymorphic Authentication protocol used to randomize the

PI/PP and/or the CPI data. Further, in this ST the PIN/PUK code can be used as a PACE password. This extension does not conflict with the strict conformance to PACE PP and EAC PP.

FMT_MTD.1/CAPK - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **load or create** the **Chip Authentication private key** to **the personalisation agent**.

FMT_MTD.1/Initialize_PIN - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **write** the **initial PIN and PUK according to [TR-03110]** to **the Polymorphic Personalisation Agent**.

Application Note: This SFR is included from [EACv2-PP] for PIN management according to [TR-03110].

FMT_MTD.1/Change_PIN - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **change** the **blocked PIN** to **the Polymorphic eMRTD document holder (using the PUK for unblocking and changing) according to [PCA-eMRTD]**.

Application Note: This SFR is included from [EACv2-PP] for PIN management according to [TR-03110].

FMT_MTD.1/Unblock_PIN - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **unblock** the **blocked PIN** to **the Polymorphic eMRTD document holder (using the PUK for unblocking and changing) according to [PCA-eMRTD]**.

Application Note: This SFR is included from [EACv2-PP] for PIN management according to [TR-03110].

FMT_MTD.1/Resume_PIN - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **resume** the **suspended PIN or PUK** to **the Polymorphic eMRTD document holder**.

Application Note: This SFR is included from [EACv2-PP] for PIN/PUK management according to [TR-03110] and [PCA-eMRTD]. Resuming a PIN or PUK is a two-step procedure, subsequently using PACE with the CAN and VERIFY with the PIN or respectively the PUK.

FMT_MTD.1/LDS2_PA - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **access and write** the **SignedData structure in EF.CardSecurity** to **the Personalisation Agent**.

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 v.1 and the Access Control.**

Refinement:

The certificate chain is valid if and only if

1. 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
2. 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 Document Verifier Certificate is not before the Current Date of the TOE,
3. 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 and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of 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.

FMT_SMR.1/POLY - Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles **in addition to FMT_SMR.1/PACE**

1. **Polymorphic Authentication Terminal/Service,**
2. **Polymorphic eMRTD Document Holder**

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

FMT_LIM.1/POLY - Limited capabilities

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

1. **sensitive Polymorphic User Data (PI, PP and CPI) to be disclosed**

FMT_LIM.2/POLY - 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 does not allow:**

1. **sensitive Polymorphic User Data (PI, PP and CPI) to be disclosed**

FMT_MTD.1/PI_PP_CPI_Load - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **load** the **PI, PP and CPI data** to **personalisation agent**.

Application Note: This SFR is added to restrict the ability to load the PI, PP and CPI to the Personalisation Agent only. The verb 'load' means here that the PI, PP and CPI data are generated securely outside the TOE and written into the TOE memory. The TOE supports only secure loading of the PI, PP and CPI data.

FMT_MTD.1/PI_PP_CPI_Read - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **read** the **PI, PP and CPI data stored on the TOE** to **none**.

Application Note: This SFR is added to restrict the ability to read the PP, PI and optional CPI data to none.

FMT_MTD.1/PINPUK - Management Of Tsf Data

FMT_MTD.1.1 The TSF shall restrict the ability to **set** the **retry value for PIN and PUK** to **personalisation agent**.

FMT_MTD.1/Activate_DBI - Management Of Tsf Data

FMT_MTD.1.1/Activate_DBI The TSF shall restrict the ability to **digitally blur** the **images in EF DG1 to EF DG8** to the **personalisation agent**.

Application Note:

Even though practically EF DG2, EF DG3 and EF DG 4 will be the files which will be directly acted upon by the personalization agent but since the implementation is not restricted to only these files, so EF DG1 to EF DG 8 is also mentioned in above instantiation.

FMT_MTD.1/Deactivate_DBI - Management Of Tsf Data

FMT_MTD.1.1/Deactivate_DBI The TSF shall restrict the ability to **remove the blurring on** the **digital images** to **the terminal whose name is set by the personalisation agent**.

FMT_MTD.1/DBI_Terminal - Management Of Tsf Data

FMT_MTD.1.1/DBI_Terminal The TSF shall restrict the ability to **set** the **name (or beginning of the name) of the terminal allowed to remove the digital blurring in phase 7, and identifiers of these files** to **personalisation agent**.

FMT_LIM.1 - Limited capabilities

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced **deploying test features after TOE delivery do not allow**

1. **User Data to be manipulated and disclosed,**
2. **TSF data to be manipulated or disclosed,**

3. **software to be reconstructed,**
4. **substantial information about construction of TSF to be gathered which may enable other attacks,**
5. **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**

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

9.1.6 FPT : Protection of the TSF

FPT_EMS.1 - TOE Emanation

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

1. **Chip Authentication Session Keys**
2. **PACE session Keys (PACE-K MAC, PACE-KEnc),**
3. **the ephemeral private key ephem SK PICC-PACE,**
4. **Active Authentication Private Key,**
5. **Personalisation Agent Key(s),**
6. **Chip Authentication Private Key,**
7. **Modular inverse of the CA key**
8. **PIN, PUK,**
9. **PI, PP and CPI,**
10. **The ephemeral random secret key k used for PI, PP and CPI randomisation as part of the Polymorphic Authentication protocol.**

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

1. **Chip Authentication Session Keys**
2. **PACE session Keys (PACE-K MAC, PACE-KEnc),**
3. **the ephemeral private key ephem SK PICC-PACE,**
4. **Active Authentication Private Key,**
5. **Personalisation Agent Key(s),**
6. **Chip Authentication Private Key,**

7. **Modular inverse of the CA key**
8. **PIN, PUK,**
9. **PI, PP and CPI,**
10. **The ephemeral random secret key k used for PI, PP and CPI randomisation as part of the Polymorphic Authentication protocol.**

Application Note: This SFR covers the definition in EAC PP [EAC-PP-V2] and extends it by PIN/PUK, PI/PP/CPI data and the ephemeral private key K as part of the Polymorphic Authentication protocol aspects. This extension does not conflict with the strict conformance to EAC PP and PACE PP.

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:

1. **Exposure to operating conditions causing a TOE malfunction,**
2. **Failure detected by TSF according to FPT_TST.1,**
3. **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

1. **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**.

9.1.7 FTP : Trusted Path

FTP_ITC.1/PACE - Inter-Tsf Trusted Channel

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

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

Application Note: In FTP_ITC.1.3/PACE, the word "initiate" is changed to 'enforce", as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel. This refinement does not conflict with the strict conformance to PACE PP and EAC PP.

9.1.8 FPR : Privacy

FPR_ANO.1 - Anonymity

FPR_ANO.1.1 [Editorially Refined]

The TSF shall ensure that **no subjects** are able to determine the real user name bound to **the eMRTD Polymorphic Holder.**

Application Note: The identity of the polymorphic eMRTD document holder is never connected with the non-randomized content of his/her PI, PP and CPI data.

FPR_UNL.1 - Unlinkability

FPR_UNL.1.1 The TSF shall ensure that **Attacker and/or Authentication Terminal/Service** are unable to determine whether **the Polymorphic Authentication response and eMRTD are related as follows: none**.

9.2 Security Assurance Requirements

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_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.

9.2.1.5 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.

9.2.2 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_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.

9.2.3.6 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_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.

9.2.4.2 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.

9.2.4.3 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.

9.2.4.4 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_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.

9.2.4.6 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.

9.2.4.7 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 Security Objectives for the TOE

9.3.1.1 Security Objectives listed in PP PACE

OT.Data_Integrity

The security objective OT.Data_Integrity "Integrity of personal data" requires the TOE to protect the integrity of the logical travel document stored on the travel 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 travel 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 travel document (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SO_D 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 v.1, and Terminal Authentication v.1. 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 travel document data after Chip Authentication v.1. The SFR FIA_UAU.6/EAC and FDP_UIT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 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.

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 v.1 (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 SO_D 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.

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 and 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 v.1 (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. 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 SO_D 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.

OT.Tracing

The security objective OT.Tracing aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel 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 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 SO_D is card-individual) – FTP_ITC.1/PACE.

OT.Prot_Abuse-Func

The security objective OT.Prot_Abuse-Func "Protection against Abuse of Functionality" is ensured by the SFR FMT_LIM.1, FMT_LIM.2, FMT_LIM.1/POLY and FMT_LIM.2/POLY 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 travel 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.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.AC_Pers

The security objective OT.AC_Pers "Access Control for Personalisation of logical travel document" addresses the access control of the writing the logical travel 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 travel 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 travel document only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SO_D 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 v.1 (after Chip Authentication v.1) 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 v.1), 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 v.1) 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.

9.3.1.2 Additional Security Objectives from PP EAC

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) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 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 v.1 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_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. 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.

OT.Chip_Auth_Proof

The security objective OT.Chip_Auth_Proof "Proof of travel document's chip authenticity" is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1/CA proving the identity of the TOE. The Chip Authentication Protocol v.1 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 v.1 [TR-03110] 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.

9.3.1.3 Security Objectives related to Polymorphic eMRTD

OT.Polymorphic_Data_Confidentiality

SFRs that contribute to meet this objective are mentioned in the table 'SFR vs Security Objectives'.

OT.Polymorphic_Data_Integrity

SFRs that contribute to meet this objective are mentioned in the table 'SFR vs Security Objectives'.

OT.Polymorphic_Data_Authenticity

SFRs that contribute to meet this objective are mentioned in the table 'SFR vs Security Objectives'.

OT.Polymorphic_Data_Privacy

SFRs that contribute to meet this objective are mentioned in the table 'SFR vs Security Objectives'.

OT.AC_Pers_Polymorphic

SFRs that contribute to meet this objective are mentioned in the table 'SFR vs Security Objectives'.

9.3.1.4 Additional Security Objectives related to LDS2 extension

OT.LDS2_Data_Confidentiality

SFRs that contribute to meet this objective are mentioned in the table 'SFR vs Security Objectives'.

OT.AC_Pers_LDS2

SFRs that contribute to meet this objective are mentioned in the table 'SFR vs Security Objectives'.

9.3.1.5 Additional Security Objectives for the TOE

OT.Chip_Auth_Proof_PACE_CAM

OT.Chip_Auth_Proof_PACE_CAM aims to ensure the authenticity of the electronic document's chip by the PACE-CAM protocol. This is supported by FCS_CKM.1/CAM for cryptographic key-generation, and FCS_COP.1/CAM for the implementation itself, as well as FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE_CAM and FIA_UAU.5/PACE_CAM and FIA_UAU.6/PACE_CAM, the latter supporting the PACE protocol.

OT.AA_Proof

The security objective OT.AA_Proof is ensured by the Active Authentication Protocol as defined in FIA_API.1/AA. The FCS_CKM.1/AA provides key generation for Active Authentication. 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/AAPK.

OT.BAC_Expiration

The security objective OT.BAC_Expiration "Automatic deactivation of BAC protocol" is ensured by the SFR FMT_SMF.1 and detailed in FMT_MOF.1/BAC_EXP regarding mechanism activation and FMT_MTD.1/BAC_EXP regarding mechanism configuration.

OT.DBI

OT.DBI is met by FMT_MTD.1/Activate_DBI that allows the personalization agent to digitally blur the images in defined EFs. FMT_MTD.1/DBI_Terminal helps to ensure that only an authorized terminal whose name is set by the personalization agent can remove the blurring as defined in FMT_MTD.1/Deactivate_DBI.

FMT_SMF.1 provides the necessary management functions based on the roles identified in FMT_SMR.1/PACE.

9.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.Data_Integrity	FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/PACE_MAC, FCS_RND.1, FDP_RIP.1, FDP_UIT.1/TRM, FDP_ACF.1/TRM, FDP_ACC.1/TRM, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/EAC, FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK, FPT_PHP.3, FTP_ITC.1/PACE, FCS_CKM.1/CAM	Rationale
OT.Data_Authenticity	FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/PACE_MAC, FCS_RND.1, FDP_RIP.1, FIA_UID.1/PACE, FIA_UAU.1/PACE,	Rationale

	FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/EAC, FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FTP_ITC.1/PACE, FCS_CKM.1/CAM	
OT.Data_Confidentiality	FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_ENC, FCS_COP.1/PACE_ENC, FCS_RND.1, FDP_RIP.1, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FDP_ACF.1/TRM, FDP_ACC.1/TRM, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/EAC, FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FTP_ITC.1/PACE, FCS_CKM.1/CAM	Rationale
OT.Tracing	FIA_AFL.1/PACE, FTP_ITC.1/PACE	Rationale
OT.Prot_Abuse-Func	FMT_LIM.1, FMT_LIM.2, FMT_LIM.1/POLY, FMT_LIM.2/POLY	Rationale
OT.Prot_Inf_Leak	FPT_EMS.1, FPT_FLS.1, FPT_PHP.3, FPT_TST.1	Rationale
OT.Prot_Phys-Tamper	FPT_PHP.3	Rationale
OT.Prot_Malfunction	FPT_TST.1, FPT_FLS.1	Rationale
OT.Identification	FAU_SAS.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_SMF.1, FMT_SMR.1/PACE	Rationale
OT.AC_Pers	FAU_SAS.1, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/SIG_VER, FCS_RND.1, FDP_ACF.1/TRM, FDP_ACC.1/TRM, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FPT_EMS.1	Rationale
OT.Sens_Data_Conf	FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/SIG_VER, FCS_RND.1, FDP_UCT.1/TRM, FDP_ACF.1/TRM, FDP_ACC.1/TRM, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK, FMT_MTD.3	Rationale
OT.Chip_Auth_Proof	FCS_CKM.1/CA, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FIA_API.1/CA, FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK	Rationale
OT.Polymorphic_Data_Confidentiality	FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.1/POLY, FCS_CKM.4, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC,	Rationale

	FCS_COP.1/SIG_VER, FCS_COP.1/POLY, FCS_RND.1, FDP_RIP.1, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FDP_ACF.1/TRM, FDP_ACC.1/TRM, FDP_ACC.1/POLY, FDP_ACF.1/POLY, FDP_RIP.1/POLY, FIA_AFL.1/PINPUK, FIA_UID.1/POLY, FIA_UAU.1/POLY, FIA_UAU.4/POLY, FIA_UAU.5/POLY, FIA_UAU.6/POLY, FIA_UAU.6/EAC, FMT_SMF.1, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/AAPK, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.3, FMT_SMR.1/POLY, FMT_MTD.1/PI_PP_CPI_Load , FMT_MTD.1/PI_PP_CPI_Read , FTP_ITC.1/PACE, FMT_MTD.1/PINPUK	
OT.Polymorphic_Data_Integrity	FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.1/POLY, FCS_CKM.4, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/POLY, FCS_RND.1, FDP_RIP.1, FDP_UIT.1/TRM, FDP_ACF.1/TRM, FDP_ACC.1/TRM, FDP_ACC.1/POLY, FDP_ACF.1/POLY, FDP_RIP.1/POLY, FIA_AFL.1/PINPUK, FIA_UID.1/POLY, FIA_UAU.1/POLY, FIA_UAU.4/POLY, FIA_UAU.5/POLY, FIA_UAU.6/POLY, FIA_UAU.6/EAC, FMT_SMF.1, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Resume_PIN, FMT_SMR.1/POLY, FMT_MTD.1/PI_PP_CPI_Load , FMT_MTD.1/PI_PP_CPI_Read , FPT_PHP.3, FTP_ITC.1/PACE, FMT_MTD.1/PINPUK	Rationale
OT.Polymorphic_Data_Authenticity	FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.1/POLY, FCS_CKM.4, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_COP.1/POLY, FCS_RND.1, FDP_RIP.1, FDP_RIP.1/POLY, FIA_AFL.1/PINPUK, FIA_UID.1/POLY, FIA_UAU.1/POLY, FIA_UAU.4/POLY, FIA_UAU.5/POLY, FIA_UAU.6/POLY, FIA_UAU.6/EAC, FMT_SMF.1, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Resume_PIN, FMT_SMR.1/POLY, FTP_ITC.1/PACE, FMT_MTD.1/PINPUK	Rationale
OT.Polymorphic_Data_Privacy	FCS_CKM.1/DH_PACE, FCS_CKM.1/POLY, FCS_CKM.4, FCS_COP.1/POLY,	Rationale

	FIA_AFL.1/PINPUK, FMT_MTD.1/PI_PP_CPI_Read, FPR_ANO.1, FPR_UNL.1, FMT_MTD.1/PINPUK	
OT.AC_Pers_Polymorphic	FAU_SAS.1, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/SIG_VER, FCS_RND.1, FDP_ACF.1/TRM, FDP_ACC.1/TRM, FDP_ACC.1/POLY, FDP_ACF.1/POLY, FIA_AFL.1/PINPUK, FIA_UID.1/POLY, FIA_UAU.1/POLY, FIA_UAU.4/POLY, FIA_UAU.5/POLY, FIA_UAU.6/POLY, FIA_UAU.6/EAC, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Resume_PIN, FMT_SMR.1/POLY, FMT_MTD.1/PI_PP_CPI_Load, FMT_MTD.1/PI_PP_CPI_Read, FPT_EMS.1, FMT_MTD.1/PINPUK	Rationale
OT.LDS2_Data_Confidentiality	FCS_CKM.1/CA, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_COP.1/SIG_VER, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/EAC, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK, FMT_MTD.1/LDS2_PA, FMT_MTD.3, FTP_ITC.1/PACE, FDP_ACC.1/LDS2, FDP_ACF.1/LDS2	Rationale
OT.AC_Pers_LDS2	FAU_SAS.1, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/SIG_VER, FCS_RND.1, FDP_ACC.1/LDS2, FDP_ACF.1/LDS2, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FMT_MTD.1/LDS2_PA, FPT_EMS.1	Rationale
OT.Chip_Auth_Proof_PACE_CAM	FCS_COP.1/CAM, FCS_CKM.1/CAM, FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM, FIA_UAU.6/PACE_CAM	Rationale
OT.AA_Proof	FCS_COP.1/AA, FCS_RND.1, FIA_API.1/AA, FMT_MTD.1/AAPK, FCS_CKM.1/AA	Rationale
OT.BAC_Expiration	FMT_SMF.1, FMT_MOF.1/BAC_EXP, FMT_MTD.1/BAC_EXP	Rationale
OT.DBI	FMT_MTD.1/Activate_DBI, FMT_MTD.1/Deactivate_DBI, FMT_MTD.1/DBI_Terminal, FMT_SMF.1, FMT_SMR.1/PACE	Rationale

Table 25 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FAU_SAS.1	OT.Identification, OT.AC_Pers, OT.AC_Pers_Polymorphic, OT.AC_Pers_LDS2
FCS_CKM.1/DH_PACE	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.Polymorphic_Data_Privacy
FCS_CKM.1/CA	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic, OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2
FCS_CKM.1/AA	OT.AA_Proof
FCS_CKM.1/CAM	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Chip_Auth_Proof_PACE_CAM
FCS_CKM.1/POLY	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.Polymorphic_Data_Privacy
FCS_CKM.4	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.Polymorphic_Data_Privacy, OT.AC_Pers_Polymorphic, OT.AC_Pers_LDS2
FCS_COP.1/AA	OT.AA_Proof
FCS_COP.1/CAM	OT.Chip_Auth_Proof_PACE_CAM
FCS_COP.1/CA_MAC	OT.Data_Integrity, OT.AC_Pers, OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic, OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2
FCS_COP.1/CA_ENC	OT.Data_Integrity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic, OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2
FCS_COP.1/PACE_ENC	OT.Data_Confidentiality, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Authenticity, OT.LDS2_Data_Confidentiality
FCS_COP.1/PACE_MAC	OT.Data_Integrity, OT.Data_Authenticity, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Authenticity, OT.LDS2_Data_Confidentiality
FCS_COP.1/SIG_VER	OT.AC_Pers, OT.Sens_Data_Conf, OT.Polymorphic_Data_Confidentiality, OT.AC_Pers_Polymorphic, OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2

FCS_COP.1/POLY	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.Polymorphic_Data_Privacy
FCS_RND.1	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic, OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2, OT.AA_Proof
FDP_RIP.1	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity
FDP_UCT.1/TRM	OT.Data_Confidentiality, OT.Sens_Data_Conf, OT.Polymorphic_Data_Confidentiality
FDP_UIT.1/TRM	OT.Data_Integrity, OT.Data_Confidentiality, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity
FDP_ACC.1/TRM	OT.Data_Integrity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.AC_Pers_Polymorphic
FDP_ACF.1/TRM	OT.Data_Integrity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.AC_Pers_Polymorphic
FDP_ACC.1/POLY	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.AC_Pers_Polymorphic
FDP_ACF.1/POLY	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.AC_Pers_Polymorphic
FDP_RIP.1/POLY	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity
FDP_ACC.1/LDS2	OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2
FDP_ACF.1/LDS2	OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2
FIA_UID.1/PACE_CAM	OT.Chip_Auth_Proof_PACE_CAM
FIA_UAU.1/PACE_CAM	OT.Chip_Auth_Proof_PACE_CAM
FIA_UAU.4/PACE_CAM	OT.Chip_Auth_Proof_PACE_CAM
FIA_UAU.5/PACE_CAM	OT.Chip_Auth_Proof_PACE_CAM
FIA_UAU.6/PACE_CAM	OT.Chip_Auth_Proof_PACE_CAM
FIA_AFL.1/PACE	OT.Tracing
FIA_UID.1/PACE	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2
FIA_UAU.1/PACE	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2
FIA_UAU.4/PACE	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2

FIA_UAU.5/PACE	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2
FIA_UAU.6/PACE	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.LDS2_Data_Confidentiality
FIA_API.1/AA	OT.AA_Proof
FIA_API.1/CA	OT.Chip_Auth_Proof
FIA_AFL.1/PINPUK	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.Polymorphic_Data_Privacy, OT.AC_Pers_Polymorphic
FIA_UID.1/POLY	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic
FIA_UAU.1/POLY	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic
FIA_UAU.4/POLY	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic
FIA_UAU.5/POLY	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic
FIA_UAU.6/POLY	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic
FIA_UAU.6/EAC	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic, OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2
FMT_SMF.1	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Identification, OT.AC_Pers, OT.Chip_Auth_Proof, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_LDS2, OT.BAC_Expiration, OT.DBI
FMT_SMR.1/PACE	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Identification, OT.AC_Pers, OT.Chip_Auth_Proof, OT.AC_Pers_LDS2, OT.DBI
FMT_MOF.1/BAC_EXP	OT.BAC_Expiration
FMT_MTD.1/BAC_EXP	OT.BAC_Expiration
FMT_MTD.1/INI_ENA	OT.Identification, OT.AC_Pers, OT.AC_Pers_Polymorphic, OT.AC_Pers_LDS2
FMT_MTD.1/INI_DIS	OT.Identification, OT.AC_Pers, OT.AC_Pers_Polymorphic, OT.AC_Pers_LDS2
FMT_MTD.1/CVCA_INI	OT.Sens_Data_Conf, OT.Polymorphic_Data_Confidentiality, OT.LDS2_Data_Confidentiality
FMT_MTD.1/CVCA_UPD	OT.Sens_Data_Conf, OT.Polymorphic_Data_Confidentiality, OT.LDS2_Data_Confidentiality

FMT_MTD.1/AAPK	OT.Polymorphic_Data_Confidentiality, OT.AA_Proof
FMT_MTD.1/DATE	OT.Sens_Data_Conf, OT.LDS2_Data_Confidentiality
FMT_MTD.1/PA	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.AC_Pers, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic, OT.AC_Pers_LDS2
FMT_MTD.1/KEY_READ	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic, OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2
FMT_MTD.1/CAPK	OT.Data_Integrity, OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.LDS2_Data_Confidentiality
FMT_MTD.1/Initialize_PIN	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic
FMT_MTD.1/Change_PIN	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic
FMT_MTD.1/Unblock_PIN	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic
FMT_MTD.1/Resume_PIN	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic
FMT_MTD.1/LDS2_PA	OT.LDS2_Data_Confidentiality, OT.AC_Pers_LDS2
FMT_MTD.3	OT.Sens_Data_Conf, OT.Polymorphic_Data_Confidentiality, OT.LDS2_Data_Confidentiality
FMT_SMR.1/POLY	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.AC_Pers_Polymorphic
FMT_LIM.1/POLY	OT.Prot_Abuse-Func
FMT_LIM.2/POLY	OT.Prot_Abuse-Func
FMT_MTD.1/PI_PP_CPI_Load	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.AC_Pers_Polymorphic
FMT_MTD.1/PI_PP_CPI_Read	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Privacy, OT.AC_Pers_Polymorphic
FMT_MTD.1/PINPUK	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.Polymorphic_Data_Privacy, OT.AC_Pers_Polymorphic
FMT_MTD.1/Activate_DBI	OT.DBI
FMT_MTD.1/Deactivate_DBI	OT.DBI
FMT_MTD.1/DBI_Terminal	OT.DBI
FMT_LIM.1	OT.Prot_Abuse-Func
FMT_LIM.2	OT.Prot_Abuse-Func

FPT_EMS.1	OT.Prot_Inf_Leak, OT.AC_Pers, OT.AC_Pers_Polymorphic, OT.AC_Pers_LDS2
FPT_FLS.1	OT.Prot_Inf_Leak, OT.Prot_Malfunction
FPT_PHP.3	OT.Data_Integrity, OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper, OT.Polymorphic_Data_Integrity
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, OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Integrity, OT.Polymorphic_Data_Authenticity, OT.LDS2_Data_Confidentiality
FPR_ANO.1	OT.Polymorphic_Data_Privacy
FPR_UNL.1	OT.Polymorphic_Data_Privacy

Table 26 SFRs and Security Objectives - Coverage

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_COP.1/CA_ENC,FCS_COP.1/CA_MAC,FCS_CKM.4
FCS_CKM.1/AA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4,FCS_COP.1/AA
FCS_CKM.1/CAM	(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/POLY	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/POLY,FCS_CKM.4
FCS_CKM.4	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1/DH_PACE,FCS_CKM.1/CA,FCS_CKM.1/AA,FCS_CKM.1/POLY
FCS_COP.1/AA	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FCS_CKM.1/AA,FCS_CKM.4
FCS_COP.1/CAM	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FCS_CKM.1/CA,FCS_CKM.4
FCS_COP.1/CA_MAC	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FCS_CKM.1/CA,FCS_CKM.4
FCS_COP.1/CA_ENC	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FCS_CKM.1/CA,FCS_CKM.4
FCS_COP.1/PACE_ENC	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE,FCS_CKM.4
FCS_COP.1/PACE_MAC	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FCS_CKM.1/CA,FCS_CKM.4

FCS_COP.1/SIG_VER	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FCS_CKM.1/CA,FCS_CKM.4
FCS_COP.1/POLY	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FCS_CKM.1/POLY,FCS_CKM.4
FCS_RND.1	No Dependencies	
FDP_RIP.1	No Dependencies	
FDP_UCT.1/TRM	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FTP_ITC.1/PACE,FDP_ACC.1/TRM
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/TRM	(FDP_ACF.1)	FDP_ACF.1/TRM
FDP_ACF.1/TRM	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/TRM
FDP_ACC.1/POLY	(FDP_ACF.1)	FDP_ACF.1/POLY
FDP_ACF.1/POLY	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/POLY
FDP_RIP.1/POLY	No Dependencies	
FDP_ACC.1/LDS2	(FDP_ACF.1)	FDP_ACF.1/LDS2
FDP_ACF.1/LDS2	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/LDS2
FIA_UID.1/PACE_CAM	No Dependencies	
FIA_UAU.1/PACE_CAM	(FIA_UID.1)	FIA_UID.1/PACE_CAM
FIA_UAU.4/PACE_CAM	No Dependencies	
FIA_UAU.5/PACE_CAM	No Dependencies	
FIA_UAU.6/PACE_CAM	No Dependencies	
FIA_AFL.1/PACE	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_UID.1/PACE	No Dependencies	
FIA_UAU.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FIA_UAU.4/PACE	No Dependencies	
FIA_UAU.5/PACE	No Dependencies	
FIA_UAU.6/PACE	No Dependencies	
FIA_API.1/AA	No Dependencies	
FIA_API.1/CA	No Dependencies	
FIA_AFL.1/PINPUK	(FIA_UAU.1)	FIA_UAU.1/POLY
FIA_UID.1/POLY	No Dependencies	
FIA_UAU.1/POLY	(FIA_UID.1)	FIA_UID.1/POLY
FIA_UAU.4/POLY	No Dependencies	
FIA_UAU.5/POLY	No Dependencies	
FIA_UAU.6/POLY	No Dependencies	
FIA_UAU.6/EAC	No Dependencies	
FMT_SMF.1	No Dependencies	
FMT_SMR.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FMT_MOF.1/BAC_EXP	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/BAC_EXP	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/INI_ENA	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE

FMT_MTD.1/INI_DIS	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/CVCA_INI	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/AAPK	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/DATE	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/PA	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/CAPK	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/Initialize_PIN	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/Change_PIN	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/Unblock_PIN	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/Resume_PIN	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/LDS2_PA	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.3	(FMT_MTD.1)	FMT_MTD.1/INI_ENA,FMT_MTD.1/INI_DIS,FMT_MTD.1/PA,FMT_MTD.1/CVCA_INI,FMT_MTD.1/CVCA_UPD,FMT_MTD.1/DATE,FMT_MTD.1/CAPK,FMT_MTD.1/KEY_READ
FMT_SMR.1/POLY	(FIA_UID.1)	FIA_UID.1/POLY
FMT_LIM.1/POLY	(FMT_LIM.2)	FMT_LIM.2/POLY
FMT_LIM.2/POLY	(FMT_LIM.1)	FMT_LIM.1/POLY
FMT_MTD.1/PI_PP_CPI_Load	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMR.1/POLY,FMT_SMF.1
FMT_MTD.1/PI_PP_CPI_Read	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMR.1/POLY,FMT_SMF.1
FMT_MTD.1/PINPUK	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMR.1/POLY,FMT_SMF.1
FMT_MTD.1/Activate_DBI	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/Deactivate_DBI	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_MTD.1/DBI_Terminal	(FMT_SMR.1) and (FMT_SMF.1)	FMT_SMF.1,FMT_SMR.1/PACE
FMT_LIM.1	(FMT_LIM.2)	FMT_LIM.2
FMT_LIM.2	(FMT_LIM.1)	FMT_LIM.1
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	
FPR_ANO.1	No Dependencies	
FPR_UNL.1	No Dependencies	

Table 27 SFRs Dependencies Rationale for the exclusion of Dependencies

The dependency FMT_MSA.3 of FDP_ACF.1/TRM is discarded. The dependency FMT_MSA.3 of FDP_ACF.1/TRM is discarded. 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 personalization, 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/POLY is discarded. The dependency FMT_MSA.3 of FDP_ACF.1/POLY is discarded. The access control TSF according to FDP_ACF.1/POLY uses security attributes that have been defined during personalization, 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/LDS2 is discarded. The dependency FMT_MSA.3 of FDP_ACF.1/LDS2 is discarded. The access control TSF according to FDP_ACF.1/LDS2 uses security attributes that have been defined during personalization, 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.

9.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.1,ADV_TDS.1,
ADV_FSP.5	(ADV_TDS.1) and (ADV_IMP.1)	ADV_TDS.1,ADV_IMP.1,
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3,ALC_TAT.1,
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	ADV_IMP.1,ADV_TDS.3,ALC_TAT.1,
ADV_TDS.4	(ADV_FSP.5)	ADV_FSP.5,
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.1,
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.1,ALC_DVS.1,ALC_LCD.1,
ALC_CMS.5	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.2	(ADV_IMP.1)	ADV_IMP.1,
ASE_INT.1	No Dependencies	
ASE_CCL.1	(ASE_INT.1) and (ASE_ECD.1) and (ASE_REQ.1)	ASE_INT.1,ASE_ECD.1,ASE_REQ.1,
ASE_SPD.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1,
ASE_ECD.1	No Dependencies	
ASE_REQ.2	(ASE_OBJ.2) and (ASE_ECD.1)	ASE_OBJ.2,ASE_ECD.1,
ASE_TSS.1	(ASE_INT.1) and (ASE_REQ.1) and (ADV_FSP.1)	ASE_INT.1,ASE_REQ.1,ADV_FSP.1,
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.2,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.1,
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.2,AGD_OPE.1,AGD_PRE.1,ATE_COV.1,ATE_FUN.1,
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_TDS.3) and (ADV_IMP.1) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1,ADV_FSP.4,ADV_TDS.3,ADV_IMP.1,AGD_OPE.1,AGD_PRE.1,ATE_DPT.1,

Table 28 SARs Dependencies Rationale for the Security Assurance Requirements

The EAL5 was chosen to permits a developer to gain maximum assurance from positive security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

9.3.4 ALC_DVS.2

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.

9.3.5 AVA_VAN.5

The selection of the component AVA_VAN.5 provides the assurance that the TOE is shown to be highly resistant to penetration attacks to meet the security objectives OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper and OT.Prot_Malfunction.

10 TOE Summary Specification

10.1 TOE Summary Specification

10.1.1 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-personalization Agent keys,
- Personalization Agent keys,
- CA private key,
- PACE passwords and
- Ephemeral secret ephemeral key k used to randomize the PI/PP and/or the CPI data as part of the Polymorphic Authentication protocol.

It controls access to the Initialization and Pre-Personalization data by allowing read access without authentication prior to delivery. After delivery, only the personalization 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 based on the access control policies defined in [ICAO-9303].
- Nobody should have access to the name bound to the Polymorphic eMRTD holder.
- Nobody should be able to read PI, PP and CPI data stored on the TOE.
- The read access to the extended LDS2 applications is based on the access conditions defined in [9303-10_LDS2].

In the Production and preparation stage:

The Manufacturer can read the Initialization Data in Stage 2 “Production”. The pre-personalization agent and the Personalization 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.

10.1.2 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) as imposed by [ICAO-9303]. 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.

Only the polymorphic eMRTD holder is allowed to change and unblock the blocked PIN as well as resume the suspended PIN/PUK.

For the extended LDS2 applications only after a successful PACE authentication followed by a Chip Authentication and Terminal Authentication, a user can append to the VISA records and write to the EFs in additional biometric records based on the access conditions defined in [9303-10_LDS2].

In the Production and preparation stage:

The Manufacturer can write all the Initialization and data for the Pre-personalization. The Personalization 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-Personalization Agent can write through a valid secure channel data to be used by the personalization agent (after it is authenticated by the TOE using its authentication keys). The Pre-personalization agent is only active after delivery. The key that is written in the TOE for authentication purposes during manufacturing in meant for the pre-personalizaiton agent. the Pre-personalization agent (which is seen as a sub-role of thep Personalization agent) will refresh this key. The personalization agent is allowed to write the initial values of PIN and PUK. The personalization agent is allowed to access and write SignedData in EF.CardSecurity.

10.1.3 F.AA - Active Authentication

This security functionality ensures the Active Authentication is performed as described in [ICAO-9303] (if it is activated by the personalizer).

10.1.4 F.CLR_INFO - Clear Residual Information

This security function ensures clearing of sensitive information

1. Authentication state is securely cleared in case an error is detected or a new authentication is attempted
2. Authentication data related to Active Authentication, PACE authentication, EAC and Polymorphic eMRTD holder authentication data is securely cleared to prevent reuse
3. Session keys are securely erased in case an error is detected or the secure communication session is closed
4. ephem-SK picc-PACE is securely erased,
5. the randomized PI, PP and optional CPI is securely cleared,

6. the ephemeral (random) secret key k, used for the randomisation during the execution of the Polymorphic Authentication protocol is securely erased.

10.1.5 F.CRYPTO - Cryptographic Support

This Security Function provides the following cryptographic features:

1. Key generation based on ECDH compliant to [TR_03111] with key sizes 192, 224, 256, 320, 384, 512 and 521 bits in combination with 112 bits 3DES or 128, 192 or 256 bits AES.
2. Key generation based on DH with key size 2048 bits.
3. Key generation using ECC with key sizes 320, 384 and 512 bits.
4. RSA key pair generation with key sizes 1536, 1792, 2048, 2560, 3072, 3584 and 4096
5. EC key pair generation with key sizes 192, 224, 256, 320, 384, 512 and 521
6. 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).
7. Secure messaging (message authentication code) using:
    - Triple DES Retail MAC with key size 112 bits.
    - AES CMAC with key sizes 128,192 and 256 bits.
8. Digital signature verification using:
    - ECDSA with SHA1, SHA224, SHA256, SHA384, SHA512 with key sizes 192 to 521 bits.
    - RSA with SHA-1, SHA-256 and SHA-512 with key sizes 1280, 1536, 1792, 2048, 2560, 3072, 3584 and 4096 bits.
9. Digital signature generation using:
    - ECDSA with key sizes 192 to 521 bits.
    - RSA with key sizes 1536, 1792, 2048, 2560, 3072, 3584 and 4096 bits.
10. PACE-CAM Protocol with EC key sizes 192 to 521 bits.
11. Deterministic random number generation specified by FCS_RNG.1 Quality metric for random numbers of [PTF-ST].
12. PI, PP and optional CPI randomization according to ECC with key sizes 320, 384 and 512 bits.

10.1.6 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]. It also provides the following management functions:

1. Maintain the roles: Document Verifier, CVCA, Domestic EIS, Foreign EIS,
2. Limit the ability to update the CVCA Public key and CVCA Certificate to the Country Verifying Certification Authority,

3. Limit the ability to update the date to CVCA, Document Verifier and Domestic Extended Inspection System (also contributes to the deactivation of BAC protocol),
4. Ensures only secure values are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control,
5. The terminal whose name is set by the personalization agent is allowed to remove the digital blurring on images.

10.1.7 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 wait for linear increasing time for further authentication attempts.

10.1.8 F.PERS - MRTD Personalization

This security functionality ensures that the TOE, when delivered to the Personalization Agent, provides and requires authentication for data exchange. This authentication is based on GP authentication mechanism. This security function is also responsible for management operations during personalization phase. This function allows to:

1. Configuration of the TOE
2. Write the Document Security Object (SOD),
3. Write the initial CVCA Public Key, CVCA Certificate and Current Date,
4. Load or generate Active Authentication Keys,
5. Load or generate CA Keys,
6. Write the initial PIN/PUK,
7. Digitally blur the images in EF DG1 to EF DG8,
8. Set the name (or beginning of the name) of the terminal allowed to remove the digital blurring in phase 7
9. Access and write SignedData in EF.CardSecurity,
10. Set the retry value for PIN and PUK,
11. Load user data,
12. Load the PI, PP and CPI data,
13. Configure BAC deactivation mechanism,
14. Load of key data PACE in encrypted form.

10.1.9 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 leakage via these emanations that might reveal or provide access to sensitive data.

Furthermore, it prevents deploying test features after TOE delivery.

10.1.10 F.PREP - MRTD Pre-personalization

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 GP authentication mechanism. This function allows to:

1. Manage symmetric authentication using Pre-personalization Agent keys,
2. Compute session keys to be used by F.SM,
3. Initialization of the TOE,
4. Store the Initialization and Pre-Personalization data in audit records.

10.1.11 F.POLY - Polymorphic Authentication

The TOE supports Polymorphic eMRTD extensions that can be configured using the same applet during personalisation. The polymorphic eMRTD holder is allowed to:

1. Change the blocked PIN,
2. Unblock the blocked PIN,
3. Resume the suspended PIN or PUK.

The function also maintains the following roles:

1. Polymorphic Authentication Terminal/Service,
2. Polymorphic eMRTD Document Holder

In case the number of consecutive failed authentication attempts crosses the administrator defined number defined in FIA_AFL.1/PINPUK the TSF will wait for linear increasing time for further authentication attempts.

It also ensures the attacker isn't able to identify how the authentication response and eMRTD are related to protect the TOE.

10.1.12 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, a secure channel is established. 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.

10.1.13 F.SS - Safe State Management

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

1. a tearing occurs (during a copy of data in NVM).
2. an error due to self test as defined in FPT_TST.1.
3. 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.

10.1.14 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.

10.2 SFRs and TSS

10.2.1 Security Functional Requirements

10.2.1.1 FAU : Security Audit

FAU_SAS.1

is met by F.PREP - MRTD Pre-personalization

10.2.1.2 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, EAC that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support

FCS_CKM.1/AA

is met by F.CRYPTO - Cryptographic Support

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/POLY

is met by 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/AA

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

FCS_COP.1/CAM

is met by F.PACE - Authentication using PACE that uses F.CRYPTO - Cryptographic Support to provide PACE-CAM functionality

FCS_COP.1/CA_MAC

s 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

s 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_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/SIG_VER

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

FCS_COP.1/POLY

is met by F.Crypto - Cryptographic Support

FCS_RND.1

is met by F.CRYPTO - Cryptographic Support

10.2.1.3 FDP : User Data Protection

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.

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 and F.EAC - Extended Access Control

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 and F.EAC - Extended Access Control

FDP_ACC.1/POLY

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.POLY - Polymorphic Authentication

FDP_ACF.1/POLY

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.POLY - Polymorphic Authentication

FDP_RIP.1/POLY

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

FDP_ACC.1/LDS2

is met by F.ACR - Access Control in Reading and F.ACW - Access Control in Writing that authorizes read and write access according to F.PACE - Authentication using PACE and F.EAC - Extended Access Control.

FDP_ACF.1/LDS2

is met by F.ACR - Access Control in Reading and F.ACW - Access Control in Writing that authorizes read and write access according to F.PACE - Authentication using PACE and F.EAC - Extended Access Control.

10.2.1.4 FIA : Identification and Authentication

FIA_UID.1/PACE_CAM

is met by F.PACE - Authentication using PACE that provides PACE authenticaton with all mappings

FIA_UAU.1/PACE_CAM

is met by F.PACE - Authentication using PACE that provides PACE authenticaton with all mappings

FIA_UAU.4/PACE_CAM

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

FIA_UAU.5/PACE_CAM

is met by F.PACE - Authentication using PACE that provides PACE authenticaton with all mappings

FIA_UAU.6/PACE_CAM

is met by F.SM - Secure Messaging that ensures all messages are sent through secure messaging after PACE authentication (chip authentication mapping)

FIA_AFL.1/PACE

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

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, Chip Authentication and Terminal Authentication.

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, Chip Authentication and Terminal Authentication.

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 Personalization and F.PREP - MRTD Pre-personalization that provides manufacturer and personalization agent authentication.
It is also met by F.SM - Secure Messaging that provides a secure messaging channel.

FIA_UAU.6/PACE

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

FIA_API.1/AA

is met by F.AA - Active Authentication that provides Active Authentication.

FIA_API.1/CA

is met by F.EAC - Extended Access Control that provides Chip Authentication

FIA_AFL.1/PINPUK

is met by F.POLY - Polymorphic Authentication

FIA_UID.1/POLY

is met by F.POLY - Polymorphic Authentication and F.PACE - Authentication using PACE

FIA_UAU.1/POLY

is met by F.POLY - Polymorphic Authentication and F.PACE - Authentication using PACE

FIA_UAU.4/POLY

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

FIA_UAU.5/POLY

is met by F.POLY - Polymorphic Authentication, F.PACE - Authentication using PACE and F.EAC - Extended Access Control

FIA_UAU.6/POLY

is met by F.SM - Secure Messaging that ensures all messages are sent through secure messaging after 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

10.2.1.5 FMT: Security Management

FMT_SMF.1

is met by F.POLY - Polymorphic Authentication, F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that provide the required management functions.

FMT_SMR.1/PACE

is met by F.PACE - Authentication using PACE, F.EAC - Extended Access Control, F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization. These roles are maintained by means of the authentication states during the authentication mechanisms provided by the security functions.

FMT_MOF.1/BAC_EXP

is met by F.EAC - Extended Access Control

FMT_MTD.1/BAC_EXP

is met by F.PERS - MRTD Personalization

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-personalization

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-personalization

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 Personalization

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/AAPK

is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PERS - MRTD Personalization

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/PA

is met by F.PERS - MRTD Personalization

FMT_MTD.1/KEY_READ

s met by F.ACR - Access Control in Reading that ensures the secret keys are never readable

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 Personalization

FMT_MTD.1/Initialize_PIN

is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PERS - MRTD Personalization

FMT_MTD.1/Change_PIN

is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.POLY - Polymorphic Authentication

FMT_MTD.1/Unblock_PIN

is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.POLY - Polymorphic Authentication

FMT_MTD.1/Resume_PIN

is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.POLY - Polymorphic Authentication

FMT_MTD.1/LDS2_PA

is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PERS - MRTD Personalization

FMT_MTD.3

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

FMT_SMR.1/POLY

is met by F.POLY - Polymorphic Authentication that provides the authentication mechanism to authenticate the roles.

FMT_LIM.1/POLY

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/POLY

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/PI_PP_CPI_Load

is met by F.PERS - MRTD Personalization

FMT_MTD.1/PI_PP_CPI_Read

is met by F.ACE - Access Control in Reading

FMT_MTD.1/PINPUK

is met by F.Pers - MRTD Personalization that provides the personalisation agent the ability to set the retry value of PIN and PUK

FMT_MTD.1/Activate_DBI

is met by F.PERS - MRTD Personalization

FMT_MTD.1/Deactivate_DBI

is met by F.EAC - Extended Access Control, EAC

FMT_MTD.1/DBI_Terminal

is met by F.PERS - MRTD Personalization

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.

10.2.1.6 FPT : Protection of the TSF

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

10.2.1.7 FTP : Trusted Path

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.

10.2.1.8 FPR : Privacy

FPR_ANO.1

is my by F.ACR - Access Control in Reading that ensures nobody has read access to information regarding name bound to the polymorphic eMRTD Holder.

FPR_UNL.1

is met by F.POLY - Polymorphic Authentication

10.2.2 Association Tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FAU_SAS.1	F.PREP - MRTD Pre-personalization
FCS_CKM.1/DH_PACE	F.CRYPTO - Cryptographic Support, F.PACE - Authentication using PACE
FCS_CKM.1/CA	F.CRYPTO - Cryptographic Support, F.EAC - Extended Access Control
FCS_CKM.1/AA	F.CRYPTO - Cryptographic Support
FCS_CKM.1/CAM	F.CRYPTO - Cryptographic Support, F.PACE - Authentication using PACE
FCS_CKM.1/POLY	F.CRYPTO - Cryptographic Support
FCS_CKM.4	F.CLR_INFO - Clear Residual Information , F.SM - Secure Messaging
FCS_COP.1/AA	F.AA - Active Authentication, F.CRYPTO - Cryptographic Support
FCS_COP.1/CAM	F.CRYPTO - Cryptographic Support, F.PACE - Authentication using PACE
FCS_COP.1/CA_MAC	F.CRYPTO - Cryptographic Support, F.SM - Secure Messaging
FCS_COP.1/CA_ENC	F.CRYPTO - Cryptographic Support, F.SM - Secure Messaging
FCS_COP.1/PACE_ENC	F.CRYPTO - Cryptographic Support, F.SM - Secure Messaging
FCS_COP.1/PACE_MAC	F.CRYPTO - Cryptographic Support, F.SM - Secure Messaging
FCS_COP.1/SIG_VER	F.CRYPTO - Cryptographic Support, F.EAC - Extended Access Control
FCS_COP.1/POLY	F.CRYPTO - Cryptographic Support
FCS_RND.1	F.CRYPTO - Cryptographic Support
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/TRM	F.ACR - Access Control in Reading, F.ACW - Access Control in Writing, F.EAC - Extended Access Control, F.PACE - Authentication using PACE

FDP_ACF.1/TRM	F.ACR - Access Control in Reading, F.ACW - Access Control in Writing, F.EAC - Extended Access Control, F.PACE - Authentication using PACE
FDP_ACC.1/POLY	F.ACR - Access Control in Reading, F.ACW - Access Control in Writing, F.POLY - Polymorphic Authentication
FDP_ACF.1/POLY	F.ACR - Access Control in Reading, F.ACW - Access Control in Writing, F.POLY - Polymorphic Authentication
FDP_RIP.1/POLY	F.CLR_INFO - Clear Residual Information
FDP_ACC.1/LDS2	F.ACR - Access Control in Reading, F.ACW - Access Control in Writing, F.EAC - Extended Access Control, F.PACE - Authentication using PACE
FDP_ACF.1/LDS2	F.ACR - Access Control in Reading, F.ACW - Access Control in Writing, F.EAC - Extended Access Control, F.PACE - Authentication using PACE
FIA_UID.1/PACE_CAM	F.PACE - Authentication using PACE
FIA_UAU.1/PACE_CAM	F.PACE - Authentication using PACE
FIA_UAU.4/PACE_CAM	F.CLR_INFO - Clear Residual Information
FIA_UAU.5/PACE_CAM	F.PACE - Authentication using PACE
FIA_UAU.6/PACE_CAM	F.SM - Secure Messaging
FIA_AFL.1/PACE	F.PACE - Authentication using PACE
FIA_UID.1/PACE	F.ACR - Access Control in Reading, F.EAC - Extended Access Control, F.PACE - Authentication using PACE
FIA_UAU.1/PACE	F.ACR - Access Control in Reading, F.EAC - Extended Access Control, F.PACE - Authentication using PACE
FIA_UAU.4/PACE	F.CLR_INFO - Clear Residual Information
FIA_UAU.5/PACE	F.PACE - Authentication using PACE , F.PREP - MRTD Pre-personalization , F.SM - Secure Messaging
FIA_UAU.6/PACE	F.SM - Secure Messaging
FIA_API.1/AA	F.AA - Active Authentication
FIA_API.1/CA	F.EAC - Extended Access Control
FIA_AFL.1/PINPUK	F.POLY - Polymorphic Authentication
FIA_UID.1/POLY	F.PACE - Authentication using PACE , F.POLY - Polymorphic Authentication
FIA_UAU.1/POLY	F.PACE - Authentication using PACE , F.POLY - Polymorphic Authentication
FIA_UAU.4/POLY	F.CLR_INFO - Clear Residual Information
FIA_UAU.5/POLY	F.EAC - Extended Access Control, F.PACE - Authentication using PACE , F.POLY - Polymorphic Authentication
FIA_UAU.6/POLY	F.SM - Secure Messaging
FIA_UAU.6/EAC	F.SM - Secure Messaging
FMT_SMF.1	F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization , F.POLY - Polymorphic Authentication
FMT_SMR.1/PACE	F.EAC - Extended Access Control, F.PACE - Authentication using PACE , F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization

FMT_MOF.1/BAC_EXP	F.EAC - Extended Access Control
FMT_MTD.1/BAC_EXP	F.PERS - MRTD Personalization
FMT_MTD.1/INI_ENA	F.PREP - MRTD Pre-personalization
FMT_MTD.1/INI_DIS	F.ACR - Access Control in Reading, F.PREP - MRTD Pre-personalization
FMT_MTD.1/CVCA_INI	F.ACW - Access Control in Writing, F.PERS - MRTD Personalization
FMT_MTD.1/CVCA_UPD	F.ACW - Access Control in Writing, F.EAC - Extended Access Control
FMT_MTD.1/AAPK	F.ACW - Access Control in Writing, F.PERS - MRTD Personalization
FMT_MTD.1/DATE	F.ACW - Access Control in Writing, F.EAC - Extended Access Control
FMT_MTD.1/PA	F.PERS - MRTD Personalization
FMT_MTD.1/KEY_READ	F.ACR - Access Control in Reading
FMT_MTD.1/CAPK	F.ACW - Access Control in Writing, F.PERS - MRTD Personalization
FMT_MTD.1/Initialize_PIN	F.ACW - Access Control in Writing, F.PERS - MRTD Personalization
FMT_MTD.1/Change_PIN	F.ACW - Access Control in Writing, F.POLY - Polymorphic Authentication
FMT_MTD.1/Unblock_PIN	F.POLY - Polymorphic Authentication
FMT_MTD.1/Resume_PIN	F.ACW - Access Control in Writing, F.POLY - Polymorphic Authentication
FMT_MTD.1/LDS2_PA	F.ACW - Access Control in Writing, F.PERS - MRTD Personalization
FMT_MTD.3	F.EAC - Extended Access Control
FMT_SMR.1/POLY	F.POLY - Polymorphic Authentication
FMT_LIM.1/POLY	F.PHY - Physical Protection , F.SS - Safe State Management
FMT_LIM.2/POLY	F.PHY - Physical Protection , F.SS - Safe State Management
FMT_MTD.1/PI_PP_CPI_Load	F.PERS - MRTD Personalization
FMT_MTD.1/PI_PP_CPI_Read	F.ACR - Access Control in Reading
FMT_MTD.1/PINPUK	F.PERS - MRTD Personalization
FMT_MTD.1/Activate_DBI	F.PERS - MRTD Personalization
FMT_MTD.1/Deactivate_DBI	F.EAC - Extended Access Control
FMT_MTD.1/DBI_Terminal	F.PERS - MRTD Personalization
FMT_LIM.1	F.PHY - Physical Protection , F.SS - Safe State Management
FMT_LIM.2	F.PHY - Physical Protection , F.SS - Safe State Management
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.EAC - Extended Access Control, F.PACE - Authentication using PACE , F.SM - Secure Messaging
FPR_ANO.1	F.ACR - Access Control in Reading
FPR_UNL.1	F.POLY - Polymorphic Authentication

Table 29 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
F.ACR - Access Control in Reading	FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_ACC.1/POLY, FDP_ACF.1/POLY, FDP_ACC.1/LDS2, FDP_ACF.1/LDS2, FIA_UID.1/PACE, FIA_UAU.1/PACE, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_READ, FMT_MTD.1/PI_PP_CPI_Read , FPR_ANO.1
F.ACW - Access Control in Writing	FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_ACC.1/POLY, FDP_ACF.1/POLY, FDP_ACC.1/LDS2, FDP_ACF.1/LDS2, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/AAPK, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/LDS2_PA
F.AA - Active Authentication	FCS_COP.1/AA, FIA_API.1/AA
F.CLR_INFO - Clear Residual Information	FCS_CKM.4, FDP_RIP.1, FDP_RIP.1/POLY, FIA_UAU.4/PACE_CAM, FIA_UAU.4/PACE, FIA_UAU.4/POLY
F.CRYPTO - Cryptographic Support	FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.1/AA, FCS_CKM.1/CAM, FCS_CKM.1/POLY, FCS_COP.1/AA, FCS_COP.1/CAM, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_COP.1/SIG_VER, FCS_COP.1/POLY, FCS_RND.1
F.EAC - Extended Access Control	FCS_CKM.1/CA, FCS_COP.1/SIG_VER, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_ACC.1/LDS2, FDP_ACF.1/LDS2, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_API.1/CA, FIA_UAU.5/POLY, FMT_SMR.1/PACE, FMT_MOF.1/BAC_EXP, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.3, FMT_MTD.1/Deactivate_DBI, FTP_ITC.1/PACE
F.PACE - Authentication using PACE	FCS_CKM.1/DH_PACE, FCS_CKM.1/CAM, FCS_COP.1/CAM, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_ACC.1/LDS2, FDP_ACF.1/LDS2, FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM, FIA_UAU.5/PACE_CAM, FIA_AFL.1/PACE, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5/PACE, FIA_UID.1/POLY, FIA_UAU.1/POLY, FIA_UAU.5/POLY, FMT_SMR.1/PACE, FTP_ITC.1/PACE
F.PERS - MRTD Personalization	FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/BAC_EXP, FMT_MTD.1/CVCA_INI, FMT_MTD.1/AAPK, FMT_MTD.1/PA, FMT_MTD.1/CAPK, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/LDS2_PA , FMT_MTD.1/PI_PP_CPI_Load , FMT_MTD.1/PINPUK, FMT_MTD.1/Activate_DBI, FMT_MTD.1/DBI_Terminal
F.PHY - Physical Protection	FMT_LIM.1/POLY, FMT_LIM.2/POLY, FMT_LIM.1, FMT_LIM.2, FPT_EMS.1, FPT_PHP.3
F.PREP - MRTD Pre-personalization	FAU_SAS.1, FIA_UAU.5/PACE, FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS
F.POLY - Polymorphic Authentication	FDP_ACC.1/POLY, FDP_ACF.1/POLY, FIA_AFL.1/PINPUK, FIA_UID.1/POLY, FIA_UAU.1/POLY, FIA_UAU.5/POLY, FMT_SMF.1, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Resume_PIN, FMT_SMR.1/POLY, FPR_UNL.1
F.SM - Secure Messaging	FCS_CKM.4, FCS_COP.1/CA_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FIA_UAU.6/PACE_CAM, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/POLY, FIA_UAU.6/EAC, FTP_ITC.1/PACE

F.SS - Safe State Management	FMT_LIM.1/POLY, FMT_LIM.2/POLY, FMT_LIM.1, FMT_LIM.2, FPT_FLS.1, FPT_PHP.3
F.STST - Self Test	FPT_TST.1

Table 30 TSS and SFRs - Coverage