SECURITY TARGET LITE

IDEAL PASS v2.3-n JC WITH PRIVACY PROTECTION (SAC/EAC/POLYMORPHIC EMRTD CONFIGURATION)

Reference: 2018_2000036361

DOCUMENT EVOLUTION

Date	Index	Author	Revision
11/06/2018	1.0	IDEMIA	Initial version based on the full security target (Reference: 2017_2000032696, Version: 1.5)
30/01/2019	1.1	IDEMIA	Second version based on the full security target (Reference: 2017_2000032696, Version: 1.6): - JCOP 3 Platform CC certifcate updated to CC-18-98209/2. - Applet ROM masking added.

Table of Contents

Table of figures

Table of tables

1 ST Introduction

The aim of this document is to describe the Security Target for IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration), the Machine Readable Travel Document (MRTD) with the ICAO application, Password Authenticated Connection Establishment (covering PACE-GM, PACE-IM and PACE-CAM), Extended Access Control and Polymorphic eMRTD on NXP JCOP 3 P60.

1.1 ST Identification

Title	Security Target Lite IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration)
Reference	2018_2000036361
Version	1.1
Certification Body	NSCIB
Author	IDEMIA
CC Version	3.1 Revision 5
Assurance Level	EAL5 augmented with ALC_DVS.2 and AVA_VAN.5
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 1.0.1, 22 July 2014, BSI [PACE-PP].

1.2 TOE Reference

TOE name	IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration)
TOE identification	7126-9301-0311 for applet loaded in EEPROM 7126-9301-0319 for applet loaded in ROM
TOE version	v2.3.0.14
Name of Platform	NXP JCOP 3 P60 certified by the Dutch NSCIB certification body (CC-18-98209/2) on 29-11-2018
Platform identification	Platform ID: "JxHyyy0019790400" (SVN 6521; "OSB RC9") Patch ID: 00 00 00 00 00 00 00 00 (no patch) 04 00 00 00 00 00 00 00 (PL4)
IC reference	NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software certified by the German BSI certification body (BSI-DSZ-CC-1059-2018) on 18-05-2018
Crypto Lib reference	Crypto Library V3.1.x on P6022y VB certified by the Dutch NSCIB certification body (CC-18-67206) on 31-05-2018

1.3 TOE Overview

The Security Target (ST) defines the security objectives and requirements for a contact or contactless based chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO), EU requirements for biometric European passport (Council Regulation (EC) No 2252/2004 and Commission Implementing Decision 6181) and Biometric European Resident Permit (REGULATION (EU) 2017/1954 and Commission Implementing Decision 6178). This product is intended to enable verification of the authenticity of the travel document and to identify its holder during a border control, using an inspection system. The verification process is based on Extended Access Control with Password Authenticated Connection Establishment (PACE) and optionally Active Authentication (AA).

The main features and their origin are the following:

- **Password Authenticated Connection Establishment (PACE)** according to ICAO Technical Report "Supplemental Access Control" [ICAO-9303] part 11 and strictly conform to BSI-CC-PP-0068-V2 [PACE-PP] for protection of the communication between terminal and chip. The following PACE mapping modes are supported and covered by the TOE:
  - Generic Mapping (PACE-GM)
  - Integrated Mapping (PACE-IM)
  - Chip Authentication Mapping (PACE-CAM), which combines PACE-GM with Chip Authentication into a single protocol.

- **Chip Authentication v1**
  according to BSI TR-03110 parts 1 and 3 [TR-03110-1], [TR-03110-3] and strictly conform to BSI-CC-PP-0056-V2-2012 [EAC-PP-V2], authenticates the travel document's chip to the inspection system.
- **Terminal Authentication v1**
  according to BSI TR-03110 parts 1 and 3 [TR-03110-1], [TR-03110-3] and strictly conform to BSI-CC-PP-0056-V2-2012 [EAC-PP-V2], authenticates the inspection system to travel document's chip and protects the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system.

As a feature that can be optionally configured the TOE supports:

- **Active Authentication**
  which according to [ICAO-9303] prevents copying the SO_D and proves that it has been read from the authentic chip. It proves that the chip has not been substituted.

- **Polymorphic Authentication**
  which according to [PCA-eMRTD] provides additional privacy by randomisation of returned Polymorphic Identities, Polymorphic Pseudonyms and Complementary Polymorphic ID attributes in combination with standard ICAO and EAC1 eMRTD protocols specified in ICAO Doc 9303 [ICAO-9303] and BSI TR-03110 parts 1 and 3 [TR-03110-1] and [TR 03110-3].

The TOE may also be used as an ISO driving license, compliant to ISO/IEC 18013 or ISO/IEC TR 19446 supporting PACE, AA and CA, as both applications (MRTD and IDL) share the same protocols and data structure organization. Therefore, in the rest of the document, the word "MRTD" MAY be understood either as a 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.

Application note

This TOE claims an assurance level EAL5 augmented with AVA_VAN.5 and ALC_DVS.2. AVA_VAN.5 implies that the TOE is resistant to attacks performed by an attacker possessing "High attack potential".

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].

1.4 TOE Description

1.4.1 TOE Definition

The Target of Evaluation (TOE) addressed by the current security target is an electronic travel document representing a contactless / contact based smart card or passport programmed according to Logical data structure (LDS) and protocols specified in ICAO Doc 9303 [ICAO-9303] and additionally providing the Extended Access Control according to BSI TR-03110 part 1 [TR-03110-1] and part 3 [TR-03110-3] and Active Authentication according to [ICAO-9303]. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE), optionally with Chip Authentication Mapping (PACE CAM) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2 [PACE-PP]. Polymorphic eMRTD extensions are present on the TOE that enable secure authentication with enhanced privacy protection features. It provides the holder the possibility to authenticate towards a service provider in a non-traceable and non-linkable manner thanks to usage of Polymorphic Pseudonyms and other Polymorphic ID attributes.

The TOE (IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration)) is composed of

- the NXP JCOP 3 P60, composed of
  - the circuitry of the MRTD's chip (NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software) with hardware for the contact and contactless interface;
  - the Crypto Library V3.1.x on P6022y VB;
  - the IC Embedded Software (operating system): NXP JCOP 3;
- The MRTD application IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) loaded in ROM or in EEPROM;
- the associated guidance documentation in [AGD_PRE] and [AGD_OPE];
- the Personalisation Agent Key set.

The TOE utilizes the evaluation of NXP JCOP 3 P60 which has been certified by the Dutch NSCIB certification body (CC-18-98209/2).

A schematic overview of the TOE is shown in Figure 1:

- The MRTD's chip circuitry and the IC dedicated software forming the Smart Card Platform (Hardware Platform and Hardware Abstraction Layer);
- The IC embedded software running on the Smart Card 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.
- Mifare implementation can be enabled or disabled for this TOE.
- Crypto Library.

- The Applet Layer is IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) applet.

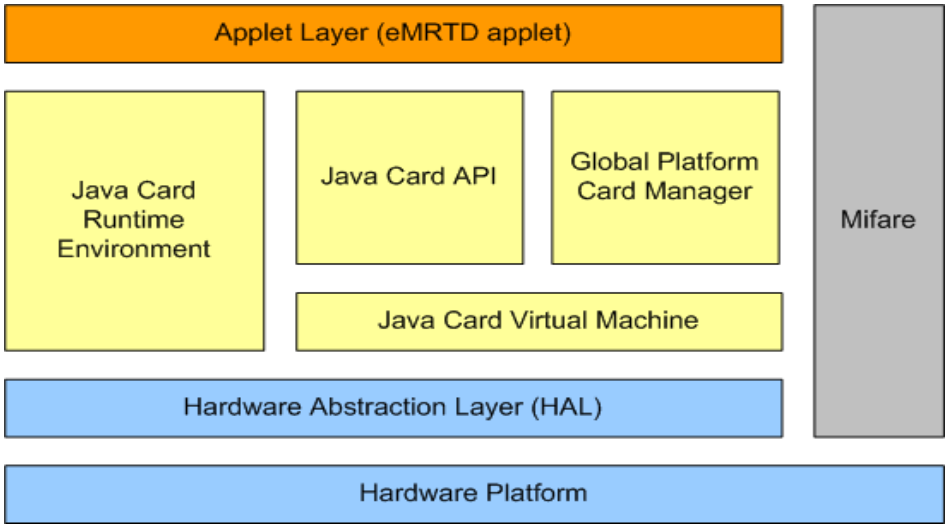


Figure 1: TOE

1.4.2 TOE usage and security features for operational use

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

- ICAO/EAC eMRTD,
- 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 applet having their own dedicated application identifiers and personalisation. The following TOE configurations are covered within the scope of this Security Target:

Configuration	ICAO/EAC eMRTD	Polymorphic eMRTD	Driver licence
1	present	-	-
2	present	present	-
3	-	-	present
4	-	present	present
5	-	Present	-

The authentication protocols PACEv2, Chip authentication (CAv1), Active Authentication and Terminal Authentication (TAv1) specified in [ICAO-9303] and

[TR-03110] have also been refered 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)
Traveler	Holder

***Access rights to the biometric data in DG3 and DG4 are also mapped to DG7 and DG8, respectively.**

The following two sub sections explain the TOE security features for operational use of TOE configured as respectively ICAO/EAC eMRTD/Driving licence and Polymorphic eMRTD.

1.4.2.1 ICAO/EAC eMRTD and ISO Driving licence

This sub section explains the TOE security features for operational use of TOE configured as ICAO/EAC eMRTD or as Driving Licence.

A State or Organisation issues travel documents to be used by the holder for international travel. The traveller presents a travel document to the inspection system to prove his or her identity. The travel document 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 travel document's chip according to LDS in case of contactless machine reading.

The authentication of the traveller is based on:

I. the possession of a valid travel document personalized for a holder with the claimed identity as given on the biographical data page and
II. biometrics using the reference data stored in the travel document.

The issuing State or Organization ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organization.

For this Security Target the travel document is viewed as unit of:

(i) the **physical part of the travel document** in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder
   (a) the biographical data on the biographical data page of the travel document surface,
   (b) the printed data in the Machine Readable Zone (MRZ) and
   (c) the printed portrait.

(ii) the **logical travel document** as data of the travel document holder stored according to the Logical Data Structure as defined in [ICAO-9303] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including(but not limited to) personal data of the travel document holder
   (a) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
   (b) the digitized portraits (EF.DG2),
   (c) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1],
   (d) the other data according to LDS (EF.DG5 to EF.DG16) and
   (e) the Document Security Object (SO_D).

The issuing State or Organisation implements security features of the travel document to maintain the authenticity and integrity of the travel document and their data. The physical part of the travel document and the travel document's chip are identified by the Document Number.

The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organisational security measures (e.g. control of materials, personalisation procedures) [ICAO-9303].These security measures can include the binding of the travel document's chip to the travel document.

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

The ICAO Doc 9303 [ICAO-9303] defines the baseline security methods Passive Authentication, advanced security access methods Basic Access Control (BAC) and Password Authenticated Connection Establishment to the logical travel

[1]These biometric reference data are optional according to [ICAO-9303]. This ST assumes that the issuing State or Organisation uses this option and protects these data by means of extended access control.

document, Active Authentication of the travel document's chip, Extended Access Control and the Data Encryption of sensitive biometrics as optional security measure. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

The BSI TR-03110 parts 1 and 3 [TR-03110-1] and [TR 03110-3] specify the Extended Access Control protocols Chip Authentication version 1 (CAv1) and Terminal Authentication (TAv1), which are required to get secured access to the biometric data stored in data groups DG3 and DG4 in combination with PACE or BAC.

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.

This Security Target addresses the Chip Authentication Version 1 described in [TR-03110-1] and PACE-CAM described in [ICAO-9303] part 11 as an alternative to the Active Authentication stated in [ICAO-9303].

For Basic Access Control (BAC) supported by the product, a separate evaluation and certification is performed with ST [ST-BAC].

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The travel document shall strictly conform to the 'Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP]. Note that [PACE-PP] considers high attack potential.

For the PACE protocol according to [ICAO-9303] part 11, the following steps shall be performed:

(i) the travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.
(ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ or CAN data. This nonce shall be converted to a group generator using one of the following mapping algorithms, which maps a static generator to an ephemeral generator:
    a. Generic mapping (PACE-GM) or
    b. Integrated mapping PACE-IM)
(iii) The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.
(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

In case of PACE with Chip Authenticated Mapping (PACE-CAM), in addition to the steps above executed for the PACE-GM variant, the MRTD chip computes Chip Authentication Data CAIC, encrypts them AIC = E(KSEnc, CAIC) and sends them

to the terminal. The terminal decrypts AIC and verifies the authenticity of the chip using the recovered Chip Authentication Data CAIC.

After successful key negotiation, the terminal and the travel document's chip provide private communication (secure messaging) [TR-03110-1], [ICAO-9303].

This Security Target requires the TOE to implement the Extended Access Control as defined in [TR-03110-1]. The Extended Access Control consists of two parts:
(i) the Chip Authentication Protocol Version 1 and
(ii) the Terminal Authentication Protocol Version 1 (v.1).

The Chip Authentication Protocol v.1
(i) authenticates the travel document’s chip to the inspection system and
(ii) establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1has been successfully executed.

The Terminal Authentication Protocolv.1 consists of
(i) the authentication of the inspection system as entity authorized by the receiving State or Organisation through the issuing State, and
(ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems.

The Active Authentication protocol may be optionally configured during personalisation.

The issuing State or Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

1.4.2.2 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 or 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, PUK and CAN 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.

1.4.3 TOE life cycle

The TOE life cycle is described in terms of its four life cycle phases. (With respect to the [SIC-PP], the TOE life-cycle is additionally subdivided into 7 steps in the ST. These steps are denoted too in the following although the sequence of the steps differs for the TOE life cycle).

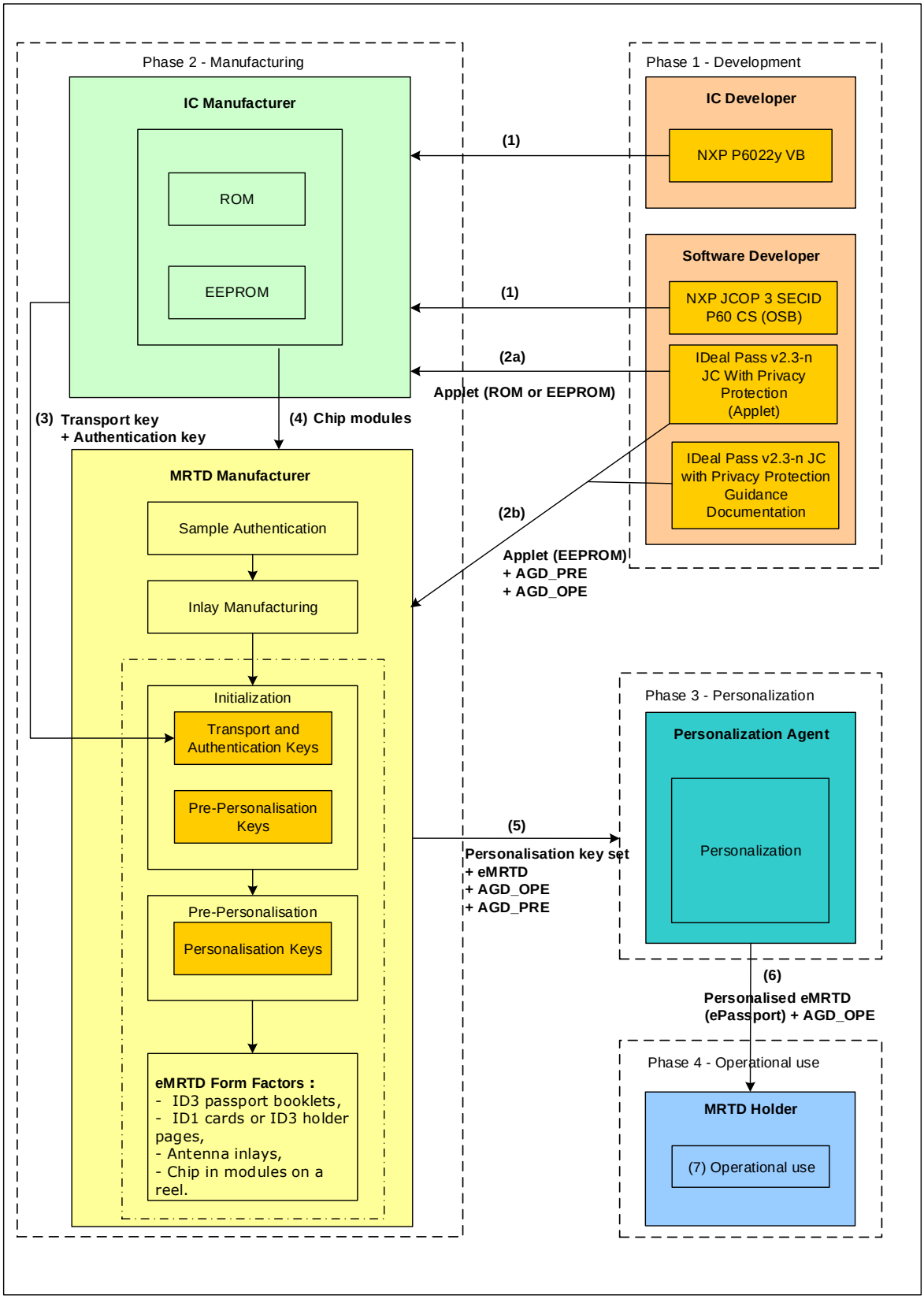


Figure 2: TOE life-cycle

Actors :

IC Developer, IC Manufacturer	NXP
Software Developer	Platform: NXP ePassport applet: IDEMIA R&D sites (Osny, Meyreuil and Noida)
Travel document manufacturer	IDEMIA plants (Haarlem and Noida)

1.4.3.1 Phase 1 "Development"

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.
The IC developer also acts as the developer of the embedded software (operating system), which is the NXP JCOP 3 P60.

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the NXP JCOP 3 P60 and develops the ePassport application and the guidance documentation associated with this TOE component.

The ePassport application (i.e. the IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) applet run time code) may be integrated either in ROM or in EEPROM of the chip. Depending on the intention:

(a) the ePassport application is securely delivered directly from the software developer (IDEMIA development dept.) to the IC manufacturer (NXP). The applet code will be integrated into the ROM mask code or inEEPROM by the IC manufacturer, or

(b) the ePassport application is securely delivered directly from the software developer (IDEMIA development dept.) to the travel document manufacturer (IDEMIA production dept.) .) for loading in EEPROM.

Notice that the guidance documentation of the ePassport application is always securely delivered directly from the software developer (IDEMIA development dept.) to the travel document manufacturer (IDEMIA production dept.).

1.4.3.2 Phase 2 "Manufacturing"

(Step3) In a first step the TOE integrated circuit is produced containing the travel document's chip Dedicated Software, the parts of the travel document's chip Embedded Software and in case of alternative a) the ePassport application in ROM or in EEPROM.

The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. The IC is securely delivered from the IC manufacturer to the travel document manufacturer.

If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM).

(Step4 optional) The travel document manufacturer combines the IC with hardware for the contact based / contactless interface in the travel document unless the travel document consist of the chip only.

(Step5) The travel document manufacturer

i. adds the IC Embedded Software or part of it in the non-volatile programmable memories (for instance EEPROM) if necessary and in case of alternative (b), loads the ePassport application into the non-volatile programmable memories (for instance EEPROM),

ii. creates the ePassport application and

iii. equips travel document's chips with pre-personalization Data.

EAC PP Application Note 1: Creation of the application for this TOE implies Applet instantiation.

For this Security Target the following name mappings to the protection profile [EAC-PP-V2] apply:

- IC Dedicated SW = Low level IC libraries
- travel document's chip Embedded Software = NXP JCOP 3 P60 operating system.
- ePassport application = IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) Applet run time code or an instantiation of it.
- Pre-personalization Data = Personalization Agent Key Set, Card Production Life Cycle (CPLC) data and buffer settings.

Both the underlying platform and IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) Applet provide configuration and life-cycle management functions required for TOE preparation. TOE preparation steps are performed in manufacturing phase and consist of the following 2 activities:

1. Platform initialisation
2. Pre-personalisation

Platform initialisation

Platform initialisation consists of the configuration of the NXP JCOP 3 P60 in accordance with requirements specified in the platform administrator guidance [PLTF-PRE] by using the dedicated platform commands. Furthermore the Pre-Personalisation Agent key set is installed and (a part of) the CPLC data is updated. To prevent unattended tracing of the MRTD document, the NXP JCOP 3 P60 is configured such that unauthenticated access to any platform unique idenfiable data is not possible.

Pre-personalisation

The pre-personalisation consists of the following steps:

a. IC (chip) Authentication and getting chip access with the pre-personalisation key set.
b. [optional] In case the IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) applet runtime code does not reside in ROM, it is loaded into EEPROM.
c. Install the applet application instances depending on the desired TOE configuration specified in section 1.4.2, using IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) applet.
d. Set the ePassport (and if present) the Polymorphic eMRTD applet irreversibly in its PERSONALISATION life-cycle state by installation of the Personalisation Agent specific personalisation key set(s).

During step (c) the CPLC data with the IC Identifier as well as the other pre-personalisation data is configured in the TOE. The last step (d) finalizes the TOE. This is the moment the TOE starts to exist and is ready for delivery to the Personalisation Agent. The guidance documentation for the Personalisation Agent is [AGD_PRE].

The pre-personalised travel document together with the IC Identifier is securely delivered from the travel document manufacturer to the Personalisation Agent. The travel document manufacturer also provides the relevant parts of the guidance documentation [AGD_PRE] and [AGD_OPE] and the Personalisation Agent Key set to the Personalisation Agent. The following table describes the physical delivery of the TOE components:

TOE component	**Identification**	**Version**	**Package**	**Delivery method**
IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration)	- 7126-9301-0311 for applet loaded in EEPROM - 7126-9301-0319 for applet loaded in ROM	v2.3.0.14	The package can be either of the following: - Chip embedded in ID3 passport booklets, - Chip embedded in ID1 cards or ID3 holder pages, - Chip embedded in antenna inlays, - Chip in modules on a reel.	Trusted courier
[AGD_OPE]*	2017_2000032685	2.1	Electronic document	PGP-encrypted email
[AGD_PRE]*	2017_2000032686	2.7	Electronic document	PGP-encrypted email
Personalisation Agent Key set	n.a	n.a	Electronic file	PGP encrypted parts on USB or CD media, off-line registered distribution by trusted courier.

* : Distribution of guidance documents [AGD_PRE] and [AGD_OPE] is only managed by the IDEMIA Haarlem manufacturing site.

1.4.3.3 Phase 3 "Personalisation of the travel document"

(Step 6) The personalisation of the travel document includes

i. the survey of the MRTD holder's biographical data,
ii. the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
iii. the printing of the visual readable data onto the physical MRTD,
iv. the writing of the TOE User Data and TSF Data into the logical MRTD and
v. configuration of the TSF if necessary.

The step (iv) is performed by the Personalisation Agent and includes but is not limited to the creation of:

i. the digital MRZ data (EF.DG1),
ii. the digitized portrait (EF.DG2), and
iii. the Document security object.

The signing of the Document security object by the Document signer [ICAO-9303] finalizes the personalisation of the genuine travel document for the travel document holder. The personalised travel document (together with appropriate guidance (AGD_OPE) for TOE usage if necessary) is handed over to the travel document holder for operational use.

The personalisation of Polymorphic eMRTD application instance includes:

i. establishing the identity of the polymorphic eMRTD document holder,
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 (PIN, PUK, CAv1 private key) as defined in [PCA-eMRTD],
v. signing the Document Security Object defined in [ICAO-9303] (in the role of DS).

The signing of the Document security object by the Document signer [ICAO-9303] finalizes the personalisation of the genuine Polymorphic eMRTD document for the travel document holder. The personalised Polymorphic eMRTD document (together with appropriate guidance (AGD_OPE) for TOE usage if necessary) is handed over to the Polymorphic eMRTD document holder for operational use.

EAC PP Application note 2: The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [CC-1] §92) comprise (but are not

limited to) the Personalisation Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key.

EAC PP Application note 3: This ST distinguishes between the Personalisation Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [ICAO-9303]. This approach allows but does not enforce the separation of these roles.

1.4.3.4 Phase 4 "Operational Use"

(Step 7) 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.

EAC PP Application note 4[2]**:** The intention of the ST is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organisation. In this case the national body of the issuing State or Organisation is responsible for these specific production steps.
Note that the personalisation process and its environment may depend on specific security needs of an issuing State or Organisation. All production, generation and installation procedures after TOE delivery up to the "Operational Use" (phase 4) have to be considered in the product evaluation process under AGD assurance class. Therefore, the Security Target outlines the split up of P.Manufact, P.Personalisation and the related security objectives into aspects relevant before vs. after TOE delivery.

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

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

[2] For this ST all steps of both phase 1 and phase 2 are part of the evaluation and therefore define the TOE delivery according to the CC evaluation after this phase.

2 Conformance Claims

2.1 CC Conformance Claim

This security target claims to be conformant to the Common Criteria version 3.1,which comprises

- Common Criteria for Information Technology Security Evaluation, Part 1:Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 5, April 2017
  [CC-1]
- Common Criteria for Information Technology Security Evaluation, Part 2:Security Functional Requirements; CCMB-2012-09-002, Version 3.1, Revision 5, April 2017 [CC-2]
- Common Criteria for Information Technology Security Evaluation, Part 3:Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 5, April 2017 [CC-3]

  as follows:
  - Part 2 extended
    - FAU_SAS Audit data storage
    - FCS_RND Generation of random numbers
    - FIA_API Authentication proof of identity
    - FMT_LIM Limited capabilities and availability
    - FPT_EMS TOE emanation
  - Part 3 conformant

The Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017 [CEM] has been taken into account.

2.2 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 1.0.1, 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.

2.3 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].

2.4 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.

2.4.1 Main aspects

- The TOE description (chapter 1.3) is based on the TOE definition and TOE usage of [EAC-PP, 1.1]. It was enhanced by product specific details.

- All definitions of the security problem definition in [EAC-PP, 3] have been taken exactly from the protection profile in the same wording.

- All security objectives have been taken exactly from [EAC-PP, 4] in the same wording, except for **OT.Chip_Auth_Proof** which is enhanced to support Active Authentication.

- The part of extended components definition has been taken originally from [EAC-PP, 5].

- All SFRs for the TOE have been taken originally from the [EAC-PP, 6.1] added by according iterations, selections and assignments.

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

2.4.2 Overview of differences between the PP and the ST

The Active Authentication has been added to the TOE. For that:
- One assumption has been added to cover Active Authentication during personalization: **A.Pers_Agent_AA**
- 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.
- Three security functional requirements have been added:
    - FCS_COP.1/SIG_GEN
    - FIA_API.1/AA
    - FMT_MTD.1/AAPK

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.

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
- FMT_MTD.1/PACE_CAM_KEY_READ
- FMT_MTD.1/PACE_CAM_KEY_WRITE

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].

3 Security Problem Definition

3.1 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]:

3.1.1 Primary Assets travel document

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

Authenticity

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

Authenticity

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

3.1.2 Secondary Assets travel document

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

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

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

TOE internal non-secret cryptographic material

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

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

Integrity

Authenticity

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, 3.1]. The secondary assets also have to be protected by the TOE in order to achieve a sufficient protection of the primary assets.

3.1.3 Additionals Assets

Logical travel document sensitive User Data

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

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 traveler to prove his possession of a genuine travel document.

3.1.4 Assets related to Polymorphic eMRTD

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].

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

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.

3.2 Users / Subjects

3.2.1 Subjects listed in PP PACE

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

travel document holder

Definition A person for whom the travel document Issuer has personalized 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).

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 'Traveler' in [BAC-PP]. Please note that a travel document presenter can also be an attacker (s. below)

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].

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.

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.

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.

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:

(i) establishing the identity of the travel document holder for the biographic data in the travel document,

(ii) enrolling the biometric reference data of the travel document holder,

(iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO-9303],

(iv) writing the document details data,

(v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO-9303](in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. This entity is commensurate with 'Personalisation agent' in [BAC-PP].

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].

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

(i) to manipulate the logical travel document without authorization,

(ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4),

(iii) to forge a genuine travel document, or

(iv) to trace a travel document.

3.2.2 Additional Subjects

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

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.

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.

Inspection system (IS)

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

The Extended Inspection System (EIS) performs the Advanced Inspection Procedure and therefore

(i)contains a terminal for the communication with the travel document's chip,

(ii) implements the terminals part of PACE and/or BAC;

(iii) gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information.

(iv) implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [TR-03110-1] and

(v) is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.

3.2.3 Subjects related to Polymorphic eMRTD

Polymorphic Authentication Terminal/Service

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

(i) verifying the user as Polymorphic eMRTD document holder by verifying the user's PIN PACE password as part of the PACE protocol

(ii) examining a Polymorphic eMRTD document presented by the user and verifying its authenticity by Passive Authentication (PA) (signature verification of DG14 using SOD)

(iii) Performing Chip Authentication (CAv1) and Terminal Authentication (TAv1)

(iv) 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:

- 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.

Application Note:

This subject is an extension of the subject 'Inspection system (IS)' defined in [EAC-PP-V2].

Polymorphic Personalisation Agent

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

(i) 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,

(ii) 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,

(iii) write document non-card unique identifiable meta data (i. e. document type, scheme version, issuer, etc.),

(iv) writing the initial TSF data and

(v) sign the Document Security Object according to [ICAO-9303] and [TR-03110-3]) in the role of DS.

Note that the role personalization 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].

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].

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].

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].

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].

3.3 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.

3.3.1 Threats listed in PP PACE

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.

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.

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.

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.

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.

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.

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.

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.

3.3.2 Additional Threats

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)

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 traveler 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.

3.3.3 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 EACv1 PP [EAC-PP-V2]:

Threats related to the polymorphic eMRTD	Threats from PACE PP	Threats from EACv1 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		
T.DoS		

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].

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.

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 EACv1 PP [EAC-PP-V2].

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.

T.DoS

An attacker prevents correct authentication process. This could potentially deny a user access to the service. An Attacker can attempt to deny access for legitime users using a wrong PACE PIN code.

3.4 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).

3.4.1 OSP listed in PP PACE

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.

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.

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.

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.

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].

3.4.2 Additional OSPs from PP EAC

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.

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.

3.4.3 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 EACv1 PP [EAC-PP-V2]:

OSPs related to the polymorphic eMRTD	OSPs from PACE PP	OSPs from EACv1 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

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 Polymorhic (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].

P.Polymorphic_Authentication_Terminal

Terminals/Services that intent 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.

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 personalization agent or the manufacturer.

Application Note:

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

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].

3.5 Assumptions

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

3.5.1 Assumptions listed in PP PACE

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].

3.5.2 Assumptions listed in PP EAC

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.

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

A.Auth_PKI

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.

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

3.5.3 Assumptions related to Active Authentication

A.Pers_Agent_AA

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

3.5.4 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 EACv1 PP [EAC-PP-V2]:

As related to the polymorphic eMRTD	As from PACE PP	As from EACv1 PP
A.Auth_PKI_Polymorphic		A.Auth_PKI
A.Insp_Sys_Polymorphic		A.Insp_Sys
A.Polymorphic_Auth		

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 personalization 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 has 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 EACv1 PP [EAC-PP-V2].

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 personalization 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.

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.

4 Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

4.1.1 Security Objectives listed in PP PACE

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.

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).

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.

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.

OT.Prot_Abuse-Func

Protection against Abuse of Functionality

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

OT.Prot_Inf_Leak

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

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

OT.Prot_Phys-Tamper

Protection against Physical Tampering

The TOE must provide protection the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with high attack potential by means of

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

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 (especially electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

OT.Identification

Identification and Authentication 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).

OT.AC_Pers

Access Control for Personalisation of logical MRTD

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.

4.1.2 Additional Security Objectives from PP EAC

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.

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-03110-1] **and (optionaly)** ***the Active Authentication as defined in [ICAO-9303]***[3]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

4.1.3 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 EACv1 PP [EAC-PP-V2]:

OTs related to the polymorphic eMRTD	OTs from PACE PP	OTs from EACv1 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		
OT.DoS		

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

[3] The bold text below has been added to support active authentication.

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 and EACv1 PPs.

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 and EACv1 PPs.

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 and EACv1 PPs.

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 and EACv1 PPs.

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 and EACv1 PPs.

OT.DoS

PIN and PUK are blocking PACE passwords. Therefore the number of incorrect authentication attempts on the PACE PIN and PUK passwords shall be controlled by the TOE to prevent a denial of service.

The TOE shall implement the suspend and resume mechanisms specified in [TR-3110-2] for blocking PACE passwords, PIN and (if present) PUK.

4.2 Security Objectives for the Operational Environment

4.2.1 Issuing State or Organisation

The Issuing State or Organization will implement the following security objectives of the TOE environment.

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.

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.

Justification: This security objective for the operational environment is needed additionally to those from [PACE-PP] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE described only in [EAC-PP-V2] and not in [PACE-PP].

OE.Auth_Key_MRTD

MRTD Authentication Key[4]

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.

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.

Justification: This security objective for the operational environment is needed additionally to those from [PACE-PP] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the additional features of the TOE described only in [EAC-PP-V2] and not in [PACE-PP].

4.2.2 Travel document Issuer and CSCA: travel document PKI (issuing) branch

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

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

(i) generate a cryptographically secure CSCA Key Pair,

(ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and

[4] Added in this ST with respect to [EAC-PP-V2]

(iii) publish the Certificate of the CSCA Public Key (CCSCA). Hereby authenticity and integrity of these certificates are being maintained.

A Document Signer acting in accordance with the CSCA policy must

(i) generate a cryptographically secure Document Signing Key Pair,

(ii) ensure the secrecy of the Document Signer Private Key,

(iii) hand over the Document Signer Public Key to the CSCA for certification,

(iv) sign Document Security Objects of genuine 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.

OE.Personalisation

Personalisation of travel document

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

(i) establish the correct identity of the travel document holder and create the biographical data for the travel document,

(ii) enroll the biometric reference data of the travel document holder,

(iii) 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],

(iv) write the document details data,

(v) write the initial TSF data,

(vi) sign the Document Security Object defined in [ICAO-9303] (in the role of a DS).

4.2.3 Terminal operator: Terminal receiving branch

OE.Terminal

Terminal operating

The terminal operators must operate their terminals as follows:

1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [ICAO-9303].

2.) The related terminals implement the terminal parts of the PACE protocol [ICAO-9303] part 11, of the Passive Authentication [ICAO-9303] part 11 (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 CCSCA and CDS) 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] part 12).

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 current PP.

4.2.4 Travel document holder Obligations

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.

4.2.5 Receiving State or Organisation

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 traveler 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-9303] part 11 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.

Justification: This security objective for the operational environment is needed additionally to those from [PACE-PP] in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocolv.1. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in [PACE-PP] and therefore also counters T.Forgery and A. Passive_Auth from [PACE-PP]. This is done because a new type of Inspection System is introduced in this PP as the Extended Inspection System is needed

to handle the additional features of a travel document with Extended Access Control.

OE.AA_MRTD

Active Authentication - Inspection Systems[5]

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).

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.

Justification: This security objective for the operational environment is needed additionally to those from [PACE-PP]in order to handle the Assumption A.Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1.

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.

Justification: This security objective for the operational environment is needed additionally to those from [PACE-PP] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A. Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier and the Inspection Systems.

[5] Added in this ST with respect to [EAC-PP-V2]

4.2.6 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 EACv1 PP [EAC-PP-V2]:

Oes related to the polymorphic eMRTD	Oes from PACE PP	Oes from EACv1 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 personalization 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 EACv1 PP [EAC-PP-V2].

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 personalization 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].

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 intent 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].

OE.Personalisation_Polymorphic

Personalisation of the polymorphic eMRTD document by the Personaliztion Agent

The Personaliztion 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].

4.3 Security Objectives Rationale

4.3.1 Threats

4.3.1.1 Threats listed in PP PACE

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 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 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 'Forgery of data' addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. Additionally to the security objectives from PACE PP [PACE-PP] which counter this threat, the examination of the presented MRTD passport book according to OE.Exam_Travel_Document 'Examination of the physical part of the 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.

The threat T.Forgery also 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.

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 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 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 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.

4.3.1.2 Additional Threats

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

access to the sensitive biometric reference data as demanded by OE.Ext_Insp_Systems 'Authorization of Extended Inspection Systems'.

T.Counterfeit '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 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.

4.3.1.3 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.

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

- **OT.DoS** requiring the TOE to control the authentication process and the number of authentication attempts executed by attackers on the PACE PIN and PUK passwords in order to prevent a denial of service.

4.3.2 Organisational Security Policies

4.3.2.1 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.

4.3.2.2 Additional OSPs from PP EAC

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

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.

4.3.2.3 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.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.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.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.

4.3.3 Assumptions

4.3.3.1 Assumptions listed in PP PACE

A.Passive_Auth The assumption A.Passive_Auth 'PKI for Passive Authentication' is directly covered by the security objective for the TOE environment OE.Passive_Auth_Sign 'Authentication of travel document by Signature' from PACE PP [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'.

4.3.3.2 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' and OE.AA_MRTD 'Active Authentication - Inspection Systems' which requires the inspection system to examine physically the travel document, the Basic Inspection System to implement the Basic Access Control, the General Inspection Systems and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol Version 1 and the Active Authentication Protocol 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 '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.

4.3.3.3 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.Personalization** including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

4.3.3.4 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.

4.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Skimming	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OE.Travel_Document_Holder	Section 4.3.1
T.Eavesdropping	OT.Data_Confidentiality	Section 4.3.1
T.Tracing	OT.Tracing, OE.Travel_Document_Holder	Section 4.3.1
T.Forgery	OT.AC_Pers, OT.Data_Integrity, OT.Data_Authenticity, OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper, OE.Personalisation, OE.Passive_Auth_Sign, OE.Terminal, OE.Exam_Travel_Document	Section 4.3.1
T.Abuse-Func	OT.Prot_Abuse-Func	Section 4.3.1
T.Information_Leakage	OT.Prot_Inf_Leak	Section 4.3.1
T.Phys-Tamper	OT.Prot_Phys-Tamper	Section 4.3.1
T.Malfunction	OT.Prot_Malfunction	Section 4.3.1
T.Read_Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 4.3.1
T.Counterfeit	OT.Chip_Auth_Proof, OE.Auth_Key_Travel_Document, OE.Exam_Travel_Document, OE.Auth_Key_MRTD, OE.AA_MRTD	Section 4.3.1
T.Sensitive_Polymorphic_Data	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Authenticity, OT.Polymorphic_Data_Privacy, OE.Authoriz_Polymorphic_Data	Section 4.3.1
T.Forgery_Polymorphic	OT.Polymorphic_Data_Integrity, OT.AC_Pers_Polymorphic,OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper	Section 4.3.1
T.Compromise_Privacy_Poly	OT.Polymorphic_Data_Privacy, OT.Polymorphic_Data_Confidentiality	Section 4.3.1
T.Eavesdropping_Polymorphic	OT.Polymorphic_Data_Confidentiality	Section 4.3.1
T.DoS	OT.DoS	Section 4.3.1

Table 1 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
OT.Prot_Inf_Leak	T.Information_Leakage
OT.Prot_Phys-Tamper	T.Forgery, T.Phys-Tamper, T.Forgery_Polymorphic
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.DoS	T.DoS
OE.Legislative_Compliance	
OE.Auth_Key_Travel_Document	T.Counterfeit
OE.Auth_Key_MRTD	T.Counterfeit
OE.AA_MRTD	T.Counterfeit
OE.Authoriz_Sens_Data	T.Read_Sensitive_Data
OE.Passive_Auth_Sign	T.Forgery
OE.Personalisation	T.Forgery
OE.Terminal	T.Forgery
OE.Travel_Document_Holder	T.Skimming, T.Tracing
OE.Exam_Travel_Document	T.Forgery, T.Counterfeit
OE.Ext_Insp_Systems	T.Read_Sensitive_Data
OE.Prot_Logical_Travel_Document	
OE.Polymorphic_Auth	
OE.Authoriz_Polymorphic_Data	T.Sensitive_Polymorphic_Data
OE.Insp_Sys_Polymorphic	
OE.Personalisation_Polymorphic	

Table 2 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.Manufact	OT.Identification	Section 4.3.2
P.Pre-Operational	OT.Identification, OT.AC_Pers, OE.Personalisation, OE.Legislative_Compliance	Section 4.3.2
P.Card_PKI	OE.Passive_Auth_Sign	Section 4.3.2
P.Trustworthy_PKI	OE.Passive_Auth_Sign	Section 4.3.2
P.Terminal	OE.Terminal, OE.Exam_Travel_Document	Section 4.3.2
P.Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 4.3.2
P.Personalisation	OT.AC_Pers, OT.Identification, OE.Personalisation	Section 4.3.2
P.Polymorphic_Data	OT.Polymorphic_Data_Confidentiality, OT.Polymorphic_Data_Privacy, OE.Authoriz_Polymorphic_Data	Section 4.3.2
P.Pre-Operational_Polymorphic	OT.AC_Pers_Polymorphic, OE.Polymorphic_Auth, OE.Authoriz_Polymorphic_Data, OE.Insp_Sys_Polymorphic, OE.Personalisation_Polymorphic	Section 4.3.2
P.Polymorphic_Authentication_Terminal	OE.Insp_Sys_Polymorphic	Section 4.3.2
P.Personalisation_Polymorphic	OT.AC_Pers_Polymorphic, OE.Personalisation_Polymorphic	Section 4.3.2

Table 3 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
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
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.DoS	
OE.Legislative_Compliance	P.Pre-Operational
OE.Auth_Key_Travel_Document	
OE.Auth_Key_MRTD	
OE.AA_MRTD	
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.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.Pre-Operational_Polymorphic, P.Polymorphic_Authentication_Terminal
OE.Personalisation_Polymorphic	P.Pre-Operational_Polymorphic, P.Personalisation_Polymorphic

Table 4 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.Passive_Auth	OE.Passive_Auth_Sign, OE.Exam_Travel_Document	Section 4.3.3
A.Insp_Sys	OE.Exam_Travel_Document, OE.Prot_Logical_Travel_Document, OE.AA_MRTD	Section 4.3.3
A.Auth_PKI	OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 4.3.3
A.Polymorphic_Auth	OE.Polymorphic_Auth	Section 4.3.3
A.Auth_PKI_Polymorphic	OE.Authoriz_Polymorphic_Data	Section 4.3.3
A.Insp_Sys_Polymorphic	OE.Insp_Sys_Polymorphic	Section 4.3.3
A.Pers_Agent_AA	OE.Personalisation	Section 4.3.3

Table 5 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.Auth_Key_MRTD	
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	A.Insp_Sys
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	

Table 6 Security Objectives for the Operational Environment and Assumptions - Coverage

5 Extended Requirements

5.1 Definition of the Family FAU_SAS

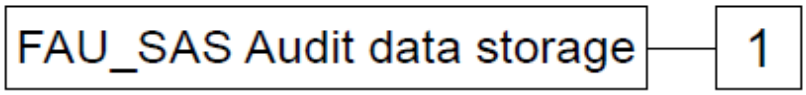
To describe the security functional requirements of the TOE, the family FAU_SAS of the class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the 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:

Family behavior:

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

Component leveling:



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

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

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

FAU_SAS.1 Audit Storage

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.2 Definition of the Family FCS_RND

To describe the IT security functional requirements of the TOE, the family FCS_RND of the class FCS (Cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is not limited to generation

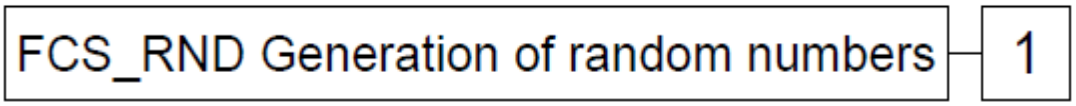
of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

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

Family behavior:

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

Component leveling:



FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

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

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

FCS_RND.1 Quality Metric for Random Numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.3 Definition of the Family FIA_API

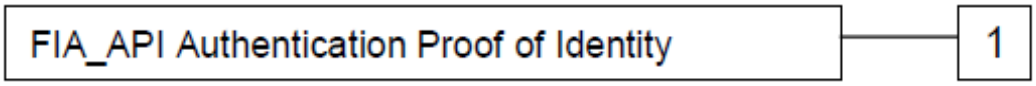
To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external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

The family "Authentication Proof of Identity (FIA_API)" is specified as follows:

Family behavior:

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

Component levelling:



FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.4 Definition of the Family FMT_LIM

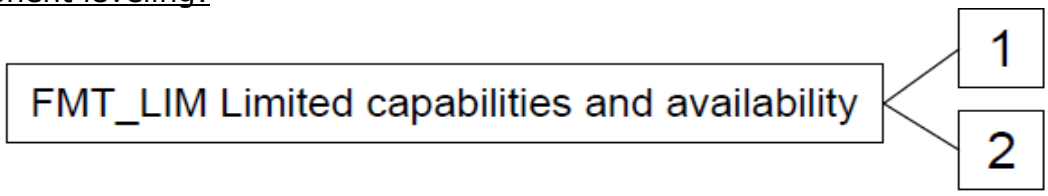
The family FMT_LIM describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class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

The family "Limited capabilities and availability (FMT_LIM)" is specified as follows:

Family behavior:

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

Component leveling:



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

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's lifecycle.

Management: FMT_LIM.1, FMT_LIM.2
There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2
There are no actions defined to be auditable.

FMT_LIM.1 Limited Capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

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].

FMT_LIM.2 Limited Availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 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].

5.5 Definition of the Family FPT_EMS

The 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 secret data stored in and used by the TOE 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, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2.
The family "TOE Emanation (FPT_EMS)" is specified as follows:

Family behavior:

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMS TOE emanation	1

FPT_EMS.1 TOE emanation has two constituents:
FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

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

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

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6 Security Requirements

6.1 Security Functional Requirements

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality. Several SFRs of the PACE PP [PACE-PP] are only listed in the EAC PP [EAC-PP-V2]. Therefore the descriptions of these SFRs are taken directly from PACE PP into the Security target on hand

Definition of security attributes:

Security attribute	Values	Meaning
terminal authentication status	none (any Terminal)	default role
	CVCA	roles defined in the certificate used for authentication (cf. [TR-03110-1]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	roles defined in the certificate used for authentication (cf. [TR-03110-1]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1
	DV (foreign)	roles defined in the certificate used for authentication (cf. [TR-03110-1]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 and TA v.1
	IS	roles defined in the certificate used for authentication (cf. [TR-03110-1]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	none	-
	DG4 (Iris)	Read access to DG4: (cf. [TR-03110-1])
	DG3 (Fingerprint)	Read access to DG3: (cf. [TR-03110-1])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: (cf. [TR-03110-1])
Terminal Authorization	Randomized PP	Read access to the randomized value of PP after successful executed PACE with PIN, CAv1, TAv1 and PMA(PP)
Terminal Authorization	Randomized PP and PI	Read access to the randomized value of PP and PI after successful executed PACE with PIN, CAv1, TAv1 and PMA(PIP)
Terminal Authorization	Randomized CPI	Read access to the randomized value of CPI after successful executed PACE with PIN, CAv1, TAv1 and PMA(CPI)

The following table provides an overview of the keys and certificates used:

Name	Data
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Country Verifying Certification Authority Private Key (SKCVCA)	The Country Verifying Certification Authority (CVCA) holds a private key (SKCVCA) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PKCVCA)	The TOE stores the Country Verifying Certification Authority Public Key (PKCVCA) as part of the TSF data to verify the Document Verifier Certificates. The PKCVCA has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (CCVCA)	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [TR-03110-1] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PKCVCA) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (CDV)	The Document Verifier Certificate CDV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PKDV) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security
Inspection System Certificate (CIS)	The Inspection System Certificate (CIS) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PKIS), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SKICC, PKICC) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Public Key (PKICC)	The Chip Authentication Public Key (PKICC) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication v.1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SKICC)	The Chip Authentication Private Key (SKICC) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the Issuing State or Organization signs the Document Signer Public Key Certificate(CDS) with the Country Signing Certification Authority Private Key (SKCSCA)and the signature will be verified by Receiving State or Organization (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key (PKCSCA). The CSCA also issues the self-signed CSCA Certificate (CCSCA) to be distributed by strictly secure diplomatic means, see [ICAO-9303], 5.5.1.
Document Signer Key Pairs and Certificates	The Document Signer Certificate CDS is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key (PKDS) as authentication reference data. The Document Signer acting under the policy of the CSCA signs the Document Security Object (SOD) of the travel document with the Document Signer Private Key (SKDS) and the signature will be verified by a terminal as the Passive Authentication with the Document Signer Public Key (PKDS)

Chip Authentication Session Key	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
PACE Session Keys (PACE-KMAC, PACE-KEnc)	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) or3DES Keys for message authentication and message encryption (both CBC) agreed between the TOE and a terminal as result of the PACE Protocol, see [ICAO_SAC].
PACE authentication ephemeral key pair (ephem-SKPICC-PACE,ephem-PKPICC-PACE)	The ephemeral PACE Authentication Key Pair (ephem-SKPICC-PACE, ephem-PKPICC-PACE) is used for Key Agreement Protocol: Diffie-Hellman (DH) according to PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03111 [TR-03111], cf. [ICAO_SAC].

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality. Several SFRs of the PACE PP [PACE-PP] are only listed in the EAC PP [EAC-PP-V2]. Therefore the descriptions of these SFRs are taken directly from PACE PP into the Security target on hand.

6.1.1 Class Cryptographic Support (FCS)

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

6.1.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1/DH_PACE Cryptographic key generation

FCS_CKM.1.1/DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH compliant to [TR-03111]** and specified cryptographic key sizes **192, 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] part 11**.

FCS_CKM.1/CA Cryptographic key generation

FCS_CKM.1.1/CA [Editorially Refined] The TSF shall generate cryptographic keys in accordance with the specified cryptographic key generation algorithm **Chip Authentication Protocol Version 1[TR-03110-1] based on the ECDH protocol compliant to [TR-03111]** with 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**

and

based on the Diffie-Hellman protocol compliant to [RSA-PKCS3] and [TR-03110-1] with specified cryptographic key size of **2048 bits in combination with 112 bits 3DES or 128, 192 or 256 bits AES**

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**.

6.1.1.2 Cryptographic operation (FCS_COP.1)

The TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/PACE_ENC Cryptographic operation

FCS_COP.1.1/PACE_ENC The TSF shall perform **secure messaging - encryption and decryption**

in accordance with a specified cryptographic algorithm **3DES and AES in CBC mode** and cryptographic key sizes **respectively 112 and 128, 192 and 256** that meet the following: **compliant to [ICAO-9303] part 11**.

FCS_COP.1/PACE_MAC Cryptographic operation

FCS_COP.1.1/PACE_MAC The TSF shall perform **secure messaging - message authentication code**

in accordance with a specified cryptographic algorithm **Retail-MAC and CMAC** and cryptographic key sizes **respectively 112 and 128, 192, 256** that meet the following: **compliant to [ICAO-9303] part 11**.

FCS_COP.1/CA_ENC Cryptographic operation

FCS_COP.1.1/CA_ENC The TSF shall perform **secure messaging encryption and decryption** in accordance with a specified cryptographic algorithm **3DES and AES in CBC mode** and cryptographic key sizes **respectively 112 and 128, 192 and 256** that meet the following: **[TR-03110-1]**.

FCS_COP.1/SIG_VER Cryptographic operation

FCS_COP.1.1/SIG_VER The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **ECDSA** and cryptographic key sizes **192, 224, 256, 320, 384, and 512 bits** that meet the following: **ISO15946-2 specified in [ISO15946-2], in combination SHA1, SHA224, SHA256, SHA384, SHA512 digest algorithms**.

FCS_COP.1/SIG_GEN Cryptographic operation

FCS_COP.1.1/SIG_GEN The TSF shall perform **digital signature generation** in accordance with a specified cryptographic algorithm **ECDSA and RSA** and cryptographic key sizes **192, 224, 256, 320, 384, 512 and 521 bits for ECDSA and 1024, 1536, 1792**,**2048, 3072 and 4096 bits for RSA** that meet the following: **ISO15946-2 specified in [ISO15946-2] for ECDSA and ISO9796-2 specified in [ISO9796-2] for RSA, in combination with SHA1, SHA224, SHA256, SHA384 and SHA512 digest algorithms specified in [NIST-180-4] for both ECDSA and RSA signatures**.

Application Note:

This SFR has been added to this ST in order to support the signing of challenges generated by the Inspection System as part of the optional Active Authentication protocol specified in [ICAO-9303].

FCS_COP.1/CA_MAC Cryptographic operation

FCS_COP.1.1/CA_MAC The TSF shall perform **secure messaging message authentication code** in accordance with a specified cryptographic algorithm **3DES Retail-MAC and AES CMAC** and cryptographic key sizes **112 bits 3DES and 128, 192 and 256 bits AES** that meet the following: **[ICAO-9303] for 3DES Retail-MAC and [NIST-800-38B] for AES CMAC**.

6.1.1.3 Random Number Generation (FCS_RND.1)

FCS_RND.1 Quality metric for random numbers

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

6.1.1.4 Additional SFRs for Polymorphic eMRTD

FCS_COP.1/POLY Cryptographic operation

FCS_COP.1.1/POLY 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 identitity 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_CKM.1/POLY Cryptographic key generation

FCS_CKM.1.1/POLY 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.

6.1.2 Class FIA Identification and Authentication

FIA_AFL.1/PACE Authentication failure handling

FIA_AFL.1.1/PACE 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/PACE When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **wait a linear increasing time, starting at a minimum of 1 s, before the next authentication attempt can be performed**.

Application Note:

Note here, the PACE password could be a MRZ, CAN, PIN or PUK.

FIA_UID.1/PACE Timing of identification

FIA_UID.1.1/PACE The TSF shall allow

1. to establish the communication channel,

2. carrying out the PACE Protocol 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/PACE The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/PACE Timing of authentication

FIA_UAU.1.1/PACE The TSF shall allow

1. to establish the communication channel,

2. carrying out the PACE Protocol 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. to carry out Personalisation Agent Authentication based on a symmetric mechanism according to [ICA0-9303] for 3DES and [ISO18013-3] for AES-128, -192 and 256

8. None

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

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

FIA_UAU.4/PACE Single-use authentication mechanisms

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

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].

FIA_UAU.5/PACE Multiple authentication mechanisms

FIA_UAU.5.1/PACE 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/PACE 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 either the authentication mechanism and secure messaging protocol defined in [ICAO-9303] for 112 bits 3DES

or

ISO18013 BAP authentication mechanism defined in [ISO18013-3] for AES-128, 192 or 256 bits using AES secure messaging (CMAC, IV value, tags) as specified in EAC TR-03110 [TR-03110-1]

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/EAC Re-authenticating

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

FIA_UAU.6/PACE Re-authenticating

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

FIA_UID.1/PACE_CAM Timing of identification

FIA_UID.1.1/PACE_CAM 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/PACE_CAM 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/PACE_CAM The TSF shall allow **in addition 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/PACE_CAM 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/PACE_CAM 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/PACE_CAM The TSF shall provide

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

to support user authentication.

FIA_UAU.5.2/PACE_CAM 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/PACE_CAM 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.**

FMT_MTD.1/PACE_CAM_KEY_READ Management of TSF data

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

a. **PACE passwords**
b. **Modular invert of the CA key**

to **none**.

FMT_MTD.1/PACE_CAM_KEY_WRITE Management of TSF data

FMT_MTD.1.1/PACE_CAM_KEY_WRITE The TSF shall restrict the ability to **write** the **Modular invert of the CA key** to **Personalization Agent**.

FIA_API.1/CA Authentication Proof of Identity

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

FIA_API.1/AA Authentication Proof of Identity

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

6.1.2.1 Additional SFRs for Polymorphic eMRTD

FIA_AFL.1/Suspend_PIN Authentication failure handling

FIA_AFL.1.1/Suspend_PIN The TSF shall detect when **an administrator configurable positive integer within 3 to 15** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts using the PIN as the shared password for PACE**.

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

Application Note:

This SFR is included from [EACv2-PP]. This SFR is not in conflict to FIA_AFL.1/PACE from [PACE-PP], since it just adds a requirement specific to the

case where the PIN is the shared password. Thus the assigned integer number for unsuccessful authentication attempts with any PACE password could be different to the integer for the case when using a PIN.

Resuming is a two-step procedure, subsequently using PACE with the CAN and VERIFY PIN. It must be implemented according to [TR-03110-2], and is relevant for the status as required by FIA_AFL.1/Suspend_PIN. The polymorphic eMRTD Document holder is authenticated as required by FIA_UAU.1/PACE using the PIN as the shared password.

FIA_AFL.1/Suspend_PUK Authentication failure handling

FIA_AFL.1.1/Suspend_PUK The TSF shall detect when **an administrator configurable positive integer within 3 to 15** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts using the PUK as the shared password for PACE**.

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

Application Note:

This SFR is not in conflict to FIA_AFL.1/PACE from [PACE-PP], since it just adds a requirement specific to the case where the PUK is the shared password. Thus the assigned integer number for unsuccessful authentication attempts with any PACE password could be different to the integer for the case when using a PUK.

Resuming is a two-step procedure, subsequently using PACE with the CAN and VERIFY PUK. It must be implemented according to [TR-03110-2], and is relevant for the status as required by FIA_AFL.1/Suspend_PUK. The polymorphic eMRTD Document holder is authenticated as required by FIA_UAU.1/PACE using the PUK as the shared password.

FIA_AFL.1/Block_PIN Authentication failure handling

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

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

Application Note:

This SFR is included from [EACv2-PP]. This SFR is not in conflict to FIA_AFL.1 from [PACE-PP], since it just adds a requirement specific to the case where the PIN is the shared password.

FIA_AFL.1/Block_PUK Authentication failure handling

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

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

Application Note:

This SFR is not in conflict to FIA_AFL.1 from [PACE-PP], since it just adds a requirement specific to the case where the PUK is the shared password.

FIA_UID.1/POLY Timing of identification

FIA_UID.1.1/POLY 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/POLY 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/POLY 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_UAU.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/POLY 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/POLY 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/POLY 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/POLY 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/POLY 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**.

6.1.3 Class FDP User Data Protection

FDP_ACC.1/TRM Subset access control

FDP_ACC.1.1/TRM The TSF shall enforce the **Access Control SFP** on **terminals gaining access to the eMRTD User Data (data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM) and sensitive eMRTD user data (DG3 and DG4)**.

FDP_ACF.1/TRM Security attribute based access control

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

1. **Subjects:**
   a. **Terminal,**
   b. **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 eMRTD User Data,**
   b. **data in EF.DG3 of the sensitive eMRTD,**
   c. **data in EF.DG4 of the sensitive eMRTD,**
   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/TRM 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.1.1/TRM according to [ICAO-9303] part 11 after a successful PACE authentication as required by FIA_UAU.1/PACE**.

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

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

1. **Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any eMRTD 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_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 (PACE-KMAC, PACE-KEnc), (CA-KMAC, CA-KEnc) (immediately after closing related communication session),

2. the ephemeral private key ephem - SK PICC- PACE (by having generated a DH shared secret K).

3. None.

FDP_UCT.1/TRM Basic data exchange confidentiality

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

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

6.1.3.1 Additional SFRs for Polymorphic eMRTD

FDP_RIP.1/POLY Subset residual information protection

FDP_RIP.1.1/POLY 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 and EACv1 PPs.

FDP_ACC.1/POLY Subset access control

FDP_ACC.1.1/POLY 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 [EACv1-PP] 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 and EACv1 PPs.

FDP_ACF.1/POLY Security attribute based access control

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

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

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

3. **Security attributes:**
   a. **PACE Authentication**
   b. **Chip Authentication v1 (CAv1)**
   c. **Terminal Authentication v1 (TAv1)**
   d. **Authorisation of the Terminal**

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

- **only an authenticated personalization 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/POLY The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/POLY 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 personalization 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.**

Application Note:

A Polymorphic eMRTD Document Holder can consciously enter his authentication credentials to the Polymorphic Authentication Terminal for granting access to his Polymorphic ID attributes and the PIN Management functions:

- PIN (used for Polymorphic eMRTD Document Holder verification (FIA_UAU.1.1/POLY) for
  - PMA,
  - Change PIN and
  - PIN Resume)
- PUK (used for Polymorphic eMRTD Document Holder verification (FIA_UAU.1.1/POLY) for
  - Unblock PIN,
  - Change PIN and
  - PIN Resume)

6.1.4 Class FTP Trusted Path/Channels

FTP_ITC.1/PACE Inter-TSF trusted channel

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

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

FTP_ITC.1.3/PACE [Editorially Refined] The TSF shall ~~initiate~~ **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 and EACv1 PPs.

6.1.5 Class FAU Security Audit

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide **the Manufacturer** with the capability to store **initialisation and pre-personnalization data** in the audit records.

6.1.6 Class FMT Security Management

The SFR FMT_SMR.1/PACE provides basic requirements to the management of the TSF data.

The TOE shall meet the requirement 'Security roles (FMT_SMR.1)' as specified below (Common Criteria Part 2).

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 (if any).**

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 and EACv1 PPs.

FMT_SMR.1/PACE Security roles

FMT_SMR.1.1/PACE The TSF shall maintain the roles

1. **Manufacturer,**
2. **Personalisation Agent,**
3. **Terminal,**

4. **PACE authenticated BIS-PACE,**
5. **Country Verifying Certification Authority,**
6. **Document Verifier,**
7. **Domestic Extended Inspection System**
8. **Foreign Extended Inspection System**.

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

FMT_LIM.1 Limited capabilities

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

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

FMT_LIM.2 Limited availability

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

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

FMT_MTD.1/INI_ENA Management of TSF data

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

FMT_MTD.1/INI_DIS Management of TSF data

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

FMT_MTD.1/PA Management of TSF data

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

FMT_MTD.1/CVCA_INI Management of TSF data

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

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

to **Personalization Agent**.

FMT_MTD.1/CVCA_UPD Management of TSF data

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

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

to **Country Verifying Certification Authority**.

FMT_MTD.1/DATE Management of TSF data

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

1. **Country Verifying Certification Authority,**
2. **Document Verifier,**
3. **Domestic Extended Inspection System**.

FMT_MTD.1/CAPK Management of TSF data

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

Application Note:

The TOE supports only secure loading of the Chip Authentication Private Key. Secure loading of the Chip Authentication Private Key is restricted by the TOE to the Personalisation Agent only.

FMT_MTD.1/AAPK Management of TSF data

FMT_MTD.1.1/AAPK The TSF shall restrict the ability to **load** the **Active Authentication Private Key** to **Personalization Agent**.

FMT_MTD.1/KEY_READ Management of TSF data

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

1. PACE passwords,

2. Chip Authentication Private Key,

3. Personalisation Agent Keys

4. Active Authentication Private Key

5. 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 EACv1 PP [EAC1PP] and extends it by 5. 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 and EACv1 PPs.

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

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.

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.

6.1.6.1 Additional SFRs for Polymorphic eMRTD

FMT_SMR.1/POLY Security roles

FMT_SMR.1.1/POLY 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/POLY The TSF shall be able to associate users with roles.

FMT_LIM.1/POLY Limited capabilities

FMT_LIM.1.1/POLY 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 availability

FMT_LIM.2.1/POLY 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/Initialize_PIN Management of TSF data

FMT_MTD.1.1/Initialize_PIN 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/Change_PIN 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] and refined for PIN management according to [PCA-eMRTD].

FMT_MTD.1/Unblock_PIN Management of TSF data

FMT_MTD.1.1/Unblock_PIN The TSF shall restrict the ability to **unblock** the **blocked PIN** to

- **the Polymorphic eMRTD document holder (using the PUK for unblocking and changing) according to [PCA-eMRTD].**

Application Note:

This SFR is included from [EACv2-PP] and refined for PIN management according to [PCA-eMRTD].

FMT_MTD.1/Resume_PIN Management of TSF data

FMT_MTD.1.1/Resume_PIN The TSF shall restrict the ability to **resume** the **suspended PIN or PUK** 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. It must be implemented according to [TR03110-2] and [PCA-eMRTD], and is relevant for the status as required by FIA_AFL.1/Suspend_PIN and FIA_AFL.1/Suspend_PUK. The polymorphic eMRTD Document holder is authenticated as required by FIA_UAU.1/PACE using the CAN as the shared password and FIA_UAU.1/VERIFY.

FMT_MTD.1/PI_PP_CPI_Load Management of TSF data

FMT_MTD.1.1/PI_PP_CPI_Load The TSF shall restrict the ability to **load** the **PI, PP and CPI data** to **the personalization 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/PI_PP_CPI_Read 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.

6.1.7 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. The SFRs 'Limited capabilities (FMT_LIM.1)', 'Limited availability (FMT_LIM.2)' together with the SAR 'Security architecture description' (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions. The TOE shall meet the requirement 'TOE Emanation (FPT_EMS.1)' as specified below (Common Criteria Part 2 extended).

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **variations in power consumption or variations in timing 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 invert 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,**

and **none**

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-K.Enc),**
3. **the ephemeral private key ephem SK PICC-PACE,**
4. **Active Authentication Private Key,**
5. **Personalisation Agent Key(s) and**
6. **Chip Authentication Private Key,**
7. **Modular invert 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,**

and **none**.

Application Note:

This SFR covers the definition in EACv1 PP [EAC1PP] 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 EACv1 and PACE PPs.

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_TST.1 TSF testing

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

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

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

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.

6.1.8 Class FPR

6.1.8.1 Additional SFRs for Polymorphic eMRTD

FPR_ANO.1 Anonymity

FPR_ANO.1.1 [Editorially Refined] The TSF shall ensure that **no subjects** are able to determine the real value of PI, PP and CPI data 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.**

6.2 Security Assurance Requirements

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

6.3 Security Requirements Rationale

6.3.1 Security Objectives for the TOE

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 SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The Personalisation Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE (FIA_UID.1/PACE_CAM and FIA_UAU.1/PACE_CAM for PACE CAM protocol) before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE (FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM for PACE CAM protocol) 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 FDP_UCT.1/TRM and 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 (FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM PACE_CAM Authentication) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE (FIA_UAU.5/PACE_CAM, FIA_UAU.6/PACE_CAM for PACE CAM) 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 (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENCand 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 FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ requires that the Active Authentication Key cannot be written unauthorized or read afterwards. The SFR FMT_MTD.1/PACE_CAM_KEY_WRITE and FMT_MTD.1/PACE_CAM_KEY_READ requires that the modular invert of the CA 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 (FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM for PACE CAM) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE (FIA_UAU.5/PACE_CAM, FIA_UAU.6/PACE_CAM for PACE CAM) resp. FIA_UAU.6/EAC. 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 (FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM and FCS_CKM.4 for PACE CAM) represent some required specific properties of the protocols used. The SFR FMT_MTD.1/KEY_READ restricts the access to the PACE passwords, the Chip Authentication Private Key and the Active Authentication Private Key. The SFR FMT_MTD.1/PACE_CAM_KEY_READ restricts the access to the PACE passwords and the modular invert of the CA key. FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The SFR FCS_RND.1 represents a general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

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 (FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM for PACE CAM) 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 (FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM for PACE CAM) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE (FIA_UAU.5/PACE_CAM, FIA_UAU.6/PACE_CAM for PACE CAM) 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, the Chip Authentication Private Key and the Active Authentication Private Key. The SFR FMT_MTD.1/PACE_CAM_KEY_READ restricts the access to the PACE passwords and the modular invert of the CA key. FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy. The SFR FCS_RND.1 represents the general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

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/contact-based interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ, PIN, PUK). This objective is achieved as follows:

1. While establishing PACE communication with CAN, MRZ or PUK (non-blocking authentication / authorization data) by FIA_AFL.1/PACE,
2. while establishing PACE communication using the PIN (blocking authentication data) by FIA_AFL.1/Block_PIN,
3. for listening to PACE communication and for establishing CAv1 communication by FTP_ITC.1/PACE,
4. and for listening to CAv1 communication by FTP_ITC.1/Polymorphic. The trusted channel shall be established by performing the PACE, CAv1 and TAv1 protocols according to [TR03110TR-03110] and the Polymorphic Authentication protocol (PMA).

OT.Prot_Abuse-Func The security objective OT.Prot_Abuse-Func "Protection against Abuse of Functionality" is ensured by the SFRs 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 SFRFPT_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 set). 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_UID.1/PACE_CAM for PACE CAM), FIA_UAU.1/PACE (FIA_UAU.1/PACE_CAM for PACE CAM), 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 SOD and, in generally, personalization 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 (FMT_MTD.1/PACE_CAM_KEY_READ for PACE CAM protocol) and FPT_EMS.1 restrict the access to the Personalisation Agent Keys, the Chip Authentication Private Key and the Active Authentication Private key. The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFRs FIA_UAU.4/PACE and FIA_UAU.5/PACE (FIA_UAU.4/PACE_CAM and FIA_UAU.5/PACE_CAM for PACE CAM). If the Personalisation Terminal wants 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 the 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.

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 (FIA_UID.1/PACE_CAM and FIA_UAU.1/PACE_CAM for PACE CAM) 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 (or FIA_UAU.5/PACE_CAM for PACE CAM). During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE (FIA_UAU.4/PACE_CAM for PACE CAM). 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), 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 FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ requires that the Active Authentication Key cannot be written unauthorized or read afterwards. The SFR FMT_MTD.1/PACE_CAM_KEY_WRITE and FMT_MTD.1/PACE_CAM_KEY_READ requires that the modular invert of the CA 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 Protocolv.1 provided by FIA_API.1/CA and by Active Authentication provided by FIA_API.1/AA proving the identity of the TOE. The Chip Authentication Protocolv.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 Protocolv.1 [TR-03110-1] 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. The Active Authentication defined by FCS_COP.1/SIG_GEN for the generation of the RSA Signature is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ. According to FDP_ACF.1, only the successfully authenticated Inspection Systems are allowed to request active authentication (FDP_ACF.1.2, rule 2).

OT.Polymorphic_Data_Confidentiality: SFRs that contribute to meet this objective are mentioned in table 7.

OT.Polymorphic_Data_Integrity: SFRs that contribute to meet this objective are mentioned in table 7.

OT.Polymorphic_Data_Authenticity: SFRs that contribute to meet this objective are mentioned in table 7.

OT.Polymorphic_Data_Privacy: SFRs that contribute to meet this objective are mentioned in table 7.

OT.AC_Pers_Polymorphic: SFRs that contribute to meet this objective are mentioned in table 7.

OT.DoS: SFRs that contribute to meet this objective are mentioned in table 7.

6.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.Data_Integrity	FCS_CKM.1/DH_PACE, FCS_CKM.4, FCS_COP.1/PACE_MAC, FIA_UAU.6/PACE, FIA_UAU.6/PACE_CAM, FDP_RIP.1, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FTP_ITC.1/PACE, FMT_SMF.1, FMT_MTD.1/PA, FPT_PHP.3, FCS_CKM.1/CA, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM, FIA_UAU.6/EAC, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FMT_SMR.1/PACE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.1/AAPK, FMT_MTD.1/PACE_CAM_KEY_READ, FMT_MTD.1/PACE_CAM_KEY_WRITE, FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Suspend_PUK, FIA_AFL.1/Block_PUK	Section 6.3.1
OT.Data_Authenticity	FCS_CKM.1/DH_PACE, FCS_CKM.4, FCS_COP.1/PACE_MAC, FIA_UAU.6/PACE, FIA_UAU.6/PACE_CAM, FDP_RIP.1, FTP_ITC.1/PACE, FMT_SMF.1, FMT_MTD.1/PA, FCS_CKM.1/CA, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM, FIA_UAU.6/EAC, FMT_SMR.1/PACE, FMT_MTD.1/KEY_READ, FMT_MTD.1/PACE_CAM_KEY_READ, FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Suspend_PUK, FIA_AFL.1/Block_PUK	Section 6.3.1
OT.Data_Confidentiality	FCS_CKM.1/DH_PACE, FCS_CKM.4, FCS_COP.1/PACE_ENC, FIA_UAU.6/PACE, FIA_UAU.6/PACE_CAM, FDP_RIP.1, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FTP_ITC.1/PACE, FMT_SMF.1, FMT_MTD.1/PA, FCS_CKM.1/CA, FCS_COP.1/CA_ENC, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM, FIA_UAU.6/EAC, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FMT_SMR.1/PACE, FMT_MTD.1/KEY_READ, FMT_MTD.1/PACE_CAM_KEY_READ, FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Suspend_PUK, FIA_AFL.1/Block_PUK,	Section 6.3.1
OT.Tracing	FIA_AFL.1/PACE, FTP_ITC.1/PACE, FIA_AFL.1/Block_PIN, FIA_AFL.1/Block_PUK	Section 6.3.1
OT.Prot_Abuse-Func	FMT_LIM.1, FMT_LIM.2, FMT_LIM.1/POLY, FMT_LIM.2/POLY	Section 6.3.1
OT.Prot_Inf_Leak	FPT_FLS.1, FPT_TST.1, FPT_PHP.3, FPT_EMS.1	Section 6.3.1
OT.Prot_Phys-Tamper	FPT_PHP.3	Section 6.3.1
OT.Prot_Malfunction	FPT_FLS.1, FPT_TST.1	Section 6.3.1
OT.Identification	FMT_SMF.1, FMT_MTD.1/INI_ENA, FAU_SAS.1, FMT_SMR.1/PACE, FMT_MTD.1/INI_DIS	Section 6.3.1

OT.AC_Pers	FMT_SMF.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/PA, FAU_SAS.1, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_ENC, FCS_COP.1/CA_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_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM, FIA_UAU.6/EAC, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FMT_SMR.1/PACE, FMT_MTD.1/KEY_READ, FPT_EMS.1, FMT_MTD.1/INI_DIS, FMT_MTD.1/PACE_CAM_KEY_READ	Section 6.3.1
OT.Sens_Data_Conf	FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_ENC, FCS_COP.1/CA_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_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM, FIA_UAU.6/EAC, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_UCT.1/TRM, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.1/PACE_CAM_KEY_READ, FMT_MTD.1/PACE_CAM_KEY_WRITE FMT_MTD.3, FMT_MTD.1/AAPK, FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Suspend_PUK, FIA_AFL.1/Block_PUK	Section 6.3.1
OT.Chip_Auth_Proof	FCS_CKM.1/CA, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FIA_API.1/CA, FMT_MTD.1/AAPK, FIA_API.1/AA, FCS_COP.1/SIG_GEN	Section 6.3.1
OT.Polymorphic_Data_Confidentiality	FCS_CKM.1/DH_PACE, FCS_COP.1/SIG_VER, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_RND.1, FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Suspend_PUK, FIA_AFL.1/Block_PUK, FIA_UID.1/POLY, FIA_UAU.1/POLY, FIA_UAU.4/POLY, FIA_UAU.6/EAC, FDP_RIP.1/POLY, FDP_RIP.1, FDP_ACC.1/POLY, FDP_ACF.1/POLY, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FTP_ITC.1/PACE, FMT_SMF.1, FMT_SMR.1/POLY, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/PA, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.1/PI_PP_CPI_Read, FMT_MTD.1/PI_PP_CPI_Load, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Resume_PIN, FCS_CKM.1/CA, FIA_UAU.6/POLY, FMT_MTD.3, FCS_CKM.4, FIA_UAU.5/POLY, FCS_CKM.1/POLY, FCS_COP.1/POLY	Section 6.3.1
OT.Polymorphic_Data_Integrity	FCS_CKM.1/DH_PACE, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_RND.1, FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Suspend_PUK, FIA_AFL.1/Block_PUK, FIA_UID.1/POLY, FIA_UAU.1/POLY, FIA_UAU.4/POLY, FIA_UAU.6/EAC, FDP_RIP.1/POLY, FDP_RIP.1, FDP_ACC.1/POLY, FDP_ACF.1/POLY, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_UCT.1/TRM, FDP_UIT.1/TRM,	Section 6.3.1

	FTP_ITC.1/PACE, FMT_SMF.1, FMT_SMR.1/POLY, FMT_MTD.1/PA, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FPT_PHP.3, FMT_MTD.1/PI_PP_CPI_Read, FMT_MTD.1/PI_PP_CPI_Load, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Resume_PIN, FCS_CKM.1/CA, FIA_UAU.6/POLY, FCS_CKM.4, FIA_UAU.5/POLY, FCS_CKM.1/POLY, FCS_COP.1/POLY	
OT.Polymorphic_Data_Authenticity	FCS_CKM.1/DH_PACE, FCS_COP.1/PACE_MAC, FCS_RND.1, FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Suspend_PUK, FIA_AFL.1/Block_PUK, FIA_UID.1/POLY, FIA_UAU.1/POLY, FIA_UAU.4/POLY, FIA_UAU.6/EAC, FIA_AFL.1/PACE, FDP_RIP.1/POLY, FDP_RIP.1, FTP_ITC.1/PACE, FMT_SMF.1, FMT_SMR.1/POLY, 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, FCS_CKM.1/CA, FIA_UAU.6/POLY, FCS_CKM.4, FIA_UAU.5/POLY, FCS_CKM.1/POLY, FCS_COP.1/POLY	Section 6.3.1
OT.Polymorphic_Data_Privacy	FCS_CKM.1/DH_PACE, FCS_COP.1/POLY, FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Suspend_PUK, FIA_AFL.1/Block_PUK, FMT_MTD.1/PI_PP_CPI_Read, FPR_ANO.1, FPR_UNL.1, FCS_CKM.4, FCS_CKM.1/POLY	Section 6.3.1
OT.AC_Pers_Polymorphic	FCS_COP.1/SIG_VER, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_RND.1, FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Suspend_PUK, FIA_AFL.1/Block_PUK, FIA_UID.1/POLY, FIA_UAU.1/POLY, FIA_UAU.4/POLY, FIA_UAU.6/EAC, FDP_ACC.1/POLY, FDP_ACF.1/POLY, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FAU_SAS.1, FMT_SMF.1, FMT_SMR.1/POLY, FMT_MTD.1/PA, FMT_MTD.1/KEY_READ, FPT_EMS.1, FMT_MTD.1/PI_PP_CPI_Load, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Resume_PIN, FCS_CKM.1/CA, FMT_MTD.1/INI_DIS, FMT_MTD.1/INI_ENA, FIA_UAU.6/POLY, FCS_CKM.4, FIA_UAU.5/POLY	Section 6.3.1
OT.DoS	FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Suspend_PUK	Section 6.3.1

Table 7 Security Objectives and SFRs - Coverage

6.3.3 Dependencies

6.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FIA_AFL.1/PACE	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_AFL.1/Suspend_PIN	(FIA_UAU.1)	FIA_UAU.1/POLY
FIA_AFL.1/Suspend_PUK	(FIA_UAU.1)	FIA_UAU.1/POLY
FIA_AFL.1/Block_PIN	(FIA_UAU.1)	FIA_UAU.1/POLY
FIA_AFL.1/Block_PUK	(FIA_UAU.1)	FIA_UAU.1/POLY
FIA_UID.1/PACE	No Dependencies	
FIA_UAU.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FIA_UAU.4/PACE	No Dependencies	
FIA_UAU.5/PACE	No Dependencies	
FIA_UAU.6/EAC	No Dependencies	
FIA_UAU.6/PACE	No Dependencies	
FIA_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_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	
FMT_MTD.1/PACE_CAM_KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/PACE_CAM_KEY_WRITE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FIA_API.1/CA	No Dependencies	
FIA_API.1/AA	No Dependencies	
FDP_ACC.1/TRM	(FDP_ACF.1)	FDP_ACF.1/TRM
FDP_ACF.1/TRM	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/TRM
FDP_RIP.1	No Dependencies	
FDP_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_UCT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/TRM, FTP_ITC.1/PACE
FDP_UIT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/TRM, FTP_ITC.1/PACE
FTP_ITC.1/PACE	No Dependencies	
FAU_SAS.1	No Dependencies	
FMT_SMF.1	No Dependencies	
FMT_SMR.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE, FIA_UID.1/PACE_CAM

FMT_LIM.1	(FMT_LIM.2)	FMT_LIM.2
FMT_LIM.2	(FMT_LIM.1)	FMT_LIM.1
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/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/PA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CVCA_INI	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/DATE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CAPK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/AAPK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.3	(FMT_MTD.1)	FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD
FMT_MTD.1/Initialize_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/POLY
FMT_MTD.1/Change_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/POLY
FMT_MTD.1/Unblock_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/POLY
FMT_MTD.1/Resume_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/POLY
FMT_MTD.1/PI_PP_CPI_Load	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/POLY
FMT_MTD.1/PI_PP_CPI_Read	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/POLY
FPT_EMS.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_TST.1	No Dependencies	
FPT_PHP.3	No Dependencies	
FCS_CKM.1/DH_PACE	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC
FCS_CKM.1/CA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC
FCS_CKM.1/POLY	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/POLY
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/DH_PACE
FCS_COP.1/PACE_ENC	(FCS_CKM.1 or FDP_ITC.1	FCS_CKM.1/DH_PACE,

	or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4
FCS_COP.1/PACE_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_COP.1/CA_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/SIG_VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/SIG_GEN	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/CA_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/POLY	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/POLY, FCS_CKM.4
FCS_RND.1	No Dependencies	
FPR_ANO.1	No Dependencies	
FPR_UNL.1	No Dependencies	

Table 8 SFRs Dependencies

6.3.3.1.1 Rationale for the exclusion of Dependencies

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

6.3.3.2 SARs Dependencies

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

Table 9 SARs Dependencies

6.3.4 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.

6.3.5 AVA_VAN.5 Advanced methodical vulnerability analysis

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.

6.3.6 ALC_DVS.2 Sufficiency of security measures

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

7 TOE Summary Specification

7.1 TOE Summary Specification

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

The TOE provides security features (SF) which can be associated to following groups:

Identification and Authentication mechanisms

Cryptographic functions support

Access control /Storage and protection of logical travel document data

Secure messaging

Security and Life-cycle management

Moreover, the TOE will protect itself against interference, logical tampering and bypass. The security functionality of the TOE respectively the IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) applet will be externally available to the user by APDU commands according to the access conditions specified by the according policies considering the life cycle state, user role and security state.

7.1.1 SF.IA Identification and Authentication

The different authentication mechanisms are supported by APDU commands and parameters using the cryptographic functions provided by the platform. The authentication mechanisms are enforced by protocols and APDU methods as specified in the functional specification.

Note that Symmetric Basic Access Control (BAC) Authentication Mechanism is supported by the TOE but not covered by this Security Target.

The TOE supports the following authentication mechanisms:

- **SF.IA.1:** Password Authenticated Connection Establishment (PACE)
- **SF.IA.2:** EAC Chip Authentication v. 1
- **SF.IA.3:** EAC Terminal Authentication Protocol v.1
- **SF.IA.4:** Authentication of the Personalization Agent with a personalisation key set based on a symmetric authentication mechanism
- **SF.IA.5:** ICAO Active Authentication
- **SF.IA.6:** Optionally PACE with additional Chip Authentication Mapping (PACE CAM)
- **SF.IA.7:** Polymorphic Authentication (PMA)
- **SF.IA.8:** Polymorphic eMRTD Document Holder Verification

7.1.2 SF.CF Cryptographic functions support

Cryptographic function support is provided by the underlying NXP JCOP 3 P60, i.e. the TOE relies on the underlying platform for performing its required cryptographic operations.

SF.CF Cryptographic functions include:

- **SF.CF.1:** 3DES and AES cipher operations for secure messaging
- **SF.CF.2:** Digest calculations (SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512)
- **SF.CF.3:** Signature generation (ECDSA, RSA)
- **SF.CF.4:** Signature verification (ECDSA, RSA)
- **SF.CF.5:** Diffie-Hellman Key Agreement (ECDH and DH)
- **SF.CF.6:** Key Generation (PACE ECDH/DH ephemeral keys and secure messaging MAC and ENC session keys)
- **SF.CF.7:** Key and secret authentication data Destruction
- **SF.CF.8:** True Random Number generation
- **SF.CF.9:** Randomization of PI/PP/CPI data as part of the Polymorphic Authentication protocol (PMA)

7.1.3 SF.ILTB Protection against interference, logical tampering and bypass

SF.ILTB.1

Protection against interference, logical tampering and bypass

Security domains are supported by the Java Card platform used by the TOE underlying NXP JCOP 3 P60. The NXP JCOP 3 P60 provides protection against physical attack and performs self-tests as described in [PLTF-ST].

The platform protects the TOE against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.

The IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) Applet uses transient memory where a hardware reset always reverts the IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) Applet into an unauthenticated state.

7.1.4 SF.AC Access control / Storage and protection of logical travel document data

SF.AC.1

Access control / Storage and protection of logical travel document data

The TOE provided access control, storage and protection of logical travel document data including access control to MRTD data. The TOE implements the subjects, objects, security attributes and rules according to the security attribute based access control. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification.

7.1.5 SF.SM Secure Messaging

SF.SM.1

Secure Messaging

Secure messaging MAC and ENC operations are performed by the TOE's platform.

Secure messaging in ENC_MAC mode is established during PACE or re-established during Chip Authentication v1 and is based on SF.CF.1, 5, 6 and 8.

SF.SM.2

Secure Messaging – Re-authentication

The Retail MAC for 3DES and CMAC for AES are part of every APDU command/response when secure messaging is active after a successful PACE or Chip Authentication has been accomplished. Re-authentication after reset of the SM protocol is assured by accepting only valid (mandatory) MAC or CMAC cryptograms.

7.1.6 SF.LCM Security and life cycle management

SF.LCM.1

Management of phases and roles

For the TOE the following life-cycle phases have been identified:

1. Manufacturing phase
2. Personalisation phase
3. Operational phase
4. Termination phase

Each life-cycle phase (or state) has its typical user acting as role holder.

Life-cycle phase	Role
Manufacturing phase	IC Manufacturer
	MRTD Manufacturer Platform initialisation)
	MRTD Manufacturer (Pre-personalisation)
Personalisation phase	Personalisation Agent
Operational phase	Basic or Extended Inspection system Polymorphic Authentication System Polymorphic eMRTD document holder
Terminated phase	None

All role holders in Manufacturing, Pre-Personalisation and Personalisation phases are identified by cryptographic authentication keys. In Operational phase the PACE password is required to authenticate the Basic or Extended Inspection System in order to get access to the non-sensitive ICAO LDS datagroups.

The IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) Applet maintains the internal life-cycle state the moment that the applet is installed. This state, together with the access control mechanisms force the Terminal into a specific role, for the pre-personalisation and subsequent, personalisation and operational phases. The phases (and corresponding life-cycle states) are controlled by APDU commands.

SF.LCM.2

Life Cycle states of the IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) Applet

The TOE supports the following life-cycle states:

1. Not instantiated (applet resides in ROM or in EEPROM)
2. PRE-PERSONALISATION state
3. PERSONALISATION state
4. OPERATIONAL state
5. TERMINATED state (irreversibly)

Each life-cycle phase (or state) has its typical user acting as role holder.

Life-cycle phase	Life-cycle state (maintained by applet)	Role
Manufacturing phase	- (Applet not instantiated)	IC Manufacturer
	- (Applet not instantiated)	MRTD Manufacturer Platform initialisation)
	PRE-PERSONALISATION	MRTD Manufacturer (Pre-personalisation)
Personalisation phase	PERSONALISATION	Personalisation Agent
Operational phase	OPERATIONAL	Basic or Extended Inspection system Polymorphic Authentication System Polymorphic eMRTD document holder
Terminated phase	TERMINATED	None

SF.LCM.3

Management of TSF-Data

The TOE allows only in its PERSONALISATION life-cycle state TSF data to be written onto the TOE.

In OPERATIONAL life-cycle state the management of TSF-Data can only be performed:

- After successful Terminal Authentication. Updating the Country Verifier Certification Authority Public Key and Certificate is restricted to the Country Verifier Certification Authority. Modifying the Current Date is restricted to the Country Verifier Certification Authority, the Document Verifier and the domestic Extended Inspection System.
- After verification of the user PIN or PUK by issuing a dedicated PIN change command (RRC).

SF.LCM.4

Protection of test features

The IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) Applet does not have any dedicated test features implemented.

The test features of the NXP JCOP 3 P60 are protected by ways described in [PLTF-ST] and guidance documentation.

SF.LCM.5

Protection of keys and PACE passwords

In PRE-PERSONALISATION life-cycle state personalisation Agent Key Set is installed on the TOE's platform and protected by the platform.

In all TOE life-cycle states the Personalization Agent Key set (MAC, ENC, KEK), the PACE passwords (derived from MRZ, CAN, PIN or PUK), the Chip Authentication Private Key, the Active Authentication Private Key are protected from disclosure. The IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) Applet only stores keys in Java Card specified Key structures, which are protected by NXP JCOP 3 P60.

SF.LCM.6

IC Identification data

During initialisation the IDeal Pass v2.3-n JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) Applet is installed and initiated with the Pre-Personalisation Agent key and the IC Identification data. The INSTALL for INSTALL method of the NXP JCOP 3 P60 will be used to store the IC Identification data.

7.2 SFRs and TSS

7.2.1 SFRs and TSS - Rationale

7.2.1.1 TOE Summary Specification

7.2.1.1.1 SF.IA Identification and Authentication

SF.IA.1 The implementation of PACE contributes to:

FIA_AFL.1/PACE, Authentication failure handling PACE authentication using non-blocking authorisation data. The TOE increases the reaction time of the TOE after an unsuccessful authentication attempt with a wrong PACE passwords.

FIA_UID.1/PACE, Timing of identification. The TOE allows to carry out the PACE Protocol after successful user identification

FIA_UAU.1/PACE, Timing of authentication. The TOE prevents reuse of authentication data related to the PACE protocol, i.e. according authentication mechanisms.

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

FIA_UAU.5/PACE, Multiple authentication mechanisms to support user authentication. The TOE provides multiple authentication mechanisms, PACE, symmetric key based authentication mechanism, etc.

FIA_UAU.6/PACE, Re-authenticating of Terminal by the TOE. The TOE re-authenticates the connected terminal, if a secure messaging error occurred.

FCS_CKM.1/DH_PACE, Diffie-Hellman key generation for PACE session keys provided by SF.CF.6

FCS_CKM.4, Cryptographic key destruction – Session keys provided by SF.CF.7

FCS_COP.1/PACE_ENC, Cryptographic operation – Encryption / Decryption AES / 3DES provided by SF.CF.1

FCS_COP.1/PACE_MAC, Cryptographic operation MAC/CMAC provided by SF.CF.1

FDP_ACF.1/TRM, Security attribute based access control, provided by SF.AC

FDP_UCT.1/TRM,Basic data exchange confidentiality – MRTD provided by SF.AC

FDP_UIT.1/TRM,Data exchange integrity provided by SF.AC

FDP_RIP.1, Subset residual information protection provided by SF.AC

FMT_MTD.1/KEY_READ, Management of TSF data – Key Read protection of PACE Passwords provided by SF.LCM.5

FIA_AFL.1/Suspend_PIN Authentication failure handling for Polymorphic eMRTD.

FIA_AFL.1/Suspend_PUK Authentication failure handling for Polymorphic eMRTD.

SF.IA.2 The implementation Chip Authentication v1. contributes to

FIA_API.1/CA, Authentication Proof of Identity – MRTD. Requires to implement Chip Authentication.

FIA_UAU.6/EAC Re-authenticating of Terminal by the TOE. The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.

FMT_SMR.1/PACE, Security Roles provided by SF.LCM.2

FMT_MTD.1/CAPK, Chip Authentication Private Key provided by SF.LCM.2

FMT_MTD.1/KEY_READ, Management of TSF data – Key Read provided by SF.LCM.5

SF.IA.3 The implementation of Terminal Authentication v.1 contributes to

FIA_UAU.5/PACE (FIA_UAU.5/PACE_CAM for PACE CAM), Multiple authentication mechanisms required to provide Terminal Authentication v1

FIA_UID.1/PACE (FIA_UID.1/PACE_CAM for PACE CAM), Timing of identification

FMT_MTD.3 Secure TSF data

FMT_SMR.1/PACE Security Roles

FCS_COP.1/SIG_VER (ECDSA signatures only)

SF.IA.4 The implementation contributes to

FIA_UAU.5/PACE (FIA_UAU.5/PACE_CAM for PACE CAM), Multiple authentication mechanisms, requires to authenticate the Personalization Agent by symmetric authentication mechanisms Triple-DES or AES which is provided by the TOE.

FIA_UAU.4/PACE (FIA_UAU.4/PACE_CAM for PACE CAM) Single-use authentication of the Terminal by the TOE

FIA_UAU.1/PACE (FIA_UAU.1/PACE_CAM for PACE CAM) Timing of authentication

FMT_SMR.1/PACE Security Roles

SF.IA.5 The implementation of Active Authentication contributes to

FIA_API.1/AA Authentication Proof of Identity – MRTD

FMT_SMR.1/PACE Security Roles provided by SF.LCM.2

FMT_MTD.1/AAPK, Active Authentication Private Key provided by SF.LCM.2

FMT_MTD.1/KEY_READ, Management of TSF data – Key Read provided by SF.LCM.5

FCS_COP.1/SIG_GEN, Cryptographic operation – Signature generation by travel document (RSA and ECDSA)

SF.IA.6 The implementation of PACE CAM contributes to:

FIA_AFL.1/PACE, Authentication failure handling PACE authentication using non-blocking authorisation data. The TOE increases the reaction time of the TOE after an unsuccessful authentication attempt with a wrong PACE passwords.

FIA_UID.1/PACE_CAM, Timing of identification. The TOE allows to carry out the PACE CAM Protocol after successful user identification

FIA_UAU.1/PACE_CAM, Timing of authentication. The TOE prevents reuse of authentication data related to the PACE CAM protocol, i.e. according authentication mechanisms.

FIA_UAU.4/PACE_CAM, Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

FIA_UAU.5/PACE_CAM, Multiple authentication mechanisms to support user authentication. The TOE provides multiple authentication mechanisms, PACE_CAM, symmetric key based authentication mechanism, etc.

FIA_UAU.6/PACE_CAM, Re-authenticating of Terminal by the TOE. The TOE re-authenticates the connected terminal, if a secure messaging error occurred.

FCS_CKM.1/DH_PACE, Diffie-Hellman key generation for PACE session keys provided by SF.CF.6

FCS_CKM.4, Cryptographic key destruction – Session keys provided by SF.CF.7

FCS_COP.1/PACE_ENC, Cryptographic operation – Encryption / Decryption AES / 3DES provided by SF.CF.1

FCS_COP.1/PACE_MAC, Cryptographic operation MAC/CMAC provided by SF.CF.1

FDP_ACF.1/TRM, Security attribute based access control, provided by SF.AC

FDP_UCT.1/TRM,Basic data exchange confidentiality – MRTD provided by SF.AC

FDP_UIT.1/TRM,Data exchange integrity provided by SF.AC

FDP_RIP.1, Subset residual information protection provided by SF.AC

FMT_MTD.1/PACE_CAM_KEY_WRITE, Modular invert of the CA key provided by SF.LCM.2

FMT_MTD.1/PACE_CAM_KEY_READ, Management of TSF data – Key Read protection of PACE Passwords and Modular invert of the CA key provided by SF.LCM.5

SF.IA.7 The implementation of PMA contributes to:

FIA_AFL.1/PACE, Authentication failure handling

FCS_CKM.1/DH_PACE

FCS_CKM.4, Cryptographic key destruction

FCS_COP.1/PACE_ENC

FCS_COP.1/PACE_MAC

FDP_UCT.1/TRM

FDP_UIT.1/TRM

FMT_MTD.1/KEY_READ

FDP_ACF.1/TRM

FDP_RIP.1

FIA_API.1/CA

FIA_UAU.6/EAC

FMT_MTD.1/CAPK

FMT_MTD.3

FCS_COP.1/SIG_VER (ECDSA signatures only)

FCS_COP.1/POLY Cryptograpic operation provided for randomization operation on PP, PIP and CPI polymorphic attributes (EC-Point addition and scalar multiplication)

FCS_CKM.1/POLY Cryptographic key generation provided for random number generation, used in randomization

FIA_UID.1/POLY Timing of identification

FIA_UAU.1/POLY Timing of authentication

FIA_UAU.4/POLY Single-use authentication mechanisms

FIA_UAU.5/POLY Multiple authentication mechanisms

FIA_UAU.6/POLY Re-authenticating
FDP_RIP.1/POLY Subset residual information protection
FDP_ACC.1/POLY Subset access control
FDP_ACF.1/POLY Security attribute based access control
FMT_SMR.1/POLY Security roles
FPR_ANO.1 Anonymity
FPR_UNL.1 Unlinkability

SF.IA.8 The implementation of Polymorphic eMRTD Document Holder verification for Polymorphic eMRTD contributes to:
FIA_AFL.1/PACE, Authentication failure handling
FCS_CKM.1/DH_PACE
FCS_CKM.4, Cryptographic key destruction
FCS_COP.1/PACE_ENC
FCS_COP.1/PACE_MAC
FDP_UCT.1/TRM
FDP_UIT.1/TRM
FMT_MTD.1/KEY_READ
FDP_ACF.1/TRM
FDP_RIP.1
FIA_UID.1/POLY Timing of identification
FIA_UAU.1/POLY Timing of authentication
FIA_AFL.1/Block_PIN Authentication failure handling
FIA_AFL.1/Block_PUK Authentication failure handling

7.2.1.1.2 SF.CF Cryptographic functions support

SF.CF.1 The implementation of this security function contributes to:
FCS_COP.1/PACE_ENC Cryptographic operation – Encryption / Decryption
FCS_COP.1/PACE_MAC Cryptographic operation MAC
FCS_COP.1/CA_ENC Cryptographic operation – Symmetric Encryption / Decryption
FCS_COP.1/CA_MAC Cryptographic operation – Cryptographic operation MAC

SF.CF.2 The implementation of this security function contributes to:
FCS_COP.1/SIG_GEN
FCS_COP.1/SIG_VER
FCS_CKM.1/DH_PACE

FCS_CKM.1/CA (implicitly contains the requirements for the hashing functions used for key derivation)

FIA_API.1/AA

SF.CF.3 The implementation of this security function contributes to:

FCS_COP.1/SIG_GEN (Supports ECDSA and RSA signature generation)

SF.CF.4 The implementation of this security function contributes to:

FCS_COP.1/SIG_VER (ECDSA signature verification)

SF.CF.5 The implementation of this security function contributes to:

FIA_API.1/CA

FCS_CKM.1/CA

FCS_CKM.1/DH_PACE

SF.CF.6 The implementation of this security function contributes to:

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

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

SF.CF.7 The implementation of this security function contributes to:

FCS_CKM.4/ Cryptographic key destruction – Session keys

FDP_RIP.1.

SF.CF.8 The implementation of this security function contributes to:

FCS_RND.1/ Quality metric for random numbers

SF.CF.9 The implementation of this security function contributes to:

FCS_CKM.1/POLY Cryptographic key generation for for Polymorphic eMRTD

FCS_COP.1/POLY Cryptographic operation for Polymorphic eMRTD

7.2.1.1.3 SF.ILTB Protection against interference, logical tampering and bypass

SF.ILTB.1 The implementation of this security function contributes to:

FPT_FLS.1 Failure with preservation of secure state

FPT_TST.1 TSF testing

FPT_PHP.3 Resistance to physical attack

7.2.1.1.4 SF.AC Access control / Storage and protection of logical travel document data

SF.AC.1 The implementation of this security function contributes to:

FDP_ACC.1/TRM Subset access control

FDP_ACF.1/TRM Security attribute based access control,

FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD

FDP_UIT.1/TRM Data exchange integrity

FDP_RIP.1 Subset residual information protection

7.2.1.1.5 SF.SM Secure Messaging

SF.SM.1 The implementation of this security function contributes to:

FTP_ITC.1/PACE: trusted channel after PACE

FCS_COP.1/PACE_ENC: Encryption/Decryption after PACE

FCS_COP.1/PACE_MAC: MAC generation/verification after PACE

FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE)

FCS_COP.1/CA_ENC Encryption/Decryption after Chip Authentication v1

FCS_COP.1/CA_MAC MAC generation/verification after Chip Authentication v1

FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD (ENC), after Chip Authentication v1

FDP_UIT.1/TRM Data exchange integrity – MRTD (MAC), after Chip Authentication v1

SF.SM.2 The implementation of this security function contributes to:

FIA_UAU.6/PACE (FIA_UAU.6/PACE_CAM for PACE) Re-authenticating – Re-authenticating of Terminal by the TOE

7.2.1.1.6 SF.LCM Security and life cycle management

SF.LCM.1 The implementation of this security function contributes to:

FMT_SMF.1 Specification of Management Functions (Initialisation part)

FMT_SMR.1/PACE Security roles (Manufacturer)

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialisation Data and Pre-personalization Data

FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialisation Data and Pre-personalization Data

FMT_MTD.1/PA

FMT_MTD.1/Change_PIN Management of TSF data for Polymorphic eMRTD

SF.LCM.2 The implementation of this security function contributes to:

FMT_SMF.1 Specification of Management Functions (Personalization and Configuration)

FMT_SMR.1/PACE Security roles (Personalization Agent)

FMT_MTD.1/PA, Personalization Agent Ability to write the Document Security Object (SOD)

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

FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key Restriction of the ability to load the Chip Authentication Private Key to the Personalization Agent.

FMT_MTD.1/AAPK Management of TSF data – Active Authentication Private Key Restriction of the ability to load the Active Authentication Private Key to the Personalization Agent.

FMT_MTD.1/PACE_CAM_KEY_WRITE Management of TSF data – Modular invert of the CA key Restriction of the ability to write the Modular invert of the CA key to the Personalization Agent.

FMT_MTD.1/Initialize PIN Management of TSF data for Polymorphic eMRTD

FMT_MTD.1/Change_PIN Management of TSF data for Polymorphic eMRTD

FMT_MTD.1/Unblock_PIN Management of TSF data for Polymorphic eMRTD

FMT_MTD.1/Resume_PIN Management of TSF data for Polymorphic eMRTD

FMT_MTD.1/PI_PP_CPI Load Management of TSF data for Polymorphic eMRTD

SF.LCM.3 The implementation of this security function contributes to:

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1/PACE Security roles (Personalization Agent)

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

FMT_MTD.3 Secure TSF data

FMT_MTD.1/DATE Current date

FMT_MTD.1/Initialize PIN Management of TSF data for Polymorphic eMRTD

FMT_MTD.1/Change_PIN Management of TSF data for Polymorphic eMRTD

FMT_MTD.1/Unblock_PIN Management of TSF data for Polymorphic eMRTD

FMT_MTD.1/Resume_PIN Management of TSF data for Polymorphic eMRTD

SF.LCM.4 The platform implementation provides this security function and contributes to:

FMT_LIM.1 Limited capabilities

FMT_LIM.2 Limited availability

FMT_LIM.1/POLY Limited capabilities for Polymorphic eMRTD

FMT_LIM.2/POLY Limited availability for Polymorphic eMRTD

SF.LCM.5 The implementation of this security function contributes to:

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

FMT_MTD.1/PACE_CAM_KEY_READ

FPT_EMS.1 TOE Emanation

FMT_MTD.1/Unblock_PIN Management of TSF data for Polymorphic eMRTD
FMT_MTD.1/Resume_PIN Management of TSF data for Polymorphic eMRTD
FMT_MTD.1/PI_PP_CPI Read Management of TSF data for Polymorphic eMRTD

SF.LCM.6

FAU_SAS.1 Audit storage

The audit records are usually write-only-once data of the travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS).

8 Annex

Glossary

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 SOD 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-personalization 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 personalized 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.

Term	Definition
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.
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].

Term	Definition
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CV Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [ICAO-9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Details Data	Data printed on and electronically stored in the 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

Term	Definition
	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) [6] [7]
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	[PP-SAC] 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). 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 Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.

[6] 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.

[7] 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
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 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).

Term	Definition
Inspection	The act of a State examining an MRTD presented to it by a traveler (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 traveler and verifying its authenticity and (ii) verifying the traveler 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 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) 1. personal data of the travel document holder 2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), 3. the digitized portraits (EF.DG2), 4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and 5. the other data according to LDS (EF.DG5 to EF.DG16). 6. 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]

Term	Definition
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 as read from the MRZ, see [ICAO-9303] part 11; • 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

Term	Definition
	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 1.4.3.3, TOE life-cycle, Phase 3, Step 6).
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document and (optionally) the polymorphic eMRTD extensions for the travel document or polymorphic document holder by some or all of the following activities: ICAO SAC/EAC 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 personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [TR-03110-1], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO-9303] (in the role of DS).

Term	Definition
	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. (i) individual-related data (biographic and biometric data) of the travel document holder, (ii) dedicated document details data and (iii) 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.
Personalization 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 (i) by the Personalisation Agent to prove his identity and get access to the logical travel document and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization 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) 1. biographical data, 2. data of the machine-readable zone, 3. photographic image and 4. other data.
Pre-personalization	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)

Term	Definition
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization 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 (i) PACE or BAC and (ii) Passive Authentication with SO_D. SIP can generally be used by BIS-PACE and BIS-BAC.
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.

Term	Definition
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
Travel document	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, 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.
Traveler	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) (i) stored in the context of the ePassport application of the travel document as defined in [5] and (ii) 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.

Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

References

Reference	Description
[AGD_OPE]	2017_2000032685 - OPERATIONAL PROCEDURES FOR IDEAL PASS v2.3-n JC with Privacy Protection. v2.1. IDEMIA
[AGD_PRE]	2017_2000032686 - PREPARATIVE PROCEDURES FOR IDEAL PASS v2.3-n JC with Privacy Protection. v2.7. IDEMIA
[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
[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.
[EAC-PP-V2]	Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP) BSI-CC-PP-0056-V2-2012-MA-02, Version 1.3.2, December 5th 2012, BSI
[EACv2-PP]	Common Criteria Protection Profile 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
[ICAO-9303]	International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – 7th edition, 2015
[ISO14443]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11
[ISO15946-2]	ISO/IEC15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 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

Reference	Description
[ISO7816]	ISO/IEC 7816: Identification cards — Integrated circuit cards, Version Second Edition, 2008
[ISO9796-2]	ISO/IEC 9796-2: 2002, Information Technology - Security Techniques - Digital Signature Schemes giving message recovery - Part 2: Integer factorization based mechanisms
[PLTF-ST]	JCOP 3 P60, Security Target Lite, Rev. 3.8, 2018-10-23. NXP
[PLTF-PRE]	JCOP 3 SECID P60 CS (OSB), User Guidance and Administration Manual, Rev. 3.1 - 2018-10-23. NXP
[NIST-180-4]	NIST. FIPS 180-4, Secure Hash Standard, February 2011.
[NIST-800-38B]	NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, 2005
[PACE-PP]	Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01, Version 1.0.1, 22 July 2014, BSI
[PCA-eMRTD]	Polymorphic eMRTD Specification. V2.1. 03-04-2018. IDEMIA.
[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
[SIC-PP]	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.
[ST-BAC]	2018_2000036360 - Security Target Lite IDeal Pass v2.3-n JC with Privacy Protection (BAC Configuration). IDEMIA
[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
[TR-03111]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, 17.04.2009